TIAS

SCHOOL FOR
BUSINESS AND SOCIETY

Forty Years at the Digital Frontline

From Mainframes to Artificial Intelligence: Reflections on a Career in IT Auditing

Professor Rob Fijneman

When I entered the profession in the mid-1980s, few people could have imagined that information technology would become the nervous system of every organization. What started as a specialist discipline supporting financial audits has evolved into a profession focused on topics like digital trust, resilience, cybersecurity, governance and, increasingly, artificial intelligence.

Looking back over forty years, I realize that my career has coincided with five major transformations:

- from mainframes to networks,
- from controls to governance,
- from financial assurance to digital trust,
- from periodic audits to continuous assurance, and
- from traditional information systems to artificial intelligence.

The interesting thing about information technology is that most of the time businesses have a mixture of solutions in place meaning that both the 'old' and 'new' situation can be there at the same time. Furthermore, I do not intend to offer a complete history of IT auditing. This is a personal perspective, shaped by four decades of client work, professional practice and academic engagement.

My journey has not ended. I intend to remain active in IT and digital auditing, in both business and academia. Even so, this is a fitting moment to reflect on how the profession developed, what remained constant and what is expected to come next.

Auditing the Computer Room

In the 1980s, IT auditing was primarily focused on large, centralized environments. We audited physical access controls, batch jobs, system changes and recovery procedures. Evidence was collected manually, often through printed reports and extensive documentation.

The questions were relatively straightforward:

- Can management rely on computerized processing?
- Are controls functioning properly?
- Is financial data reliable?

Although highly technical by the standards of the time, this work marked the beginning of a far-reaching transformation.

"While introducing mainframe computers in those days the relevance of validating the reliability and security of data and the processing thereof already came alive."

The foundations of today's profession were already being laid.

As computing moved from isolated processing to increasingly interconnected systems, technology became more capable and more difficult to understand. That growing complexity created the need for specialists who could assess not only whether systems processed financial data correctly, but also whether the broader digital environment remained controllable and trustworthy. The thinking in terms of auditing both the so-called general IT controls and the relevant application controls was introduced.

The introduction of early computer-crime legislation in the 1980s reflected a broader realization: organizations needed mechanisms to account for the reliability and continuity of automated data processing. In the decades that followed, cyber, privacy and resilience regulation expanded substantially as business and society became more dependent on digital technology.

The Emergence of IT Auditing as a Profession

As technology spread throughout organizations, it became clear that traditional financial and operational auditing alone was insufficient.

The Netherlands became one of the pioneers in establishing dedicated IT audit education and professional standards.

"The first IT audits were performed in the large mainframe environments of international companies, triggering the more specialized IT audit profession."

The profession matured rapidly. In the mid-1980s, several Dutch universities developed dedicated IT audit curricula. Around 1988, these programs began alongside the establishment of NOREA, creating a professional route that combined advanced education, practical experience, registration, standards and methodology. IT auditing was becoming a recognized discipline at the intersection of technology, auditing and governance.

This period convinced me that education would become one of the profession's most important pillars. As technology developed, the curricula expanded to cover the full technology lifecycle. That need for continuous learning is one reason I have remained deeply involved in academic programs throughout my career.

From Controls to Governance

The 1990s and early 2000s introduced enterprise systems, global networks and internet-enabled business models. Technology was no longer confined to the IT department. Boards increasingly depended upon technology to drive business performance.

A fundamental realization emerged: **"Technology was becoming the business."**

This changed the focus of audits. We moved from controls around individual systems to governance across entire technology landscapes. The lines of defence also became more explicit: management owned the quality of processes and digital solutions, risk and compliance functions

shaped and monitored controls, and internal and external auditors assessed those controls and provided assurance.

As I later wrote: **"It is time for boards and managers to seek certainties on the digital highway."**

Technology governance became a board responsibility. And the IT auditor increasingly became a translator between technology, risk and business strategy.

In practice, governance has always had two inseparable dimensions. The first is control: are digital risks understood and managed against clear standards? The second is strategic: are the organization's technology choices, investments and capabilities aligned with its objectives? IT auditing adds the most value when it addresses both questions rather than limiting itself to technical compliance.

The Rise of Digital Trust

The internet era fundamentally changed the profession. Cybersecurity emerged. Privacy became critical. Complex outsourcing chains developed. Algorithms started influencing decisions. The questions became broader and more societal.

"Issues of digital integrity, honesty, fairness and security have taken on social significance."

For the first time, IT auditing was no longer purely about organizational risks. It was increasingly about public trust, because digital solutions were shaping citizens' privacy, opportunities and treatment, not merely an organization's internal efficiency. This development ultimately shaped much of my later work.

"IT auditing concerns the independent assessment of the quality of information technology, including infrastructure, applications, processes, data and governance."

The scope had expanded dramatically. We were no longer auditing systems. We were helping society trust digital systems.

That broader mandate also changed the meaning of quality. Reliability, availability and security remained essential, but they were joined by privacy, fairness, honesty, effectiveness, efficiency and resilience. The profession had to move beyond confirming that technology worked as designed and ask whether the design itself was responsible, proportionate and worthy of trust.

Throughout my career, I have increasingly viewed IT auditing as helping organizations and society find quality on the digital highway. As digital systems became more interconnected and influential, stakeholders sought assurance not only about reliability and security, but also about integrity, fairness, resilience and accountability.

The Assurance Continuum

Over time, the profession developed a broader toolbox for answering different questions. Service-organization assurance supports confidence in outsourced processing. Broader non-financial

assurance can address security, privacy, confidentiality and other quality attributes. Agreed-upon procedures provide factual findings when users wish to form their own conclusions.

These forms of reporting sit on an assurance continuum. The right answer is not always the report that promises the most assurance, but the engagement that best matches the management question, the criteria, the intended users and the maturity of the controls. Scope and language matter because assurance creates value only when stakeholders understand what has, and has not, been assessed.

Securing the Quality of Digital Applications

One theme has continuously returned throughout my publications and client work. How can organizations demonstrate that their digital solutions are trustworthy? In a world of accelerating change, governance became essential.

One quote captures this challenge well:
"The responsibility for the quality of digital solutions is taking on new dimensions as developments move at lightning speed and everyone is linked to everyone."

Over time, I became increasingly convinced that quality cannot be inspected into systems afterwards. It must be designed into them.

"It is more effective and efficient to adjust the control during implementation of digital solutions than to repair it afterwards."

This principle, now often labelled **Secure by Design**, applies equally to cybersecurity, privacy and artificial intelligence.

Secure by Design also clarifies accountability across the technology chain. Suppliers should build safer solutions and transparent controls into their products, while buyers should make quality requirements explicit and challenge providers before implementation. Management cannot accept a black box merely because the underlying technology is complex. Responsibility for deployment remains with the organization.

From Annual Audits to Continuous Assurance

Cloud computing, DevSecOps and digital platforms introduced a new challenge. Traditional annual auditing cycles struggled to keep pace with systems that changed every day.

This naturally led towards continuous assurance. Several years ago, I wrote:

"If more and more continuous monitoring is provided, the IT auditor can move toward a form of continuous auditing, providing assurances at any time."

I still believe that this represents one of the most important developments for our profession.The future is not less assurance. It is more timely assurance.

Continuous monitoring creates the bridge. When controls are observed on an ongoing basis and exceptions are captured reliably, the auditor can use more current evidence and focus attention on change, anomalies and emerging risk. This does not eliminate periodic professional judgement. It makes assurance more responsive to the speed at which digital environments evolve.

Years ago, I suggested that continuous monitoring could ultimately enable an “anytime, anyplace, anywhere” form of auditing. We are not fully there yet, but the direction remains clear: assurance must become more timely, more integrated and more responsive to change.

Artificial Intelligence: The Next Chapter

Since 2023, artificial intelligence has dominated technology discussions. The opportunities are enormous. The risks are equally significant. I have often warned that governance is struggling to keep pace with innovation.

"AI governance is not meeting the AI adoption."

At the same time:

"The potential of AI is huge, the risks also, but by using sound business and governance principles it can be a fascinating year."

The profession now has a new responsibility called AI assurance.

Organizations need confidence regarding:

- Explainability
- Accountability
- Data quality
- Ethical use
- Regulatory compliance

As I recently wrote: **"AI assurance is emerging as the cornerstone of responsible AI."**

Yet the most important lesson from forty years remains unchanged:

"Technology can scale decisions, but accountability remains human."

AI therefore reinforces the need for multidisciplinary assurance. IT auditors must work with data scientists, legal specialists, ethicists, cybersecurity professionals and business owners to understand the system, its data, its intended use and its impact. The auditor’s role is not to replace those disciplines, but to connect them through independent challenge, evidence and a clear line of accountability.

The Next Evolution: Integrated IT Assurance

Today, we are approaching what I believe is the next major phase of the profession.

Integrated assurance.

Not separate reports on cybersecurity, continuity, privacy or AI. But a complete perspective on digital trust. As I noted in my Outlook for 2026:

"The next step is to offer integrated assurance across the organization's entire technology lifecycle."

This includes as also well defined in the Integrated Digital Reporting Standard initiated by NOREA:

- Digital innovation
- Data and AI
- Cybersecurity
- Third-party management
- Privacy
- Resilience.

The opportunity for the profession is significant. Stakeholders now seek assurance from different angles: financial auditors need reliable technology controls; boards need insight into strategy and governance; CIOs need assurance over projects, cyber, privacy, AI and third parties; and regulators expect evidence of compliance. Integrated IT assurance can connect those perspectives rather than treating them as isolated requests.

"IT assurance should raise the bar and play a pivotal role for stakeholders."

A Common Body of Knowledge, Built Together

The expansion of our mandate requires more than individual technical expertise. IT auditors need a common body of knowledge that connects audit principles with technology, business processes, governance and emerging regulation.

The Dutch model demonstrates the value of combining rigorous postgraduate education with practical experience and professional registration. International certifications and communities add a wider perspective. These approaches should not compete; they should reinforce one another.

No single discipline can cover today's digital landscape alone. IT auditors must work with financial auditors, cybersecurity specialists, data scientists, privacy professionals, engineers, lawyers and ethicists. Our distinctive contribution is to connect their expertise through an independent, evidence-based assurance perspective.

This collaboration should extend beyond firms, universities and national professional bodies. Shared learning outcomes, adaptable curricula and stronger international cooperation can help the profession build both capacity and consistency. A global challenge requires a profession that learns globally while remaining sensitive to local context.

"The profession will be strongest when deep expertise is combined with a common language of trust."

That common language must also be accessible to boards and management. IT auditors can improve their impact by starting with the decision or uncertainty that matters to stakeholders, using simpler language and then selecting the standards, methods and evidence that fit the question. Technical correctness remains necessary, but it is no longer sufficient.

IT auditors must therefore become better translators. Our challenge is not merely to understand technology, but to explain its risks, quality and limitations in language that boards, regulators and citizens can understand.

Lessons After Forty Years

People often ask what has changed most during my career. My answer surprises them.

Technology has changed completely. The principles have not.

Throughout four decades, six lessons remained constant:

- Technology changes faster than principles.
- Risk never disappears; it migrates.
- Governance matters more than technology.
- Trust remains the ultimate objective.
- Education is critical.
- Human judgment remains irreplaceable.

One lesson I learned is that stakeholders rarely ask for technical perfection; they ask for clarity. What uncertainty matters, and what decision must be taken? The future impact of IT auditing depends not only on sound methodology, but also on our ability to frame assurance around the questions that management and society actually care about.

The greatest IT auditors I have met were never defined solely by their technical skills. They combined expertise with curiosity, integrity, independence and courage.

Looking Ahead

The future will bring autonomous monitoring, AI-enabled audits, quantum computing, new regulations and increasingly complex digital ecosystems. These developments will change our tools and extend our reach, but they must not remove the human in the loop. Professional scepticism, ethical judgement and accountability cannot be delegated to an algorithm.

The profession should resist two extremes: treating every new technology as an entirely new assurance problem, or forcing emerging risks into old checklists. The enduring principles of independence, evidence, professional scepticism and accountability provide continuity. Our methods, skills and forms of reporting must continue to evolve.

But I believe the mission remains unchanged.

"The future of IT auditing will not be determined by technology alone. It will be determined by our ability to ensure that innovation remains trustworthy, transparent and accountable."

After forty years, I remain convinced that trust is the most valuable asset on the digital highway.

Source note

This article incorporates and develops ideas from the author's earlier publications and presentations, including "IT auditing, a strong foundation for the future" (2023), "Securing the quality of digital applications: challenges for the IT auditor" (2023), "Exporting the Dutch IT auditing profession, the common body of knowledge approach" (2024), "The future of IT auditing" (2024), and contributions to Advanced Digital Auditing: Auditing Advanced Information Systems and Technologies in a Modern Digital World (2022).