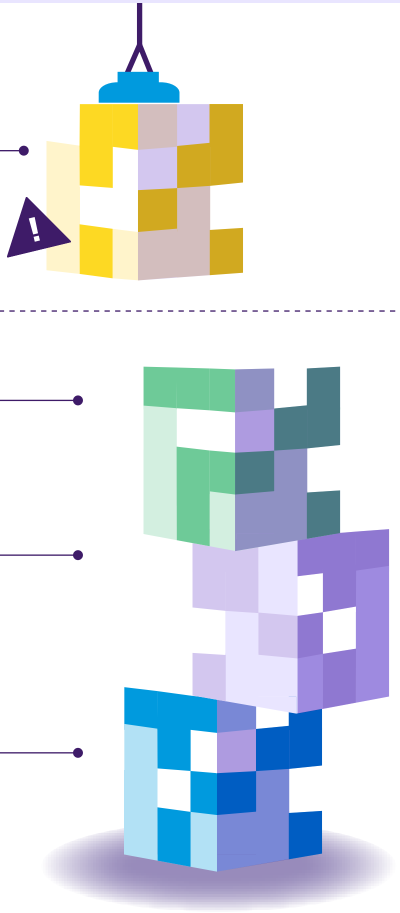
SUPERVISION REPORT

12 Building blocks for controlled use of auditing tools

In short Auditing tools – including (Gen)AI – offer significant opportunities for audit firms: more efficient processes, higher audit quality and general appeal of the audit work itself. The AFM supports innovation, provided it is applied responsibly and controlled properly. We observe that some larger audit firms are taking the lead by designing and implementing clear policies on the use of auditing tools in statutory audits, while others have yet to establish a solid foundation. Across the sector, there is still room for improvement in ensuring controlled use. To assist in this, the AFM introduces 12 building blocks that help assess what is going well and where improvement is needed. The lower three layers of the structure must be firmly in place before deploying advanced technologies such as (Gen)AI. First, solidify the foundation, strengthen it where necessary and then continue building towards sustainable quality and trust.



(Gen)AI tools 4
The (Gen)AI tool is used in a controlled manner.

Building blocks:
- The (Gen)AI tool is deployed safely and in a controlled manner.
- the outcomes from the (Gen)AI tool are verifiable or replicable.
- The external auditor is ultimately responsible for the outcomes from the (Gen)AI tool.

Establish a solid foundation

Auditing tools 3
The auditing tool is implemented in a controlled manner.

Building blocks:
- Develop knowledge and skills alongside innovation.
- Integrate the implementation of auditing tools into the overall audit strategy and audit plan.
- Follow up on the outcomes of auditing tools.

Input data 2
The input data is relevant and reliable to obtain sufficient and appropriate audit evidence.

Building blocks:
- Perform the appropriate IT procedures that ensure the relevance and reliability of the input data.
- Determine that relevant and reliable input data is used to obtain sufficient and appropriate audit evidence.
- Implement a consistent ETL process and document it.

Risk management 1
The audit firm maintains a robust risk management framework and effective internal controls.
This is the base.

Building blocks:
- Use an appropriate information security framework.
- Formalise policy on auditing tools.
- Monitor the effect of auditing tools on the audit quality.

DECEMBER 2025

Contents

Introduction

Technological developments and digitalisation are rapidly changing the way audit firms perform their work, emphasising the importance of controlled use of auditing tools. These developments create opportunities such as increased efficiency and quality of the audit work, and the general appeal of the audit practice.[1] However, these developments also introduce risks: insufficient understanding of the technology and incorrect use can undermine the quality of statutory audits and can expose audit firms to operational vulnerabilities.[2,3]

We identify several 'key drivers' behind the adoption of new auditing tools and behind the increased attention that audit firms pay to information security. Examples include the availability of new technologies, efforts to mitigate staff shortages and pressure from private equity parties to drive efficiency. These trends are making auditing tools an increasingly essential component to the audit practice. At the same time, information security risks are a growing concern for the sector. This is partly due to the increasing risk of cybercrime: audit firms process confidential data which makes them attractive targets for cyber criminals. Also, new laws and regulations – such as the Digital Operational Resilience Act (DORA), the (Dutch) 'Baseline Informatiebeveiliging Overheid versie 2' (BIO2) and the Network and Information Security Directive 2 (NIS2) – result in increased attention from audit firms to further strengthen their digital resilience.

We support innovation within the audit industry while emphasising the importance of controlled and responsible use of technologies. Audit firms manage significant volumes of data from the parties they audit. It is crucial that data is processed, transferred and stored safely and securely. The data, used as input for auditing tools, should be relevant and reliable to obtain sufficient and appropriate audit evidence to support the auditor's opinion. Furthermore, auditing tools must perform reliable and transparent analyses to guarantee the quality of statutory audits, ensuring the general public's trust in the accountancy sector.

We have conducted an exploratory review of the use and scope of auditing tools in statutory audits and its effect on the quality of the statutory audit. This concerns auditing tools in the broadest sense, from audit-documentation software to data-analytics tools[4] and (Gen)AI[5], across all phases of the audit process. An overview is presented on page 27 of this report. Our research has been carried out at eleven audit firms with a regular licence to perform statutory audits (hereinafter: non-PIE audit firms)[6] and at two audit firms with a licence that also extends to the performance of statutory audits of public interest entities (hereinafter: PIE audit firms). During the on-site investigations, we examined each firm's quality control system and the implementation of various auditing tools in two different statutory audit files. To gather additional context, we had in-depth discussions with various stakeholders, including suppliers of eight different auditing tools and various sector organisations as well as professional bodies. Lastly, in addition to data from non-PIE audit firms that is already available, we have included data from a request sent to the

[1] Committee of European Auditing Oversight Bodies ("CEAOB") - Challenges and applications of advanced technologies in audit firms. (published in October 2024)

[2] Autoriteit Financiële Markten ("AFM") – Trend Monitor 2026 p. 43 – (published in November 2025)

[3] International Forum of Independent Audit Regulators ("IFIAR") - Use of technology in audits - observations, risks and further evolution. (published in March 2025)

[4] In line with NBA Handreiking 1141 (published in June 2019) we apply the following definition of data analytics: "Data analytics is the process of identifying patterns, anomalies, and inconsistencies, and extracting additional useful information about the subject matter under review through analysis, modelling, and visualization, for the purpose of planning or performing the engagement."

[5] (Gen)AI refers to a 'general-purpose AI model' as defined in Article 3, definition 63 of Regulation (EU) 2024/1689 of the European Parliament and of the Council.

[6] These audit firms were selected based on data provided by non-PIE audit firms for the year 2024. This data is presented in Figure 4.3 on page 43 of Trend Monitor 2026.

six Dutch PIE audit firms. The data is used to compare the firm-wide use of auditing tools for the PIE audit firm population through various subsections where these supported our exploratory findings.

The sector demonstrates substantial potential for enhancement in both governance and control in relation to the implementation of auditing tools. While some larger audit firms appear to be leading the way with mature information security policies and tool-specific firm-level policies, most firms have embedded a less formalised framework for controlled implementation of auditing tools. In addition, our research indicates requirements for improvement in the areas of risk management (which includes third-party/vendor management) and the controlled implementation of auditing tools. Where audit firms implemented little formal policies, among the population in our research, the necessity for maturity in these areas is particularly evident. However, even among the firms with more mature internal control frameworks, we have identified several opportunities where improvements to governance and control measures would provide a more robust basis for the implementation of auditing tools within these firms.

To provide some support to the sector, our report defines important preconditions for the controlled use of auditing tools. We have defined these preconditions using 12 building blocks. If audit firms seriously consider these preconditions and work on their improvement areas where gaps are identified, they will be able to further enhance the firm's controlled use of auditing tools.

What does the AFM expect?
A structure that will not weaken or collapse because one or more preconditions fall short. The AFM encourages audit firms to critically assess how auditing tools are implemented within their firm, ensuring controlled use within all statutory audits.

Therefore, make sure to answer the following questions for your organisation: *Which building blocks* should or could our organisation use? Does our organisation need all of the *building blocks* to ensure a robust structure? And: Are there any other relevant *building blocks* besides the 12 mentioned in this report?

It is up to audit firms and auditors to answer these questions, based on factors such as the nature of the individual audit or the auditing tools in use at the firm. Choices to include or exclude preconditions from review should be seriously considered to ensure compliance with applicable laws and regulations.

Our call to action: We expect audit firms to use the *building blocks* in this report to evaluate their strengths and weaknesses to improve their structure where it is required. The AFM's call to action: Check your firm's foundational structure using the *building blocks*, strengthen it where necessary and continue to build on quality and trust.

In the coming years the AFM will pay more attention to the controlled use of auditing tools in further supervisory reviews.[7]

[7] AFM – Trend Monitor 2026 p. 48: Considering the risks identified by the AFM, this topic will receive increased attention in (supervisory) reviews in the coming years

12 Building blocks for controlled use of auditing tools – based on 4 preconditions

Precondition 1: the audit firm maintains a robust risk management framework and effective internal controls

Why this precondition? Effective risk management and internal controls are essential for the responsible use of auditing tools. The audit firm's management board plays a critical role in the process. The board is responsible for establishing robust information security and for developing policies that enable the controlled use of auditing tools. The board must ensure an adequate information security framework, oversee the implementation of tool-specific policies across the organisation and establish consistent monitoring activities for the use and effect of auditing tools to ensure controlled use within the firm.[8]

What are the AFM's observations for this precondition? It appears that audit firms do not always adequately establish a formalized risk management framework and relevant internal controls in relation to auditing tools. At several firms we have identified shortcomings within the information security framework. We also see that attention is required to formalize third-party vendor management. Lack of attention in these areas results in inadequate management of potential cyber risks. Furthermore, tool-specific policies for the deployment and monitoring of auditing tools are often insufficiently formalised, resulting in risks during the execution of audit procedures. Lastly, we see that risk awareness at the board-level at audit firms requires attention.

Building block 1: use an appropriate information security framework. Cybersecurity is critical for audit firms, particularly as the audit process becomes increasingly data driven. However, we see that many audit firms remain vulnerable, operating with ad hoc policies, limited oversight of third parties and insufficient awareness of the risks among the board within the firms. A robust risk management framework provides a solid foundation for ensuring that information security is designed to be future-proof and could avoid audit firms "being hacked because they slacked".

Building block 2: formalise policy on auditing tools. In practice, audit firms are increasingly integrating auditing tools into their audit approach. However, many organisations still lack a formalised policy governing its use. As a result, tool-implementation is not always efficient or effective for the purpose of the planned audit procedures. By formalising policy, the board can establish control over the implementation of auditing tools.

Building block 3: monitor the effect of auditing tools on the audit quality. Auditing tools often provide functionality for usage monitoring, enabling their deployment to be measured across the organisation. Systematic monitoring provides the board with insight into the effect of auditing tools on the statutory audit, for example by assessing whether the relevant functionalities of auditing tools are applied in preparing audit activities or whether staff continue to rely on traditional methods. These considerations allow management to make timely adjustments where necessary or to encourage desired behaviour within the firm. The AFM observes that audit firms lack structural monitoring of the use and effect of auditing tools within their audit practice. As a result, incorrect use, technical errors or potentially significant deficiencies may go unnoticed, negatively affecting audit quality.

[8] Financial Reporting Council ("FRC") - Certification of Automated Tools and Techniques (published in June 2025)

Precondition 2: The input data is relevant and reliable to obtain sufficient and appropriate audit evidence

Why this precondition? Auditing tools can assist the auditor in collecting, sorting, filtering and analysing the audit client's data. To derive appropriate and sufficient audit evidence from an auditing tool, it is crucial that its input data is relevant and reliable and aligns with the audit objective. The sufficiency and appropriateness of outcomes produced by auditing tools directly depend on the relevance and reliability of the input data. Therefore, the external auditor must perform the appropriate procedures to evaluate the relevance and reliability of information intended to be used as audit evidence, including its accuracy and completeness where necessary.

What are the AFM's observations for this precondition? We observe that auditors do not always perform adequate procedures to verify the relevance and reliability of input data (amongst which the accuracy and completeness of non-financial data-elements). We frequently identify that insufficient attention is paid to ineffective general IT controls ("GITCs")[9] in the entity's IT environment and the effect on reliance and reliability of the data derived from these systems. Also, substantive procedures in this area (e.g. verification of data at the source) are often inadequately set-up to provide a conclusion on this precondition. We see instances where input data is obtained from systems with weak internal controls, leading to doubts about the reliability of these data. However, these doubts are not addressed by the external auditor. Furthermore, auditors do not always maintain the appropriate safeguards to ensure relevant and reliable data is obtained from an audit client. This can happen when the audit firm does not have a formalized policy which ensures external auditors use a right approach to mitigate potential risks of unreliable data, leading to issues further on in the audit.

Building block 4: perform the appropriate IT procedures that ensure the relevance and reliability of the input data. The external auditor (the statutory auditor under applicable law) must have a thorough understanding of how risks related to the effectiveness of an audit client's general IT controls (GITCs) can impact the relevance and reliability of data. Therefore, the auditor should perform sufficiently detailed procedures to address potential risks. Our research indicates auditors do not always pay sufficient attention to GITCs and other IT-related risks to conclude that input data is relevant and reliable (and where relevant: accurate and complete).

Building block 5: determine that relevant and reliable input data is used to obtain sufficient and appropriate audit evidence. When the external auditor receives data from the audit client and uses it as input data for auditing tools, it is important that the appropriate procedures are performed to determine that relevant and reliable data is used to obtain sufficient and appropriate audit evidence. In practice, we see that auditors do not always maintain the right safeguards to ensure that the relevant and reliable data is received from audit clients. For example by carrying out work to verify the accuracy and completeness of input data, ensuring that such data is reconciled with underlying accounting records and, where appropriate, original source documents.

Building block 6: implement a consistent ETL process and document it. Audit firms must ensure a consistent Extract-Transform-Load ("ETL") process, preferably through firm-wide policy. The external auditor must ensure this process is documented with sufficient detail within the audit file. A more mature ETL process ensures that relevant processing-steps are traceable, even if specialists or external parties are involved, which contributes to the evaluation of the relevance and reliability of the data used as part of the audit. The external auditor should ensure the entire audit trail of data is sufficiently detailed for an experienced auditor to be able to fully understand the work performed. We have seen good examples at the audits in scope of this research, but we also see opportunities for improvement.

[9] NV COS 315.12d: This section provides the (Dutch) definition of GITCs used in this report.

Precondition 3: The auditing tool is implemented in a controlled manner

Why this precondition? Auditing tools are implemented as part of the audit process, but they only contribute to audit quality when their implementation is properly controlled. For adequate implementation on audits, it is important that the audit engagement team possesses knowledge and skills to operate these tools in a controlled manner. Similarly the role of auditing tools need to be clear in the audit plan, to ensure that the auditing tools are used appropriately.

What are the AFM's observations for this precondition? In practice, we see that auditing tools are not always implemented correctly. A controlled implementation requires the external auditor to understand the functionalities of the auditing tools, how these are deployed to achieve a high-quality audit, and how the outcomes contribute to obtaining sufficient and appropriate audit evidence. At times, we observe that the audit objective is overlooked, resulting in the use of the tool not fully aligning with the objectives set out in the audit plan.

Building block 7: develop knowledge and skills alongside innovation. Audit firms often have a wide range of auditing tools available, with many functionalities, and their full potential is not always realised. Possibly because staff members are unaware of the tool's possibilities or lack the knowledge needed to apply the tools correctly. Where knowledge or skills are lacking, audit firms can organise training programmes and provide practical guidance to staff, or draw on other specialisms to ensure that the necessary expertise and competencies are available within the organisation.

Building block 8: integrate the implementation of auditing tools into the overall audit strategy and audit plan. Auditing tools play a supporting role in the audit process; they are not an end in themselves. In practice, we observe that auditing tools are not always deployed based on the assessed audit risks or the overall audit plan, which can result in outcomes that provide less persuasive audit evidence. It is essential that auditing tools are embedded in the audit approach, aligned with identified risks and with the level of audit evidence that tools can deliver.

Building block 9: follow up on the outcomes of auditing tools. Auditing tools are used in statutory audits to generate audit evidence or other outputs. In practice we see room for improvement in how these outcomes are addressed, for example in cases of (possibly significant) exceptions and deviations that may lead to audit differences or other findings. It is important that users of auditing tools handle these outcomes appropriately to safeguard audit quality.

Precondition 4: the (Gen)AI tool is used in a controlled manner

Why this *precondition*? (Gen)AI introduces new, inherent risk factors due to the nature and complexity of the technology. The previous 9 *building blocks* are, of course, also relevant for the use of (Gen)AI tools. However, a controlled use of (Gen)AI tools in audit firms requires 3 additional building blocks.

What are the AFM's observations for this *precondition*? With (Gen) AI tools, we see a greater risk of **overreliance** compared to traditional auditing tools, due to the way outcomes are presented. Outputs from (Gen)AI tools can appear highly convincing because of the anthropomorphic characteristics of some tools. These tools mimic human traits, which often lead users to place trust in the outcomes more quickly and to assess them less critically. The phenomenon where GenAI outputs seem persuasive due to their structure and/or presentation can result in the "**Halo effect**". In addition to this effect, (Gen)AI-tool's processing steps with which outcomes are generated frequently lack transparency given the stochastic nature of the technology. For this reason, the AFM provides **3 additional building blocks** to support the controlled use of (Gen)AI.

Building block 10: the (Gen)AI tool is deployed safely and in a controlled manner. Traditional auditing tools are generally easier to control than (Gen)AI tools because traditional auditing tools are less complex. Due to the nature of (Gen)AI tools, it is more difficult to maintain control over the processing of input data and ensuring that tools continue to operate as intended by the audit firm.

Building block 11: the outcomes from the (Gen)AI tool are verifiable or replicable. With traditional auditing tools outcomes are (often) replicable because these are based on fixed and traceable rules and logic. (Gen)AI tools, such as chatbots which are built on large language models ("LLMs"), provide outputs based on statistics and complex algorithms, making the reasoning behind them often untransparent. Therefore, it is essential that outcomes of (Gen)AI tools, especially where used as audit evidence, are verifiable or replicable. This ensures the external auditor can take ultimate responsibility for outcomes.

Building block 12: the external auditor is ultimately responsible for the outcomes from the (Gen)AI tool. Auditing tools using (Gen)AI-technology are able to generate human-like outcomes. Therefore, we identify a risk that these outcomes will be adopted without the external auditor's critical assessment. It is essential that humans carefully assess the outcomes of (Gen)AI and independently make a decision. The external auditor must critically evaluate (Gen)AI output and determine independently when additional human verification is necessary.

Tone at the top essential for all building blocks

The audit firm's management board has the responsibility to ensure controlled and ethical business operations. This includes rules and procedures regarding auditing tools within the firm. The culture within the audit firm is a great influence on compliance of staff with these rules and procedures. This requires audit firm's board members to understand, internalise and communicate the risks and ethical implications of digitalisation to their employees.

For effective innovation, it's also greatly important that board members recognize technological opportunities and create enough freedom for innovation within the firm. By strategically guiding the innovation process and allowing employees to experiment with new technologies in a controlled manner, board members can stimulate sustainable and controlled innovation, ultimately resulting in a positive effect on audit quality.

We see that some audit firms distinguish between 'running the business' and 'changing the business'. By distinguishing between these two business lines, specific responsibilities are assigned to staff members who guide the innovation process. As a result daily operations are separated from the innovation strategy, providing focus for staff members. This enables board members to guarantee stability in the organisation, while simultaneously space for controlled innovation is being created.

The management board has the responsibility to promote a culture that supports sustainable and controlled innovation. We have seen good examples where the audit firm's management board creates room for discussions about obstacles, mistakes and moral dilemmas in the implementation of auditing tools. In these examples, staff members engage in dialogue with the board, and relevant signals are carefully considered when developing new policies and procedures. This culture contributes to a learning organisation in which employees experience psychological safety to work with innovative auditing tools without fear of undue consequences if they do not understand certain tool features, as they can openly discuss these challenges and seek support.

The management board determines how to address changes in staffing and knowledge requirements arising from efficiency improvements introduced by new technology. Digitalisation can enhance efficiency, freeing up time for additional tasks and potentially improving audit quality. This extra time allows for greater application of professional judgement and technical depth for auditors, which may contribute to increased job satisfaction. However, it may also require new or existing staff to obtain more in-depth knowledge necessary to complete more technical and challenging work. The audit firm's management board should assess these potential challenges and sufficiently prepare their staff to ensure they possess the necessary skills and expertise to perform more complex and technically demanding audit work. This includes implementing targeted training programmes, fostering continuous learning and monitoring progress to maintain audit quality and uphold professional standards.

Greater reliance on auditing tools makes a solid framework essential

From the exploratory research leading to this report, we have identified the following drivers at audit firms, leading to increased attention and use of innovative auditing tools and the exploration of new technology:

1. **Keeping pace with audit client digitalisation.** Audit clients are processing ever-increasing amounts of data and are working with increasingly complex interconnected IT systems. Audit firms deploy (remote access interfaced) auditing tools that supports data-driven and controls-based audit activities. This allows them to better respond to the increasingly digital business operations of their clients.
2. **Meeting client expectations on data use.** Clients expect auditors to handle their data securely, efficiently and effectively during statutory audits. Auditing tools can improve efficiency and quality while providing deeper insights into client operations – insights that may also be shared with clients.[10]
3. **Leveraging emerging technologies.** Innovations such as machine learning and generative AI offer functionalities that enhance audit quality and efficiency. We have seen that audit firms are increasingly adopting these technologies as opportunities for improvement of their services, and to realise improvements in efficiency and/or audit quality.[11]
4. **Addressing workforce challenges.** Technology enables automation of repetitive tasks and more efficient audit processes, freeing up time for complex and intellectually rewarding work. This can improve job attractiveness and support staff retention and recruitment.
5. **Transition from legacy audit documentation systems.** The phase-out of widely used on-premise audit documentation software creates an opportunity for audit firms to adopt solutions with more advanced technology and functionalities, including AI and cloud-based tools. This necessary migration accelerates innovation.
6. **Private equity-driven efficiency.** Private equity investors often pursue efficiency through digitalisation to achieve scale and streamline processes. New auditing tools can deliver speed, insight and cost control. While these offer short-term benefits, the AFM also notes potential long-term risks.[12]

[10] Dutch Civil Code – Article 393 paragraph 4 of Book 2: This article stipulates that the external auditor must report to the supervisory board and the management board as part of his examination of the financial statements. This report must at least mention the auditor's findings regarding the reliability and continuity of the automated data processing.

[11] AFM – Trend Monitor 2026 p. 42: A data request in 2024 shows that 49% of non-PIE audit firms are using innovative tools, with most firms combining multiple types of tools. PIE audit firms have been using auditing tools for a longer time but are now increasingly deploying them for risk analyses and other non-routine audit procedures. They are also experimenting with emerging technologies such as (Gen)AI.

[12] AFM – Private equity in the auditing industry: public interest under pressure (published in April 2025)

We observe growing attention towards information security within the sector:

1. **Heightened cyber risk.** Increasing digitalisation and supply chain interconnectivity raises exposure to cybercrime. Audit firms are attractive targets due to the large volumes of confidential data they handle as part of their audit engagements. Incidents such as data breaches and ransomware attacks can cause significant reputational and financial harm, underscoring the need for structural digital resilience.[13] Audit firms seem to understate their own cyber risks. Firms must remain vigilant to these risks, as the consequences of a realised threat can be severe.[14]
2. **Regulatory developments.** Legislation such as the Digital Operational Resilience Act (DORA), the Government Information Security Baseline (BIO2) and the Network and Information Security Directive 2 (NIS2) impose stricter requirements for digital resilience. While audit firms may not be directly subject to these laws, they must demonstrate secure and robust IT processes when serving entities that are regulated by these laws. This chain obligation incentivises firms to strengthen their own information security measures.

[13] Algemene Inlichtingen- en veiligheidsdienst ("AIVD") - Verdedigbaar Netwerk Hoe doe je dat? (published August 2024)

[14] AFM – Trend Monitor 2026 p. 43: Audit firms report little cyber incidents and non-PIE audit firms appear to underestimate their own cyber risks. (published in November 2025)

1. Precondition 1: the audit firm maintains a robust risk management framework and effective internal controls

1.1 Building block 1: use an appropriate information security framework

As the audit process becomes increasingly data-driven, associated risks grow. Incidents such as data breaches, ransomware attacks, supply chain compromises, unauthorised access or loss of audit information can directly undermine trust, reliability and the integrity of the audit profession. Audit firms are particularly attractive targets for cybercriminals because they handle large volumes of confidential personal, controls and transactional data and often maintain (externally accessible) interfaces with third parties, including audit clients.

Our research has identified information security concerns at nearly all audit firms assessed. Some firms manage information security in an organic or ad-hoc manner, or have limited understanding of vulnerabilities relevant to their organisation because these risks have never been formally evaluated. Audit firms seem to understate and not critically assess their own cyber risks. Notably, firms policymakers do not always appear to recognise layered dependencies and emerging risks, such as cyber threats that may arise when quantum computing becomes accessible to cybercriminals.[15] We also observe that cloud strategies and the risk of digital dependency on software providers often do not receive consistent, structural attention within audit firms.[16, 17]

Information security is also critically important for third parties that process client data for audit firms, such as providers of auditing tools. These providers form a key link in the sector because they store and process data from multiple audit firms. As a result, a single vulnerability in a provider's IT environment can potentially affect several audit firms or the sector as whole. It is the responsibility of the audit firm's management board to address these risks proactively, for example by establishing clear agreements on secure and reliable data processing, multitenancy, retention, encryption (including customer managed keys), layered interface (including API) security from additional third parties and by reviewing these periodically and revising them where necessary. In addition, it may be prudent to include measures such as requiring annual penetration testing ("pen-testing"), reporting on ISO 27001 or SOC 2 certification, or inclusion of a "right to audit" clause in contractual terms with these parties.

A structured risk management framework for information security provides audit firms with the tools to manage cyber risks effectively. Such a framework makes risks transparent, defines roles and responsibilities and establishes a systematic approach to control measures, such as regular penetration testing, training and other internal checks. It also offers support when a cyber risk materialises. By implementing a well-organised framework, audit firms can demonstrate to external stakeholders that information security is a top priority and that the appropriate steps are being taken to mitigate risks. This can help limit financial and reputational damage for both the firm and, in the broader context, the sector as a whole.

[15] AIVD – Prepare for the threat of quantumcomputers (published in September 2021)

[16] Prof. Moerel, L. et al. - Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default (published in February 2024). For concrete measures regarding cloud security, simulation and implementation, consider for example the following within Azure: Ignite'25 Spotlight: Announcing Microsoft Baseline security mode | Microsoft Community Hub

[17] DNB - Digital dependence of the financial sector (published October 2025)

A good example of a risk management framework is the Good Practice Information Security issued by De Nederlandsche Bank (DNB).[18] The control measures within this framework are proportionate to the nature, size and complexity of audit firms. These measures extend beyond technological solutions to include human behaviour, process design and necessary facilities. A robust risk management framework incorporates preventive, detective, corrective and repressive controls, such as network security, encryption, logical access management, change management policies and policies for logging, monitoring and pen-testing. Boards should also periodically assess the information security practices of third parties, such as software vendors, against their own framework to ensure alignment and mitigate risks.

Good practice
An audit firm ensures that all participating and acquired firms use a uniform technical infrastructure which is centrally governed. This infrastructure includes approved networking devices and IT assets, as well as policies and procedures for permitted software, hardening, ensuring consistency across all member firms.

Explanation
A standardised, centrally managed infrastructure reduces complexity and fragmentation, limiting potential entry points for attackers. It improves visibility and control, enables consistent policy enforcement and simplifies incident response. For audit firms – where teams work across multiple clients, often remotely – such uniformity is essential to reduce misconfigurations, limiting the attack surface and strengthen overall information security risk management.

Good practice
We observe strong examples of audit firms performing external (maturity) assessments or tests on third parties that pose supply chain risks. In some cases, this included a detailed review of the ISO 27001 certification, SOC 2 and/or ISAE 3402 assurance reports. Certain audit firms also assess pen-test results from these parties to identify potential vulnerabilities and ensure alignment with their internal information security policy, agreed service level agreements (SLAs) and documented risk appetite.

Explanation
Evaluating third parties is an important way to apply the audit firm's information security policy throughout the supply chain. It enables the management board to take corrective measures where necessary and, if required, to adjust or terminate services with third parties to safeguard information security across the chain.

[18] DNB - Good Practice Information Security 2023: This publication provides institutions guidance to ensure the continuous availability, integrity, confidentiality and authenticity of (automated) data processing. (published in December 2023)

1.2 Building block 2: formalise policy on auditing tools

A formal policy for implementing new auditing tools is essential to mitigate risks related to information security and tool functionality. This process begins with a comprehensive risk assessment across relevant areas of expertise, including professional practice, cybersecurity[19], IT, legal (such as data privacy and independence), and learning & development. Where in-house expertise is insufficient, external specialists should be engaged prior to implementation.

When procuring and deploying new tools, a structured and controlled procurement process is critical. Procurement criteria, risk assessments and contractual provisions – covering information security, data retention and minimisation and change management – should clearly define supplier responsibilities. Boards must also address risks associated with digital dependency, such as vendor lock-in, and broader considerations such as data sovereignty.[20]

Procedures for testing and validating internally developed auditing tools are equally important to limit risks related to cybersecurity and tool-functionality as a whole. Where audit firms develop their own auditing tools, it's important to note that similar risks exist as where auditing tools are procured. However, with in-house development of auditing tools, additional risks may arise, requiring further measures. For example, in relation to technical and methodological safeguards or the DTAP street ('Development, Testing, Acceptance and Production').

Updates to auditing tools should be governed by policies that ensure quality and security requirements are consistently met. These policies must specify *how* changes are implemented and tested, considering the underlying technology, e.g. on-premise or cloud-based, and update frequency. For significant changes, the audit firm's management board is responsible for timely and adequate impact assessments and any necessary follow-up actions.

Tool-specific firm-level policies should ensure methodological integration within the audit approach, embedding tools into the audit methodology rather than treating them as standalone activities. Policies should define the audit phases where tools may be used, establish selection criteria and specify which assertions or risks the tool addresses and under which conditions it may be suitable for the audit objective or not. While tools support audit activities, the ultimate responsibility to comply with the applicable auditing standards and other laws and regulations remains with the external auditor.

Policies should also prescribe the methodology for using auditing tools, including the activities the external auditor must perform in different scenarios. They should detail what information may be processed by the tool; how the information should be evaluated on relevance and reliability before using it; and how the external auditor should interpret and follow up on findings from audit procedures where auditing tools are used, including their relationship to other audit procedures.

To ensure consistency in audit procedures executed within the firm, documentation requirements which are embedded in company policy, can ensure verifiability and replicability of procedures between audit teams. Policies should require auditors to document sufficient details to enable an experienced auditor to understand the nature, timing, extent, results and conclusions of the work performed. Standardised templates for documenting tool usage can promote consistency across audit files.

Policies can specify when and how specialists – such as data analysts and IT auditors – should be involved, what their responsibilities are, and how their work fits into the audit process. The involvement of specialists is often essential when applying more complex auditing tools or when dealing with complex IT systems at audit clients. This also includes meeting the relevant requirements under auditing standards for engaging a specialist as part of the engagement team or as an external expert.[21]

[19] CEAOB - Information Security & Cybersecurity Inspection Work Program (published in November 2021)

[20] DNB - Digital dependence of the financial sector (published October 2025)

[21] NV COS 220.12 of NV COS 620

When (GenAI) tools are used in statutory audit procedures, we expect audit firms to establish specific policies to manage the implementation of this technology. These policies should cover at least three areas:

1. Information security: safeguards for the secure processing of confidential (client) data and for the controlled implementation of the technology.
2. Verifiability or replicability: the ability to fully trace or reproduce outcomes that are used as audit evidence.
3. Ultimate responsibility: the external auditor remains responsible for all outcomes generated by the tool.

In addition, relevant compliance requirements –such as those under the AI Act[22]– must be incorporated into these policies.

Where AI agents play an active role in the statutory audit, additional policies for implementing appropriate control measures are essential.[23] AI agents can perform tasks autonomously and gain access to IT systems. This creates opportunities but also introduces risks for audit firms. Clear governance and robust safeguards and therefore critical to ensure responsible and secure use of these technologies.

To ensure that auditing tools are applied appropriately, policies should also define how their use will be systematically monitored and evaluated. This includes specifying the scope and frequency of monitoring activities. Effective monitoring enables the promotion of desired use while detecting and correcting undesired use in a timely manner.

Good practice
Our research identified several audit firms that have formalised policies and procedures governing the acquisition, development and implementation of auditing tools. These policies explicitly incorporate risk management considerations by addressing the aforementioned themes. Following implementation, these themes are reassessed considering the associated risks, scope and deployment of the tools.

Explanation
We encourage audit firms to establish a structured process for implementing auditing tools and for conducting periodic reviews within a comprehensive risk management framework.

1.3 Building block 3: monitor the effect of auditing tools on the audit quality

Monitoring the effect of auditing tools should form part of the firm's management information processes, as the insights generated support both strategic and operational decision making. The approach to monitoring auditing tools' effect on audit quality depends on the scope and manner of its deployment. The board should establish a monitoring framework aligned with quality objectives and relevant risks, supported by clearly defined key performance indicators (KPIs) and periodic assessments of monitoring activities. For audit firms, the insights provide guidance for strategic and operational decisions.

[22] European Union ("EU") - Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence: The EU AI Act is a European regulation on the safe and responsible use of artificial intelligence.

[23] NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

Good practice

An audit firm uses a dashboard to monitor the utilisation and scope of an auditing tool that is used to prepare audit procedures. This dashboard enables a board member to identify any significant deviations and outliers which were identified by the tool's analyses and how the auditor has addressed them.

Explanation

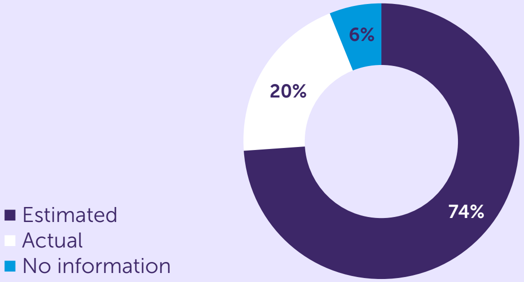
This systematic monitoring provides the management board with insights into the effect of auditing tools on the quality of statutory audits and allows the board to make timely adjustments where necessary. In addition, it allows desired behaviour to be recognised and encouraged within the organisation.

A variety of sources and methods can be used for monitoring. For example, data from auditing tools that automatically log usage patterns and anomalies can help identify trends and bottlenecks, including potential risks for the firm. Periodic engagement reviews by technical experts provide valuable insights by identifying incorrect use, inconsistencies or interpretation errors that might otherwise go unnoticed. User surveys offer additional perspectives on the effectiveness and implementation efforts of tools. Notifications from users – such as incident reports or queries – can further highlight issues related to quality and applicability. When tools are updated, A/B testing can be applied to compare changes against expected outcomes.[24] Finally, collecting metadata – such as which files and audit techniques are processed by tools, how tools are used, in specific periods or for specific audit procedures, and which functionalities are expected to be used for these procedures – can provide a robust basis for a more targeted analysis.

Monitoring – observations from the exploratory study

Our research shows that the monitoring of auditing tools and its effect on the quality of the statutory audit is not (always) prioritised. Often, organisations monitor use retrospectively, through sample-based internal quality assessments or user questionnaires. Audit firms indicated that they are assessing how to obtain better management information by adjusting monitoring activities.

Method of monitoring in % of audit tooling



Based on collected data, we see that, on average, the usage at audit engagement level is estimated for 74% of auditing tools. For 20% of auditing tools, usage is based on actual data (detailed user data). For 6% of auditing tools, it is not clear how they are monitored, because no information has been collected on the usage of these tools by the audit firms. The results are in line with similar publications.[25, 26]

[24] An A/B test (also known as a split test) is a method used to compare two versions of an auditing tool to determine which performs better.

[25] FRC - Certification of Automated Tools and Techniques (published in June 2025)

[26] IFIAR - Use of technology in audits - observations, risks and further evolution: This is the report of the Technology Task Force ("TTF") of IFIAR on the use of technology in the audit (published in November 2023)

2. Precondition 2: the input data is relevant and reliable to obtain sufficient and appropriate audit evidence

2.1 Building block 4: perform the appropriate IT procedures that ensure the relevance and reliability of the input data

We see that auditors do not always perform sufficient procedures for the assessment of GITCs in the entity's IT environment before using client data as input for auditing tools.[27] To assess risks in (often) complex internal IT systems of the audit client, relevant GITCs must be evaluated, especially when these systems form the basis of the administrative processing and/or are the source of information that is presented within the entity's financial statements.[28, 29, 30] Potential audit procedures include the review of: logical access controls, rights and roles within IT systems, change management, information security and immutable log registration.

The extent and depth of procedures performed by the auditor to assess GITCs depend on various factors.[31] If the audit client's IT systems are complex or the administrative organisation is highly IT-dependent, it becomes even more important to assess GITCs due to potential significant risks. In this scenario, the importance of assessing GITCs increases when auditing tools are used for audit procedures, as larger volumes of (potentially unreliable) information is processed to evaluate (significant) audit risks or relevant assertions to the audit.

If internal control risks are identified, the auditor must assess possible limitations impacting the relevance and reliability of information from these systems if the information is required to support the auditor's opinion. When necessary, for example if the reliability or usability of input data from the client's IT systems cannot be guaranteed, the auditor needs to plan additional procedures.[32] The results of GITC testing may impact further audit procedures and the audit strategy. When GITCs in the entity's IT environment are effective, a more efficient audit approach may be chosen using controls-based procedures. If GITCs are not effective, the external auditor can, in some cases, perform additional substantive procedures to compensate. For example, a "can-do/did-do" analysis can be used to assess whether users with certain access rights have made significant changes to systems or performed actions that could lead to audit risks. Where significant deficiencies in the client's internal controls are identified, the auditor must assess the impact of these risks on relevant assertions and substantive audit procedures. It is important for the auditor to determine whether more persuasive audit evidence is required to mitigate the identified material risks of error or fraud in relation to the financial statements.[33] The audit plan should be adjusted accordingly. Where the auditor does not have the necessary expertise to assess risks within IT systems, we already see good examples of auditors engaging an IT auditor.[34]

[27] NV COS 200.13b

[28] Dutch Civil Code - Article 393 paragraph 4 of Book 2

[29] CEAOB - IT Audit Inspection Work Program (published in November 2020)

[30] NV COS 315.25 and 315.26 in conjunction with Annex 5 'overwegingen voor het verwerven van inzicht in informatietechnologie' and Annex 6: 'overwegingen voor het verwerven van inzicht in de general IT controls'.

[31] NV COS 200.13n

[32] NV COS 315.27-28 and NV COS 500.7

[33] NV COS 315 Annex 6: overwegingen voor het verwerven van inzicht in de general IT controls

[34] NV COS 315.25 and 315.26 in conjunction with Annex 5: 'overwegingen voor het verwerven van inzicht in informatietechnologie' and Annex 6: 'overwegingen voor het verwerven van inzicht in de general IT controls'

Bad practice

The external auditor performs insufficient procedures to follow up on the identified risks and findings of the IT auditor. What is also missing is an evaluation of the usability and reliability of the input data for the auditing tool in relation to risks and findings reported by the IT auditor. The auditing tool was used without these considerations being taken into account.

Explanation

Where there is doubt about the usability and reliability of input data — such as in cases of ineffective GITCs in the entity's IT environment — the auditor must perform procedures to resolve this uncertainty before using the tool to obtain audit evidence. Similarly, when an auditor identifies that an ERP system contains numerous user accounts with elevated privileges, procedures must be carried out to address relevant risks before the tool can be used to gather audit evidence. The auditor should determine which changes these accounts have made and the implications for the use of auditing tools.

Good practice

We have observed examples where external auditors use tools to identify (and, where necessary, evaluate) roles, access rights and user and control activities within the client's IT system. This provided an integrated view of expected user activity (for example, superuser accounts or visualisation of 'happy flows') and of unauthorized activities. These insights offered supporting evidence for the overall risk assessment within these systems. Having a complete overview of the risk profile for each user, enabled the efficient planning of further (substantive) audit procedures.

Explanation

By using auditing tools that analyse GITCs (and application controls) comprehensively within the entity's IT environment, auditors can gain better insights into relevant risks of material misstatement arising from these IT systems. A holistic assessment of all relevant IT procedures can therefore provide a solid basis for the audit strategy and the planning of substantive procedures.

When assessing the relevance and reliability of input data, including its accuracy and completeness, it is essential to ensure that the data is reconciled with the underlying administrative records and, where necessary, with original source documents.[35] The data elements used by the external auditor to obtain audit evidence may include both financial and non-financial information. Examples of non-financial data elements include items such as users, general ledger codes, dates, time units or other variables used to support filtering or sorting for the auditors' analyses. These elements are assigned within IT systems based on certain procedures at the audit client and are often relevant for management reporting or aspects of the entity's internal control. The external auditor should consider which procedures are appropriate to validate the reliability and useability of this information, for example through substantive procedures or by testing the effectiveness of relevant application controls and GITCs. To determine which system configurations, application controls and GITCs are relevant, the auditor should assess the information needed for the auditing tool, possibly in consultation with specialists. The considerations for, and evaluation

[35] NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

of, these procedures must be clearly documented in the audit file to demonstrate how the auditor came to the conclusion that the data is reliable and usable for further audit procedures.

Good practice

We have observed that several audit firms provide decision trees to external auditors to support a structured process for making appropriate decisions when evaluating the usability and reliability of information produced by the entity. Part of this process includes reflecting on the effectiveness of GITCs in the entity's IT environment. These decision trees also provide examples of alternative procedures that can reduce risks to an acceptably low level where deficiencies in internal controls have been identified.

Explanation

The external auditor systematically selects suitable procedures to validate the reliability and usability of information. This enables the audit firm to maintain control over the relevance and reliability of outputs from auditing tools that are critical to forming the auditor's opinion.

2.2 Building block 5: determine that relevant and reliable input data is used to obtain sufficient and appropriate audit evidence

The external auditor is responsible for validating the input data processed by an auditing tool. In many cases, it is possible to assess the inherent risks associated with the information provided by the audit client.[36] The auditor can determine in advance which procedures are necessary to validate the relevance and reliability (including the assessment of accuracy and completeness) of information when it is used to obtain audit evidence. Where the auditor finds it challenging to perform this evaluation independently — such as in the case of complex IT systems or integrations — specialists may need to be engaged to carry out certain procedures. These specialists can assist in assessing system architecture, application controls, data flows and interfaces between various IT applications to ensure the accuracy and completeness of the data. Even when specialists are involved, it remains essential that the external auditor understands how the relevance and reliability of the data is safeguarded. This requires providing clear instructions and objectives to the specialists and complying with the relevant requirements of NV COS 620. These requirements include evaluating the independence, skills and competence of the specialist, as well as reviewing applicable professional standards or other requirements. Ultimately, the external auditor retains responsibility for all work performed, even when specialists are engaged.

Good practice

An audit firm's policy states that a third-party software provider supporting data analysis during statutory audits is classified as an engaged expert in line with NV COS 620. The policy specifies which aspects the auditor must assess and document in the audit file. The auditor formulates an assignment, assesses the expert's knowledge, independence and competence, and evaluates the adequacy of the expert's procedures in the audit file.

Explanation

By establishing in policy that relevant safeguards for engaging experts must be evaluated, the audit firm can promote consistency, independence and quality in the use of experts in statutory audits.

[36] NV COS 315 Annex 5 'overwegingen voor het verwerven van inzicht in informatietechnologie'

It is the responsibility of the external auditor to determine the extraction method that provides sufficient assurance regarding the relevance and reliability of the data.[37] Data can be obtained in various ways, each carrying specific risks. The auditor can reduce the risk of errors during data extraction, for example by being present during the extraction process or by performing the extraction themselves via an interface or an API connection with the source systems. In our review, we observed cases where external auditors extracted bank transactions directly from the client's bank using an API connection or an auditing tool. An application programming interface (API) acts as a 'bridge' that enables standardised communication between different types of software. Through an API connection, data can be exchanged and synchronised automatically without manual intervention by the auditor. When the auditor has direct access to the API connection and can extract data from the client's system independently, they can define the parameters for the data to be extracted according to their own requirements. This ensures that the auditor remains in control of extracting complete and relevant information for the audit. Where API connections are controlled by auditors, the appropriate measures must be taken to reduce information security risks to an acceptably low level, as these connections involve different cyber risks compared to traditional file transfer systems. For example, implementing at least TLS 1.2 encryption and ensuring that the connection is established exclusively via HTTPS.

Good practice
Several audit firms have established policies for determining the reliability and usability of information (audit evidence) obtained from auditees. These policies specify which audit procedures should be performed based on the type and source of the data, in accordance with the auditing standards (NV COS 500.A35). The policies also set out when and how these procedures must be documented in the audit file.

Explanation
The origin of the input data used in an auditing tool can influence the procedures the external auditor needs to perform to validate its reliability and usability. Including such procedures in policies applied consistently across the audit firm helps manage potential audit and other risks.

2.3 Building block 6: implement a consistent ETL process and document it

The Extract-Transform-Load (ETL) process helps the auditor manage the reliability and usability of the processed data and safeguard the quality of subsequent audit procedures.[38] The ETL process involves extracting relevant input data from source systems (Extract), transforming it into an appropriate file format and structure (Transform), and loading it into the auditing tool (Load). During this process, the auditor can consciously apply data minimisation by retrieving and processing only the data necessary for the tools – for example, by excluding sensitive personal data where possible. When planning the ETL process, the auditor can predetermine the extent to which the information is relevant for obtaining sufficient and appropriate audit evidence.

[37] NV COS 520.a12

[38] NV COS 500.5, 500.9, 500.A5, 500.A31, NV COS 520.A12

The auditor must confirm that data originates from a relevant and reliable source (such as the right production environment or data warehouse), that the correct extraction query has been used, and that the output is accurate and complete. The extraction process introduces specific risks to the accuracy and completeness of data, which in turn affect its relevance and reliability for obtaining sufficient and appropriate audit evidence. As part of our research, we observed procedures used by auditors to ensure data relevance and reliability during extraction. These include being present during the extraction process (physically or during an online meeting), verifying the query and parameters used, and reconciling the extracted data from IT systems to financial statements or other source documents. Good examples of source verification include reconciliations of both financial- and non-financial elements, like the verification of total amounts from each column with the relevant management reports, administrative systems and financial statements. Or the reconciliation of the total row counts or hash-totals from the exported database with the source system.

The transformation phase begins once the data has been extracted from the client's automated information system. In this phase, the data is prepared for use in an auditing tool. The external auditor assesses whether the transformation tool (for example, a script) or procedures performed (such as manual transformations) safeguard the reliability of the data. This includes verifying that the transfer of data has been accurate and complete and performing certain data quality checks. The transformation phase may involve tasks such as data cleansing, converting data types (for example, from *.XAF to *.csv), filtering and sorting data, performing calculations and other transformations necessary to deliver the data in a usable format for the auditing tool. The auditor must confirm that the transformation process has been properly designed and that relevant control measures are in place to ensure data reliability.

The auditor should additionally verify that the complete dataset has been imported from the transformation-environment into the auditing tool before initiating the analysis. At this stage, validating the accuracy and completeness of the imported data is essential. The auditor can then perform general consistency checks, such as:

- Journal entries that are not balanced;
- Normalisation of numerical values and reconciliation with other administrative records (including correct determination of decimals and FX-rates in financial data);
- Records with empty fields (for example, missing dates, missing names of individuals who posted entries, or journal entries with a value of '0');
- Testing control totals ('hash totals') or other metadata to confirm that all information from the transformation process has been fully loaded into the auditing tool.

** This list reflects common procedures and is not exhaustive. Depending on circumstances, other procedures may be relevant.*

Documenting the ETL process is important for traceability and replicability of the process.[39] Some audit firms grant significant flexibility to engagement teams in how documentation is structured within the audit file. This can lead to inconsistencies and insufficient documentation. Good examples identified in our research show the complete journey of the data – from extraction to loading into the auditing tool. In these examples, the external auditor documents all relevant transformations and configurations that support the integrity of the information used in auditing tools. ETL documentation should provide a clear audit trail of extraction, transformation and loading, with sufficient detail for an experienced auditor who was not involved in the engagement to understand the process and reach the same conclusions. Because auditing tools often process large volumes of data, increasing the complexity of the ETL process, it is critical that documentation captures all relevant characteristics and configurations in a structured and consistent manner.

[39] NV COS 230.8

3. Precondition 3: the auditing tool is implemented in a controlled manner

3.1 Building block 7: develop knowledge and skills alongside innovation

Good practice
Various audit firms record when an engagement team uses an auditing tool for the first time. The team then receives guidance from a technical specialist or a more knowledgeable staff member to maximise effectiveness and consistency and ensure quality.

Explanation
By deploying specialists who support the engagement team with their knowledge and skills, tools can be used more effectively and responsibly, safeguarding quality.

We observe that auditing tools can take over certain straightforward tasks previously performed by staff auditors.[40] This creates capacity for more substantive work by staff auditors — work that requires professional judgement, such as investigating suspicious cash flows. It also provides more scope to discuss dilemmas with the engagement team and the audit client. As a result, the competency profile required of staff auditors is changing and their learning curve is becoming steeper.

To safeguard the qualitative deployment of staff auditors, more training will be required at the start of their careers. This is particularly relevant where staff auditors work with auditing tools that support the preparation of more complex procedures. As auditing tools are increasingly implemented to prepare simple and repetitive audit procedures, audit firms must provide sufficient knowledge and resources to ensure the controlled use of these tools by staff auditors. Audit firms must be well prepared for changing staff responsibilities arising from the implementation of auditing tools.

Good practice
At several audit firms, we saw that an experienced tool user (tool ambassador) or specialist was present during planning meetings. This person advises the engagement team on risks and opportunities relevant to the use of auditing tools in their audit.

Explanation
By involving an experienced tool user in the planning phase of the audit, the experienced user or specialist is able to understand the nuances at the audit client, offering opportunities for controlled use of auditing tools and providing insights into innovative possibilities not previously considered, which are aligned with the audit plan and specific identified risks.

[40] AFM – Trend Monitor 2026 pp. 42-43 (published in November 2025)

Controlled use of auditing tools requires a combination of traditional and new skills.[41] Traditional skills remain important for selecting the appropriate auditing tool for specific procedures. However, correct implementation often requires specific knowledge. Alongside technical knowledge, staff must understand how the engagement team should deal with tool outputs. This applies both to the user of the tool and to the reviewer of the audit procedures for which the tool has been used. Audit firms must ensure that their staff possess the skills needed to evaluate whether tool outputs provide sufficient and appropriate audit evidence.

Good practice

Several audit firms have made video materials available for frequently used auditing tools. These videos provide a step-by-step explanation of the tool's functionality with practical examples. For inexperienced staff, it is recommended to complete an e-learning course before using the tool in practice. The e-learning incorporates the video material, presenting the relevant functionality of the tool in an interactive way to ensure controlled and responsible use.

Explanation

By training staff before they use auditing tools, the audit firm ensures controlled and responsible tool-implementation in statutory audits. Tool-specific training that explains relevant functionality promotes correct and consistent use of the tool. In addition, demo videos can be helpful for users who have doubts about certain functionalities of auditing tools, as the visual presentation can provide practical support during the execution of their work.

Because external auditors bear undivided responsibility, they must also understand the effect of the implementation of auditing tools. Accordingly, for complex auditing tools or specific procedures, additional expertise may be required from other disciplines (such as statistics or data science). When this knowledge is not available within the audit firm internally, we have seen good examples of firms hiring external expertise or recruiting staff with backgrounds other than accountancy.

We regard knowledge sharing as a critical success factor. Experiences with the use of auditing tools should be shared systematically and embedded subsequently within the organisation. This includes both technical knowledge and insights into the effect of auditing tools on statutory audits. During our research, we have seen that collaboration within (a network of) audit firms can promote knowledge sharing — for example, by sharing innovative applications that have added value in specific client segments, or by sharing specific experiences regarding how auditing tools have contributed to achieving audit objectives and the risks identified or resolved in the process. We also observed good examples where approaches to interpreting and finalising results generated by auditing tools were shared.

[41] AFM – State of the Auditing and Reporting Industry pp. 13-14 (published in November 2025)

Good practice

We have seen that several audit firms form networks of tool specialists consisting of the more experienced tool users. Within these networks, specialists exchange knowledge and share good and bad experiences. They use their collective knowledge and experience to create sets of practical guidelines within the audit firm, to be shared with all tool users. These guidelines provide a basis for auditors that enables them to use auditing tools efficiently in a controlled manner in order to obtain the required results. The audit firms have established communication channels between regular tool users and the networks of specialists, where specialists have a supporting role for individual users in case of questions about the auditing tool.

Explanation

A network of experienced tool users can effectively facilitate knowledge sharing about tool use. When these users work in different locations or client segments, the specialist network can stimulate knowledge transfer within the audit firm. This in turn enables effective tool-implementation in statutory audits.

3.2 Building block 8: integrate the implementation of auditing tools into the overall audit strategy and audit plan

Statutory audits comprise several phases. During the planning phase and risk assessment phase, it is important to determine how auditing tools will be deployed. Based on identified inherent- and internal control risks at the audit client, the external auditor determines which audit objectives are relevant. The auditor then selects a tool capable of achieving those objectives. The identified risks and corresponding audit objectives are decisive; auditing tools are merely a means to achieve these objectives. The conditions for using auditing tools as part of risk assessment procedures may differ from those where audit evidence will be obtained. We already observe good practices at audit firms where the audit plan states which tools are used, for which procedures, and the extent to which audit evidence is obtained from the tool. When policy prescribes the conditions the auditor must assess when using auditing tools, the auditor can already incorporate these activities in the planning phase. This prevents ad hoc decisions during the execution phase of the audit and supports the efficient and controlled implementation of the auditing tool.

Good practice

We have observed that several audit firms ensure that the external auditor clearly documents the relevance of auditing tools in the audit plan when they are used for auditing material financial statement line items. The plan specifies the impact that the (potential) outputs of the auditing tool have in relation to all other procedures addressing the same audit objectives. For exceptions and deviations, the auditor refers to the audit plan to review the predetermined impact on other audit procedures, after which the risk assessment for these procedures is adjusted where necessary.

Explanation

By documenting the relevance and impact of auditing tools in the audit plan, the auditor can use this information to align procedures effectively. This promotes consistent application of auditing tools and enables the auditor to determine quickly and in a well-founded manner which additional procedures are required in case of exceptions or deviations. Defining the role of auditing tools in advance therefore contributes to their controlled and effective use in the statutory audit.

It can be prudent to implement appropriate controls when tools are first introduced within an audit firm. With innovative tools, it is not always clear in advance whether their use will yield outcomes that provide sufficient and appropriate audit evidence, particularly where the audit firm has not previously applied the techniques for specific audit procedures. We already observe good practice where audit firms first trial new tooling in a test environment, using fictitious (but representative) data to form a realistic expectation of the tool's potential for particular audit procedures. We also see examples of audit firms deploying auditing tools in parallel with traditional audit procedures, then comparing the effect on efficiency and audit quality before broader implementation. By first establishing how auditing tools affect the quality of audit procedures before rolling them out across the organisation, the audit firm can promote high-quality and controlled use in statutory audits.

3.3 Building block 9: follow up on the outcomes of auditing tools

Where auditing tools generate risk indicators, exceptions and deviations from predefined criteria, the external auditor must follow up. Clear guidance and illustrative examples in policy help tool users to make appropriate judgements in response to tool outputs. This ensures that signals from auditing tools are not only identified but also lead to consistent and well-substantiated follow-up actions within the statutory audit. From our review, we indicate that there is room for improvement on this topic.

Bad practice

In several audit firms, we have seen auditors using auditing tools to analyse goods movements, including a reconciliation to bank transactions. The tools' objective was to obtain sufficient and appropriate audit evidence to confirm the existence and cut-off of revenue. The tool-outcomes indicated significant fluctuations and outliers which, according to the predetermined threshold, should have been investigated further. The auditor did not follow up on all material outliers by performing substantive procedures to understand their nature and overall impact on the audit. Nor did the auditor reassess the risk for financial statement items affected by these outliers, or whether they posed a risk of a material misstatement when aggregated with outliers of a similar nature. While some outliers were addressed by the engagement team in a test sheet, the team did not review external delivery notes to verify whether goods were actually shipped, and costs recorded in accordance with accounting standards.

Good practice

An audit firm used an auditing tool for a substantive analytical procedure on the 'costs' financial statement line item during the statutory audit. The analysis revealed differences compared to the expectation. The engagement team reconciled relevant data elements with external sources to support these findings and evaluated whether their expectations were sufficiently precise to obtain sufficient and appropriate audit evidence. This evaluation is clearly documented in the audit file.

Explanation

The auditor has established an expectation and uses the analyses generated by the tool to assess this expectation against predefined criteria. Where deviations from the initial expectation or benchmark are identified, it is essential that the external auditor follows up on these relevant deviations by obtaining insight into their nature and significance before using the tool's outputs into risk evaluations or as audit evidence. The auditor may apply professional judgement to determine which evidence provides the most reliable basis for this evaluation. We observed good practices where auditors utilised independent (external) sources of information when available. We also noted examples where auditors reassessed their risk evaluation based on the tool's outputs and subsequently adjusted the audit plan. This approach ensures that the procedures for which auditing tools are deployed result in sufficient and appropriate audit evidence to support the external auditor's opinion.

Use of auditing tools may lead to findings; where such findings are material, they may need to be communicated to those charged with governance in line with NV COS 450.[42] When auditing tools are used to test internal controls, certain tools — by how they present outcomes — can provide sharp insight into deficiencies identified with the procedures performed. For example, a dashboard that displays all control outcomes, enabling the auditor to assess visually which controls were applied at what time and whether this aligns with the organisation's policy. In data-focused procedures, some tools provide clear visualisations of analysis outcomes, linked to materiality or other predefined criteria for assessing the results. This helps the external auditor to evaluate deviations and determine whether these result in findings that must be communicated to management or those charged with governance at the audit client.

The way auditing tools present outcomes can also add value to the audit engagement. We have seen presentation techniques that make information clearer than traditional techniques would, for example through a dashboard with a "drill-down" option that allows navigation from audit findings to relevant details to support the auditor's narrative. It is therefore advisable that audit firms assess how auditing tools can facilitate external auditors in fulfilling their responsibilities under NV COS 450.

NV COS 230[43] and NV COS 500 require the external auditor to prepare audit documentation that is sufficient and appropriate to support the auditor's report. Depending on the tool used and the audit procedures for which it is deployed, procedures, data sources, processing steps, results and conclusions must be recorded adequately. We observed good practices where documentation clearly set out how analytical procedures were performed, how source data was validated, and how tool outputs were linked to audit conclusions. We also saw examples where replicability of tool outputs was ensured by recording parameters, assumptions and the tool configuration used (including versioning). This is particularly important when auditing tools are used to obtain audit evidence over relevant assertions or for significant risks. By ensuring clear documentation and replicability, the auditor can demonstrate that auditing tools have been applied consistently and in a controlled manner.

[42] NV COS 450 paragraph 8
[43] NV COS 230 paragraph 5

Use and scope of auditing tools – observations from the exploratory study

Observations on tool deployment for specific audit activities: During our research, we explored the use of auditing tools within various audit activities[44]:

Data analysis: Most tools support data analysis for risk assessments and substantive procedures (NV COS 315/330/520), efficiently processing multiple data sources.

Visualisation: Audit firms use dashboarding tools to present their results visually, including to management or supervisory boards of the audit client (NV COS 260).

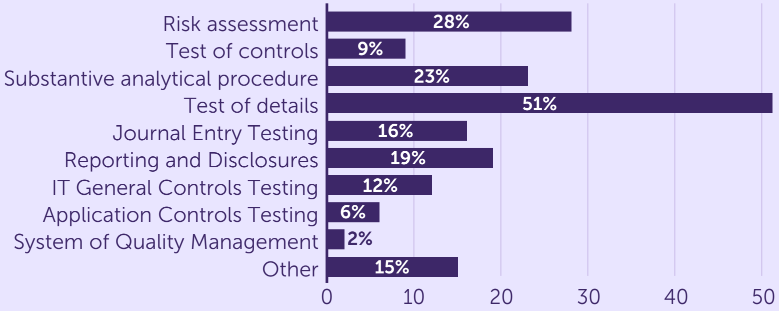
Client acceptance: Tools are used for client and engagement acceptance and continuation, as a basis for initial analysis, further investigation or documentation of work performed.

Substantive audit procedures: Tools support procedures at the level of relevant assertions or significant risks, such as:

- Detection of unusual transactions based on parameters.
- Testing internal controls (GITCs/application controls) over entire populations within the entity's IT environment.
- Document analysis, extracting data elements from unstructured sources (documents, images etc.) and presenting them in a structured way, including linking to source locations. For example, making extracted information from a PDF file visible when selecting the relevant data element in the work programme.

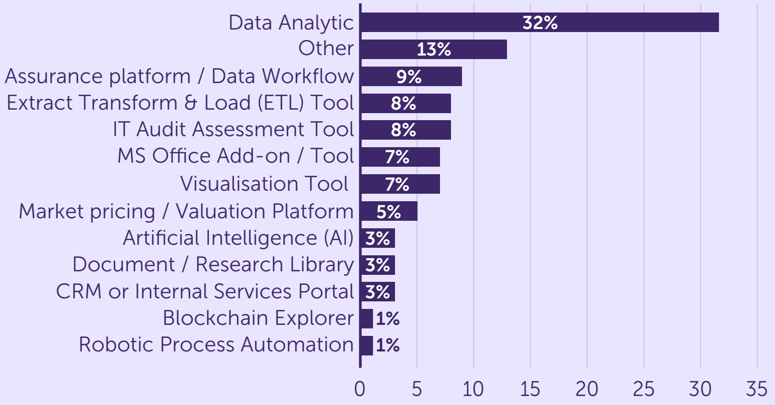
Results of data requests sent to PIE audit firms: From our data request to the six PIE audit firms, we understand that auditing tools are used in every phase of the audit. This supports the findings from our exploratory research. The following graph shows how often auditing tools are used in a particular audit area across the six PIE audit firms. An auditing tool can be used in multiple audit areas, which is why the percentages do not total to 100%.

Use of audit tooling in each audit area (average)



The data request also provided insight into the types of auditing tools available to staff. These include tools used for audit activities (e.g. data analytic tools or visualisation tools), as well as tools that support the organisation (e.g. firm-wide CRM systems). The 12 building blocks in this report are relevant to auditing tools supporting the entire audit firm. The following graph shows the average percentage across PIE audit firms for each type of auditing tool available to staff.

Type of audit tooling available to staff (average)



[44] This list is not exhaustive. These activities were the most frequently identified during our research.

4. Precondition 4: the (Gen)AI tool is used in a controlled manner

4.1 Building block 10: the (Gen)AI tool is deployed safely and in a controlled manner

The technology underlying (Gen)AI introduces new risks for information security. Whereas traditional tools operate with fixed functions and controlled algorithms, (Gen)AI technology is dynamic and less transparent. This makes it more difficult for the auditor to determine what happens to the data entered into the system – for example, whether it is used as training data or transmitted to external systems or third parties.[45] As a result, the risk of data breaches when using (Gen)AI technology is higher than with traditional technology. A breach could lead to the unintended disclosure of confidential client information (such as price-sensitive data) or violations of privacy legislation,[46] as well as violations of confidentiality obligations under the Audit Firms Supervision Act ("Wta") and the Code of Conduct and Professional Rules for Auditors ("VGBA"). Information security risks are therefore particularly relevant when implementing (Gen)AI tools in the audit-firm. It is essential that audit firms establish clear agreements on data-governance and (expected) security measures. These agreements should be made with both software providers and audit clients, as well as with third parties for whom the audit firm processes data, in order to mitigate risks effectively.

When using (Gen)AI tools, it is essential – as with other auditing tools – to establish policies covering key aspects such as data minimisation, anonymisation and pseudonymisation, and data retention periods, to safeguard the confidentiality of client data. This applies both to data processed within the firm's own environment and data handled by third parties. In addition, clear agreements should be made with stakeholders regarding processed data that may be used to train AI-models. Both software suppliers and audit clients should be involved in this agreement. Important to note: The same information security requirements for traditional auditing tools apply to (Gen)AI tools as well. A robust information security framework, as discussed in section 2.1, should therefore also cover (Gen)AI applications. Importantly, these requirements also apply to internally developed tools that use (Gen)AI, such as custom Python scripts that are connected to a Large Language Model (LLM).

Good practice

Several audit firms use a (Gen)AI tool that can retrieve information from internal systems, including manuals. Control measures are implemented – through tool configuration – to make confidential data and files inaccessible to the (Gen)AI tool. Policy is shared with all staff for safe processing and storage of confidential information in the correct locations. This prevents the (Gen)AI tool from accessing and processing the information.

Explanation

We encourage audit firms to configure (Gen)AI tools carefully to manage associated risks. We also recognise the importance of policy addressing data confidentiality and information security. With (Gen)AI, this is especially relevant, as the technology can generate output based on all available data. If information is not stored correctly and securely, it may be included in the output and accessed by unauthorised users.

[45] Autoriteit Persoonsgegevens ("AP") - The AP's vision on generative AI (published in May 2025)

[46] AP - Caution: use of AI chatbot may lead to data breaches (published in August 2024)

Audit firms must assess the reliability of outcomes produced by AI tools, especially when these outcomes are being used as audit evidence by auditors. Since (Gen)AI technology operates on probabilistic models rather than fixed rules, its outputs may not always be consistently accurate. There are various methods available to evaluate the precision of these tools. One approach involves pre-defining a benchmark outcome (a "target position") and regularly testing it against specific tasks. This includes checking the results generated from approved prompts in a prompt library after model updates to ensure that they still align with the expected benchmark. Another way to monitor accuracy is by tracking model-specific performance indicators, such as the F1 score, precision and recall, which help measure the model's quality and consistency over time.[47]

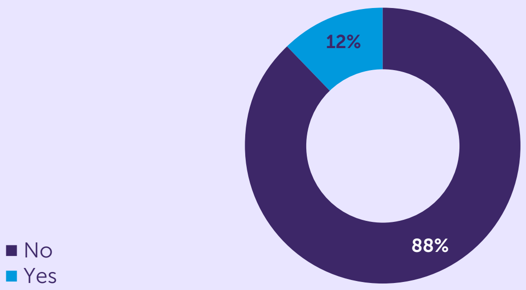
New skills and specific knowledge are needed for controlled implementation of (Gen)AI tools (and possibly also for agentic-AI in the future). The tasks of staff auditors may change because (Gen) AI tools may take over parts of the audit process for which junior professionals previously had responsibility. New joiners may therefore be more likely to perform more complex work compared to previous generations of auditors, for which they require more in-depth skills and knowledge (for example of audit methodology or advanced auditing techniques). If audit firms do not align the knowledge and skills of their new joiners to fill the gaps for their newly required expertise, this may affect the firm's overall audit quality. Therefore, more advanced tools with a broader impact in the audit practice requires a re-evaluation of the way in which novice accountants are trained. We expect audit firms to assess this potential reality and prepare for it where they can.

[47] Berghout, E. et al. - Advanced Digital Auditing p. 31-32 (published in October 2022)

Auditing tools that use (Gen)AI technology

In response to a data request from the AFM, PIE audit firms reported that 12% of the auditing tools they plan to use in 2025 incorporate AI or generative AI. These tools may either be fully powered by AI technology or include AI as one of their components. Our research indicates that the use of (Gen)AI in statutory audit practices is expected to grow significantly in the coming years. This insight is based on discussions with non-PIE audit firms and PIE audit firms.

AI embedded in auditing tools



AFM expectations

(Gen)AI requires a new way of working for current and future staff. Outcomes from (Gen)AI tools must be critically assessed. Staff must be trained in this new way of working and have the right knowledge to manage output variability and other risks associated with this technology.

We expect audit firms to ask themselves: Which procedures receive less human attention due to (Gen)AI tools? How do these changing procedures affect auditors' skills in the short, medium and long term? What knowledge and skills must be imparted to staff to manage potential risks and safeguard statutory audit quality?

4.2 Building block 11: the outcomes from the (Gen)AI tool are verifiable or replicable

The output of (Gen)AI tools cannot always be precisely reproduced, but outcomes must be verifiable or replicable. Because (Gen)AI tools are stochastic in nature, their output may vary. In addition, a neural network in an LLM consists of an extremely large number of parameters, making it non-transparent how an outcome is generated. As a result, (Gen)AI tools effectively function as a 'black box', especially when the organisation does not control all parameters that lead to the output.

When the external auditor uses output from (Gen)AI tools as audit evidence, it is essential that this output is verified. This can be achieved, for example, by having the tool reference external sources or source documents, ensuring traceability of the tool's outcomes. If exact verification is not feasible, audit firms may opt to make the results replicable. For instance, when a machine-learning model is applied to recalculate an estimated line-item in the financial statements based on specific ledger elements, combined with online data sources. If the (Gen)AI-model is a well-tested version, and the overall reliability of its outcomes has been validated within the organisation's change management process, the results could be reproduced within an acceptable margin of error.

Audit file documentation requirements when using (Gen)AI tools are equivalent to those for conventional auditing tools. Documentation must be sufficiently detailed to enable an experienced auditor to understand the nature, timing, extent, results and conclusions of the work performed.

When using any (Gen)AI tool, it is important to have insight into the relevant choices made by the (Gen)AI tools during the process that led to the output. This enables the external auditor, as well as a potential independent third party or quality reviewer, to follow these choices and verify the outcomes. It also ensures that the necessary information is available to repeat the work if required. This is no different from when a staff member or expert documents procedures in a preparatory role. A reviewer cannot see inside the preparer's mind but can follow the procedures if documented correctly.

Bad practice
The (Gen)AI auditing tool is a 'black box'. Outcomes are provided without visible reference to specific source documentation.

Explanation
Outcomes are not explainable, verifiable or replicable. There is a risk of hallucinations and biases, preventing the auditor from taking responsibility.

Good practice
The tool shows 'snips' from source documentation alongside the information sought by the auditor.

Explanation
This enables the tool to help the auditor verify outcomes and makes the process replicable. The auditor can critically assess AI output and independently determine when additional human verification is needed.

A central prompt library for (Gen)AI tools is an effective way to ensure consistent use across the organisation. By defining and sharing standard prompts, the quality of input in (Gen)AI tools can be better managed, creating uniformity in their application during statutory audits. Approved prompts help reduce the risk of variable or undesirable outcomes, particularly when tools are used for specific purposes. In addition, the library serves as a knowledge platform, making 'best practices' easily accessible and improving efficiency in the use of (Gen)AI tools. Audit firms participating in our research indicate that a prompt library can strengthen quality control, consistency and knowledge sharing within the organisation.

4.3 Building block 12: the external auditor is ultimately responsible for the outcomes from the (Gen)AI tool

(Gen)AI may facilitate the work but cannot replace professional judgment. The external auditor is responsible for assessing, weighing and validating (Gen)AI outcomes before using them. Our review shows that it is not always clear or visible where and how (Gen)AI has been applied in the audit process. It is important that the external auditor knows where (Gen)AI has been used, so that appropriate responsibility can be taken during the review process. This is particularly relevant for activities where professional judgement plays a significant role.

Good practice
In our research, we noted that auditors use (Gen)AI tools as a sounding board in the fraud risk assessment for a specific sector or typology based on concrete examples. They first make their own assessment and then use the (Gen)AI tool to soundboard their work and remove potential blind spots.

Explanation
We recognise the importance of the professional judgement of the auditor and agree that this cannot be replaced by (Gen) AI tools. (Gen)AI tools can have a supporting role in the work of the accountant but cannot replace the auditor and their ultimate responsibility for the audit.

Outputs from (Gen)AI tools can appear convincing due to the anthropomorphic characteristics of some tools. These tools mimic human traits, creating a risk that users may place undue trust in the outputs and review them less critically.[48] The persuasive nature of (Gen)AI outputs, driven by their structure or presentation, can lead to a 'halo effect'. When (Gen)AI tools present outcomes in a highly convincing manner, this may cause auditors to overlook potential hallucinations, biases or inaccuracies in responses. This increases the risk of overreliance on (Gen)AI tools.[49]

There are control measures that can mitigate the risk of overreliance on (Gen)AI tools. We have observed good practices where external auditors follow mandatory validation steps within a fixed workflow. In such processes, each step can only be completed once the auditor has confirmed that the output has been reviewed and, where necessary, supported by underlying audit evidence.

Our research found that nearly all audit firms use (Gen)AI to some extent. For example, they use chatbots to summarise meeting minutes, as a sounding board for risk assessments, or to answer simple methodological questions. Audit firms are also experimenting with more advanced, audit-specific tools, such as (Gen)AI agents that can autonomously prepare and, to some extent, perform audit procedures.

[48] NBA - VGBA section 2.4

[49] DNB and AFM – The impact of AI on the financial sector and supervision (Chapter 1.4) (published in April 2024) & AFM – Controlling model risk is crucial for asset managers (published in December 2025)

Bad practice

The (Gen)AI tool presents a conclusion in a highly convincing manner, leading the auditor to immediately include it in the audit file. The tool does not provide clarity on how the output was generated, which data was used, or how reliability was ensured.

Explanation

Because the tool presents outputs in a highly persuasive way, the user may adopt them without critical assessment. It is essential that the user understands that outputs from (Gen)AI tools are stochastic in nature and that the auditor remains ultimately responsible for obtaining sufficient and appropriate audit evidence, including traceability and verifiability of conclusions.

Good practice

The (Gen)AI tool enforces that the external auditor must validate the outputs before proceeding to the next step within the workflow of the tool. Reliability scores for the outputs are displayed, along with an alert reminding the user of the risks associated with (Gen)AI and the level of reliance that should be placed on the outcomes.

Explanation

The tool ensures that the user pauses to validate its outputs, reducing the risk of overreliance by the external auditor. By informing the user about risks and reliability during use, the tool encourages verification and supports traceable conclusions.

Culture within audit firms has a significant influence on how staff use (Gen)AI tools. It is important that employees are aware of the risks associated with this technology. At the same time, psychological safety can encourage adopting innovative auditing tools. Striking the right balance is essential for sustainable innovation.