Fifty years of IT auditing

A journey through the past, present and future

For the Dutch version of this article, please scan the QR code.

Peter van Toledo RE, MA
is a director at KPMG IT Assurance & Advisory.

Herman van Gils RE, MA
worked with KPMG for forty years.

About fifty years ago, IT audit made its appearance in auditing, which was also the reason for exchanging professional technical developments in a new journal called *Compact*. Of course, a lot has changed since then, but certain activities – albeit in a new look – have not changed all that much. As has been said so often in those fifty years, quite a lot is going to change, not only because the approach to auditing itself is constantly changing, but also because IT and audit techniques are constantly evolving, such as the emerging AI. What does this mean for the profession? Enough reason to take you on a fifty-year journey back in time and twenty years ahead in the development of IT auditing.

IT STARTED WITH THE SUBSTANTIVE AUDIT

The history of IT audit (then called EDP audit [EDP: Electronic Data Processing]) begins some fifty years ago, hence the 50th anniversary of *Compact*. IT audit is immediately entirely dominated by auditing, because IT audit is developed by major accounting firms. At that time, the approach to auditing was still almost entirely centered on substantive[1] auditing.

The quality of the audited company's IT is not relevant at all, because the auditor takes extensive samples and performs a lot of detailed checking. System-oriented auditing is not yet an option. The samples obviously have to be mathematically justified and determining the sample and the items to be considered still turns out to be quite difficult in connection with the various types of sampling routines and choices such as stratification, negative or no negative items, periods, sorting and, of course, the random nature, et cetera. This is where the IT auditor first appears on the scene. The IT auditor is then primarily a programmer, because with some theoretical sampling knowledge and knowledge of the client's files, the IT auditor can provide excellent support. The IT auditor can now provide advance insight into the items in the file, allowing the selection by the auditor to be more effective and efficient. However, good knowledge of and experience with programming is important, because standard audit software does not yet exist. Often programming is still done in languages such as COBOL (Common Business Oriented Language, a language that is conceptually almost incomparable with today's programming languages), at that time *the* standard software for administrative applications. In addition, you had to be good at (re)typing, because each program line had to go individually into a punch card. The financial auditor/financial IT auditor does not yet have a computer, so the processing has to be done on the client's computer or, in exceptional cases, on the computer of a befriended relation, for example an insurance company, because service agencies are still rare. Everything is mainframe-oriented! The IT auditor already learns something new, however: the role of system software as well as the risks of that system software, for example if access security and logging is not properly set up. Finally, the IT auditor must of course ensure that his programs and data have not been tampered with. The first generation of IT auditors is relatively technically savvy.

Fortunately, the IT market is also beginning to see the financial auditor (IT auditor) as a target audience, and the first standard audit software packages are cautiously appearing on the market. Best known from that time is CARS, a large COBOL program with sampling routines and counts in which the IT auditor can add their own COBOL rules to make it organization specific. Since the laptop hasn't been invented yet, the average IT auditor walks around with hefty suitcases with all those punch cards (having them mixed up would be a total drag ...). But it's still relatively easy as the file structure is sequential.

Introduction of the database

Shortly after, the database phenomenon makes its appearance. COBOL is not that suitable, and databases get their own supporting software. The IT auditor soon learns that using that database software is easier than CARS, although in the beginning that database software is not audit software, but mainly query software. Integration obviously does not take long and there is audit software for several database technologies, such as the independent package Culprit for IBM mainframes, for example. The problems at that time mainly involve accessing the file carriers (usually large tapes or very sensitive disks), which again are very specific to a certain type of machine. In short, they are only applicable to large known computer systems and large customers and therefore quite specialized. In the sixties and seventies, a large accounting firm like (now) KPMG had as many as thirty programmers who only programmed in the context of the annual audit.

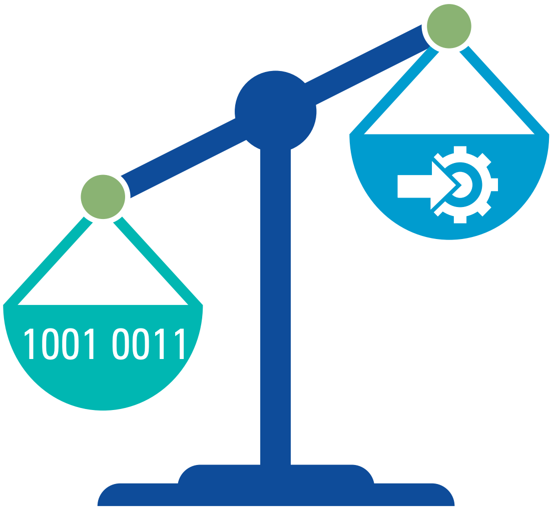

Figure 1. Data-oriented (substantive) prevails.

[1] Substantive versus system-based: in a substantive audit approach, the auditor obtains as much audit evidence as possible by selecting data and comparing it with external sources or by comparing it with other data already audited. This is often done on a sample basis. In a system-based audit approach, the auditor obtains audit evidence by assessing the adequacy of the system of internal controls in the processes and systems (design) and testing the operation of internal controls.

PC becomes widely available

The big break came in the early 80s. The PC made its appearance and so did the floppy drive (still 8-inch format). This brought medium-sized organizations into the picture to support the financial auditor on duty. Again, audit software lags behind, because the (existing) mainframe packages do not run on those PCs and the floppies do not fit into a mainframe. KPMG is even creating its own software package, of course again focused on determining and taking samples, and on making all kinds of calculations to match the client's financial records. There will even be an additional module that allows multiple files to be compared, a feat in those early days of the PC. When computerized financial accounting becomes commonplace, standard packages also become widely available. ACL and a little later IDEA are a few examples.

Need for greater understanding of security

In the 80s and certainly in the years that followed, the realization dawned that there were risks associated with all this IT, first in terms of security and then in terms of reliability. The financial auditor's clients also felt a greater need to understand this. As a result, IT auditors are increasingly taking on the role of specialists who also go to the client on behalf of the financial auditor, not just to retrieve data files, but to assess the quality of the IT and advise on it. First the physical security of the IT environment is revealed in the survey, later logical access. Tooling is still virtually unavailable on the market for that, which means that the IT auditor has to examine many specific operating systems and databases and learn how security is organized.

Although PC use increases the number of data analyses to be performed, the number of programmers decreases quite a bit, because the creation of the analyses takes much less time due to standard applications and the relatively small-scale environment in which the software can operate.

An end to file analysis?

In the 90s, system-oriented auditing is strongly on the rise and the "traditional" use of audit software declines rapidly. The previously mentioned group of as many as thirty programmers at a large accounting firm has disappeared entirely, although some of them are able to advance as 'regular IT auditors'. Yet this does not mean the end of file analysis. There are quite a few 'standardization' attempts, especially regarding the widely used SAP package. However, because of the many setting options, SAP still turns out not to be as standard as perhaps thought. The idea arises to create a front-end part for the extraction of data from the SAP databases that can be made customer specific or generation/version specific. The data is collected in a "meta database" for analysis and production of reports that strongly meet the auditor's needs. This back-end part had to be highly standardized. Of course, practice turns out unruly because the front-end part always needs adjustments after new SAP versions or implementations, but the demands of the financial auditor also keep changing as more information and exceptions are obtained from the data, which in turn need to be explained. The financial auditor has their hands full because the cost-benefit picture is constantly under scrutiny. The benefits for the insights and security of the auditor's audit approach do not always outweigh the effort required of constantly adapting SAP analyses.

Nevertheless, the seed has been planted and attempts are being made to revive data analysis in more industries, such as finance, where mostly self-developed systems at institutions predominate. The front-end part (data extraction) will always be variable here, but the back-end part (analysis and reporting) can then fit well with the auditor's audit approach. Because of the cost of developing such solutions, the approach is primarily international. However, this adds up to a much wider range of financial systems among auditees (front-end complication) and a wider range of auditors' requirements (back-end complication). Partly for this reason, only a few solutions were developed and not long-lived either.

The transition to system-based auditing

The IT auditor is already involved in examining processes and systems in the 80s. KPMG's IT auditors develop the CASA method (Course Approach to System Audits), which is adopted by the NBA (professional body for finan-

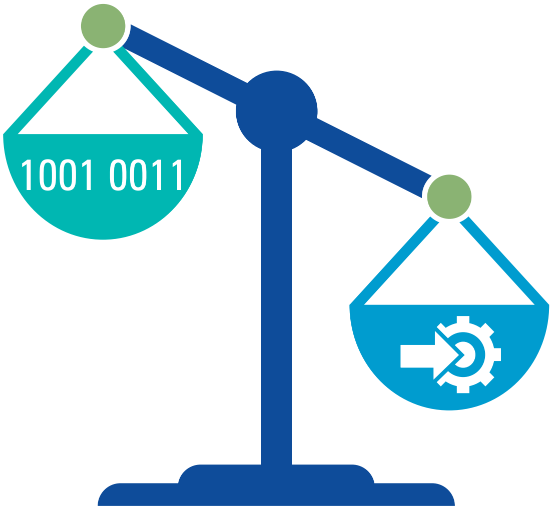

Figure 2. The balance has tipped toward system-based.

cial auditors in the Netherlands. ed.) (then NIVRA) in the publication FASA (Factual Approach to System Audits; see [Koed85] and [NIVR88]). The objective is still mainly: 'understanding the business'. In the 90s, system-based auditing emerges and there is more need for concrete insight into the processes and control measures. The IT auditor adapts the FASA method and Business Process Analysis (BPA) is born, where automated and manual internal control measures are explicitly recognized separately and per process step/risk. This distinction is important because the controls are different. For the IT auditor, this approach means a serious new object of investigation and assessing the automated controls against the general IT controls, especially change and test management and logical access security. So again, evidence of the proper functioning of the automated (application) controls must come from a system-based audit approach, i.e. entirely in line with the financial auditor's audit approach.

With the introduction of the Sarbanes Oxley (SOx) Act in 2002, much emphasis is placed on internal controls at companies. Pressured by the PCAOB regulator and the requirements of SOx 404, the field of system-based auditing is developing rapidly. The question from regulators, "How can I be sure that no one has been able to manipulate the data in question or modify application controls?" has caused headaches for many an auditor in PCAOB inspections and internal quality audits. In recent years, more guidance has emerged on how to deal with IPEs (Information Provided by the Entity, or in other words, how does the auditor determine that the auditee's information is reliable?), the various layers in IT environments, interfaces, assurance reports in the audit and cybersecurity. So, what has this yielded in recent years?

Financial auditors and IT auditors are working better together and have a better understanding of each other's fields. The audit methodologies of the various firms are making the role of the IT auditor increasingly clear. The new ISA 315 standard ("Identify and assess risks of material misstatement") has also contributed to this. This standard includes extensive guidelines for gaining insight into information technology and general IT controls. Consultation on any deficiencies in the system of internal control, on the risk assessment of those deficiencies and on any compensating controls has improved. It also seems that the work to gain assurance on the effective operation of IT controls is increasing. This makes sense in our view because IT is becoming more complex and because there is always someone in the IT environment who can (or sometimes should be able to) circumvent controls anyway. Although the probability of occurrence is low, the impact can be significant. The challenge is to be able to assess these risks and determine the impact. Not many organizations are mature enough in terms of risk management to adequately mitigate these risks, nor are they able or willing to make the investments to do so. Only a select number of organizations remain where the IT auditor or financial auditor can perform an exclusively system-based audit within the IT domain. This realization leads in some cases back to substantive audits by the IT auditor or financial auditor, which completes the circle again between substantive and system-based audits.

WHAT CAN WE EXPECT IN THE (NEAR) FUTURE?

Data-oriented

More data analysis is taking place right now. This will develop much further with all the relatively easier to access data. Consider the developments in centralized "data lakes", for example. These contain a lot of the organization's data (operational, financial, etc.), making analysis relatively easy. For large organizations, these data lakes are becoming too large and complex and there is a trend towards "data meshes", a form of decentralized small(er) data lakes, reducing complexity (also in management and responsibility). Of course there are tools that can link and analyze multiple of these data meshes. In short, a great field for the data analyst (commonly called data scientist these days), both within an organization and with the financial auditor. A financial auditor's wish to use data analysis to gain insight into the money and goods flow and (automated) analyses of the peculiarities in this money and goods flow could finally become a reality.

The question naturally arises if and when the complexity becomes so great that the financial auditor/IT auditor will start using other tools to still gain insight into the large amount of data available, both within the organization to be audited and beyond. In other words, how long will it be before the financial auditor and IT auditor together can start using AI applications themselves? Surely it would be ideal if AI software could perform the analyses, especially for the aforementioned analyses of anomalies in the money and goods flow. We expect that AI software can be a great help especially for gaining a good understanding of the nature and cause of deviations and the impact on the financial flow. This is particularly true in the current situation where data analytics has quite a bit of "fallout" and the financial auditor and/or IT auditor still has to incur significant costs to study the fallout and determine the impact. A current example of this is MindBridge Ai Auditor, with which KPMG has an alliance. MindBridge Ai Auditor supports data analytics through modern technologies and – using statistical analysis and machine learning based on a wide variety of data sets – identifies the risks per individual general ledger or income statement. This is needed to identify potential anomalies and deficiencies in financial records.

System-based

As indicated above, we see a bright future for substantive auditing. The question is whether there will still be a need for an assessment of the system of internal control. It is possible that the balance between the substantive audit with extensive data analyses on the one hand and the system-based audit with (limited) partial observations on the other hand will change. We believe that a certain degree of system-based audit will still be necessary to determine if the organization has taken a certain (minimum) level of control measures. A control approach of substantive auditing without the organization having a certain minimum level of internal control will provide greater uncertainty, in particular with regard to the quality (including completeness) of the data. This is something that substantive audits cannot determine or can only determine to a limited extent. Consider, for example, whether all data are actually in the records, or the "chiffre d'affaires," as financial auditors so eloquently call it.

In addition, regulators want to maintain continuous pressure on organizations and their auditors to ensure that the system of internal control at organizations is and remains adequate and that the risk of discontinuity and fraud remains limited. The SOx legislation and the (mandatory) role of the financial auditor in this regard is a good example and is not expected to disappear any time soon. For the IT auditor, this means that system-based audits in the area of generic IT (support) processes and specific information systems still have to take place at at least a select number of large organizations, although this also applies in a less formal way to smaller organizations.

By now, we see organizations using AI applications in practice (e.g., insurance companies). The internal control of AI applications will require the IT auditor to have a better understanding of the design and operation of such AI applications. The fact that things are moving fast is evident from the various audit frameworks that have been published, including by the Association of Insurers, as well as IIA (Institute of Internal Auditors Netherlands) and various other organizations. NOREA's (Dutch professional association for IT auditors) Algorithm & Assurance Knowledge Group has already published several frameworks.

Broader role of the IT auditor

Recent years have shown that more is expected from the financial auditor than a "bare" financial statement audit. In particular, other laws and regulations, other than for the financial statement audit, are forcing organizations to include other information in the annual report, for example on the establishment and enforcement of privacy or information security/cybersecurity and ESG.

Although the European AI law is not yet in place, it is already clear that audits of products and services equipped with AI will fit into existing quality management systems of sectors such as logistics and healthcare. The Corporate Sustainability Reporting Directive (CSRD) will also broaden the role of the IT auditor. Starting in 2024, the first organizations have to start complying with these requirements. For now, only "limited assurance" is required, but it is expected that by the end of this decade "reasonable assurance" also needs to be provided for sus-

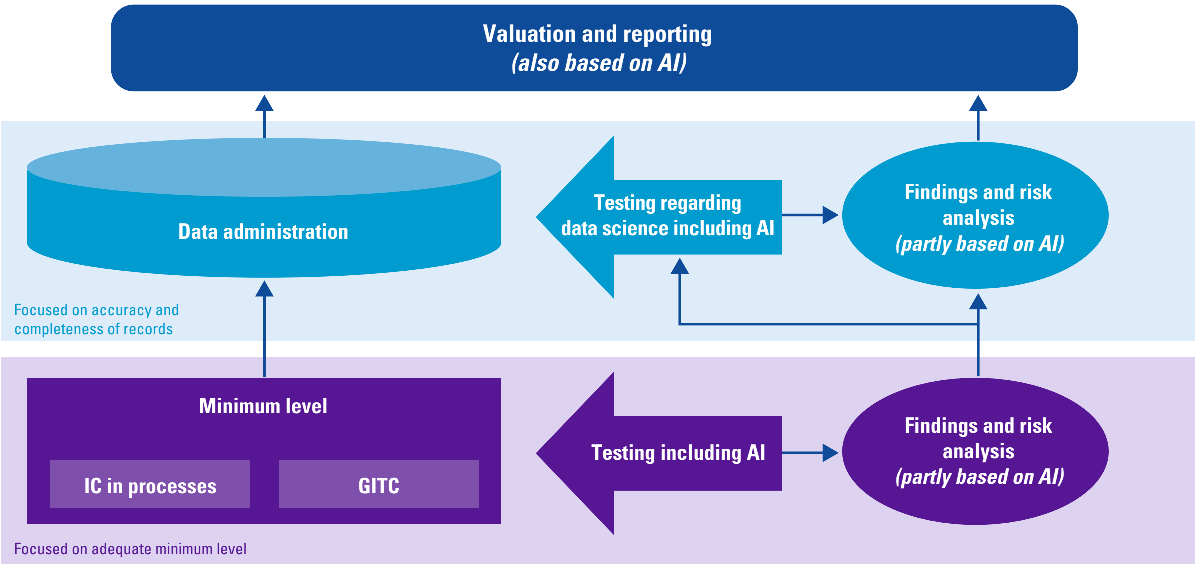
Valuation and reporting
(also based on AI)
Data administration
Testing regarding data science including AI
Findings and risk analysis (partly based on AI)
Focused on accuracy and completeness of records
Minimum level
IC in processes
GITC
Testing including AI
Findings and risk analysis (partly based on AI)
Focused on adequate minimum level

Figure 3. Approach to the financial statement audit.

tainability figures. Organizations are investing heavily to generate these figures. In this regard, reliability requirements play a role. The challenges may not be different from normal financial reporting chains, but there are specific areas of focus for ESG, partly because of the special areas of knowledge, but also because the reporting chains are still new and have never been subject to audit before. Also, employees in non-financial departments within organizations are less accustomed to strict compliance with regulations to be "in control," with the risk of incomplete information and auditability.

CONCLUSION

The profession of IT auditors grew doing data file reviews and data analysis, leading the period when auditors primarily followed the substantive audit approach. When system-based auditing emerged in the 90s, later reinforced by SOx regulations, the focus of the IT auditor became less data-oriented and concentrated primarily on assessing programmed controls in financial reporting processes and the underlying generic IT management processes, such as change management and logical access.

Although the audit orientation is still system-based, there is clearly a revival of file searches/data analysis. Data are more approachable and data analysis tools are more powerful. System-based auditing is no longer seen as the holy grail.

We expect that the balance will again tip slightly toward data analysis, with more attention being paid, on the one hand, to encompassing overall controls (think of overall movement of cash and goods) and, on the other hand, especially to the (automated) analysis and risk assessment of the anomalies. A small dot of tools supported by AI is already shining on the horizon.

System-based auditing will not disappear because, on the one hand, it provides a good understanding of the organization and its processes and, on the other, it ensures the quality of the data captured during those processes. Where quality of IT processes is essential for internal controls in financial processes, quality in processes is essential for data analysis. This means that it's not either system-based or substantive, but the best of both worlds. Those worlds are expanding as more and more topics other than purely financial statements are included in the annual report and the scope of the auditor. Most notable is ESG reporting, bringing new processes and data into scope.

In the 80s, a presentation by the Canadian Institute of Chartered Financial auditors (CICA) was frequently shown in the Netherlands. The gist was that in the magical year 2000, financial auditor Gene performed the annual audit by linking his "audit" computer with that of the auditee and the audit program did the rest. Miss Jane brought coffee (that was the way it was done in those days) and in the afternoon the results were discussed with the director of the audited organization.

In short, the future of the IT auditor in the context of the "financial statement" audit still needs a solid toolbox, but hopefully not like the punch card boxes and first draggable desktop computers which processed the data analyses. In the bottom two layers of the approach to the financial statement audit described earlier, a dual role of financial auditor knowledge and IT knowledge seems desirable, perhaps in an integrated profile of financial auditor and IT auditor. Although, given Gene's example above, that will take longer than desired.

References

[Koed85] A.H.C. Koedijk (1985). Beoordeling betrouwbaarheid van een (geautomatiseerd) informatiesysteem: De CASA methode. *Compact, 1985*(4).

[NIVR88] NIVRA (1988). NIVRA-geschrift 44, Automatisering en Controle: Feitelijke Aanpak Systems Audit.

About the authors

Peter van Toledo RE, MA is a director at KPMG IT Assurance & Advisory. He started his career at KPMG Financial auditors and switched to KPMG Advisory in the late nineties. He has several tasks at KPMG, including IT auditing for the financial audit, SOC audits, and quality assurance during project implementation. Peter is responsible for the IT Attestation service line in KPMG EMEA.

Herman van Gils RE, MA worked at KPMG for forty years, first in auditing and then in IT auditing. At both NOREA and NBA, he participated in various committees. Now retired, he is still affiliated with the University of Amsterdam.