TAX, AUDIT & ACCOUNTANCY

NR 88
N° 88

JAARGANG 20 / 20e ANNEE
MAART/MARS 2025
10X/JAAR / 10X/AN
ISSN: 2033-4575

☐ **Audit 2.0: Is the profession ready for a future with AI?**

☐ **La gestion de la sécurité de l'information dans les bureaux d'audit / Informatiebeveiligingsmanagement in auditkantoren**

☐ **L'esprit critique en matière d'audit à la lumière de la philosophie / Professioneel-kritische instelling bij auditing in het licht van de filosofie**

die Keure
la Charte

ICCI
Informatiecentrum voor het Bedrijfsrevisoraat
Centre d'Information du Réviseurs d'Entreprises

IBR-IRE
Instituut voor de Bedrijfsrevisoren
Institut des Réviseurs d'Entreprises

SOMMAIRE INHOUD

01 *L'esprit critique en matière d'audit à la lumière de la philosophie*
Professioneel-kritische instelling bij auditing in het licht van de filosofie

07 Audit 2.0: is the profession ready for a future with AI?

19 *La gestion de la sécurité de l'information dans les bureaux d'audit*
Informatiebeveiligingsmanagement in auditkantoren

TAX AUDIT & ACCOUNTANCY

Revue mensuelle du Centre d'Information du Révisorat d'entreprises (ICCI)
Abréviation recommandée : TAA

Maandelijks tijdschrift van het Informatiecentrum voor het Bedrijfsrevisoraat (ICCI)
Aanbevolen afkorting: TAA

EDITEUR RESPONSABLE
VERANTWOORDELIJKE UITGEVER
L. Guarino
Koning Albert II-laan 19 - Boulevard du Roi Albert II 19
1210 Bruxelles - Brussel

MISE EN PAGE
VORMGEVING
die Keure/la Charte
Brugge

TRIBUNE / OPINIESTUK

L'ESPRIT CRITIQUE EN MATIÈRE D'AUDIT À LA LUMIÈRE DE LA PHILOSOPHIE

A première vue, les auditeurs manient plutôt des chiffres et des données et les philosophes plutôt des mots et des concepts, ils ne vivent pas pour autant sur des planètes si différentes. Ils ont en commun la même exigence de rigueur intellectuelle.

L'esprit critique, principe fondamental qui sous-tend la profession d'auditeur, fait partie de la démarche philosophique depuis ses débuts en Grèce. Le doute et la remise en cause des apparences et des certitudes sont depuis toujours un des ressorts de la philosophie dont la visée est avant tout de s'étonner, de questionner et de clarifier.

Les enseignements de la philosophie

Remontons donc aux premiers temps de la philosophie à Athènes, avec **Socrate**. Pionnier en la matière, Socrate encourageait l'examen des croyances et des pratiques établies, soulignant l'importance de la réflexion critique pour atteindre la vérité. Il n'a jamais rien écrit et a laissé à Platon le soin de transmettre sa méthode de questionnement à travers ses fameux dialogues.

PROFESSIONEEL-KRITISCHE INSTELLING BIJ AUDITING IN HET LICHT VAN DE FILOSOFIE

Op het eerste gezicht hanteren auditors veeleer cijfers en gegevens en filosofen veeleer woorden en concepten, maar zij leven niet op zulke verschillende planeten.
Zij hebben dezelfde vereiste van intellectuele nauwkeurigheid gemeen.

De professioneel-kritische instelling, een fundamenteel beginsel dat aan het auditberoep ten grondslag ligt, maakt sinds het begin in Griekenland deel uit van de filosofische benadering. Twijfel en het in vraag stellen van uiterlijke schijn en zekerheden zijn altijd één van de drijfveren van de filosofie geweest, die vooral tot doel heeft zich te verwonderen, te bevragen en toe te lichten.

De lessen van de filosofie

Laten wij dus teruggaan naar de begindagen van de filosofie in Athene, met **Socrates**. Als pionier in het veld moedigde Socrates het onderzoek naar gevestigde overtuigingen en praktijken aan, waarbij hij wees op het belang van kritische reflectie bij het bereiken van de waarheid. Hij schreef nooit iets en liet het aan Plato over om zijn methode van vragen stellen door middel van zijn beroemde dialogen over te brengen.

2

Plutôt que de demander à ses interlocuteurs une bonne réponse, Socrate leur suggérait la pratique de la bonne question. Par exemple, une question dont le but est d'aider à clarifier et à comprendre le point de vue présenté : Qu'entendez-vous par là ? Comment expliquez-vous que… ? Une question sur les hypothèses avancées : Y a-t-il des preuves de… ? Est-ce toujours le cas ? Ou encore une question qui vise à tester la solidité de l'argumentation : Pourquoi dites-vous que… ? Comment peut-on justifier cela ? Autant de questions qui devraient être familières des auditeurs dans leur travail d'analyse et de vérification.

Socrate s'employait ainsi à dénoncer les sophismes, les erreurs de raisonnement et les arguments fallacieux, ouvrant la voie au scepticisme. Mais c'est **Pyrrhon d'Elis** qui fit du scepticisme une philosophie à part entière. Le scepticisme pyrrhonien remet en question la possibilité de connaître quelque chose avec certitude et érige le doute en système de pensée. Il constate l'impossibilité où nous sommes d'arriver à une connaissance définitive du monde et à la Vérité.

Cette approche a influencé par la suite des penseurs comme **Montaigne** qui prône une grande circonspection dans le jugement et une extrême prudence à l'égard des préjugés, des croyances et des dogmes de son époque, la Renaissance. Célèbre pour sa devise « Que sais-je ? », il reconnaît les limites humaines dans la compréhension du monde.

Montaigne invente le scepticisme moderne, contribuant à lui donner le sens que le mot a aujourd'hui : le refus d'admettre une chose sans examen critique, une attitude de doute, de réserve devant un fait, une proposition quelconque.

Au siècle suivant, **Descartes**, souvent considéré comme le père du rationalisme, propose un exercice de pensée qu'il nomme « le doute

In plaats van zijn gesprekspartners om een goed antwoord te vragen, stelde Socrates hen de praktijk van de juiste vraagstelling voor. Bijvoorbeeld een vraag die tot doel heeft het gepresenteerde standpunt toe te lichten en te begrijpen: Wat bedoelt u daarmee? Hoe verklaart u dat …? Een vraag over de naar voren gebrachte veronderstellingen: Is er enig bewijs van …? Is dat nog steeds zo? Of een vraag die tot doel heeft de deugdelijkheid van de argumentatie te toetsen: Waarom zegt u dat …? Hoe is dit te verantwoorden? Zoveel vragen waarmee auditors vertrouwd zouden moeten zijn in het kader van hun analyse- en verificatiewerkzaamheden.

Socrates wilde zo drogredenen, denkfouten en misleidende argumenten aan de kaak stellen en maakte de weg vrij voor scepticisme. Maar het was **Pyrrhon van Elis** die van scepticisme een volwaardige filosofie maakte. Het Pyrrhonische scepticisme zet vraagtekens bij de mogelijkheid om iets met zekerheid te weten en vestigt twijfel als een denksysteem. Het stelt vast dat het voor ons onmogelijk is om tot een definitieve kennis van de wereld en de Waarheid te komen.

Deze benadering beïnvloedde vervolgens denkers zoals **Montaigne** die voorstander is van grote behoedzaamheid bij het beoordelen en extreme voorzichtigheid met betrekking tot de vooroordelen, overtuigingen en dogma's van zijn tijd, de Renaissance. Beroemd om zijn motto "Wat weet ik?", erkent hij menselijke beperkingen in het begrijpen van de wereld.

Montaigne bedenkt het moderne scepticisme en heeft ertoe bijgedragen dat het woord de betekenis krijgt die het vandaag de dag heeft: de weigering om iets toe te geven zonder kritisch onderzoek, een houding van twijfel, van terughoudendheid tegenover een feit, een voorstel van welke aard dan ook.

In de volgende eeuw stelt **Descartes**, vaak beschouwd als de vader van het rationalisme, een gedachteoefening voor die hij

méthodique » ou hyperbolique par lequel il s'agit de contester la vérité de tout ce à quoi on adhère sans l'avoir démontré. Pour que le doute sceptique ne soit pas une incapacité de savoir, Descartes tâche d'en faire une étape vers la connaissance.

A la même époque, **Francis Bacon** appelle les scientifiques à détruire ce qu'il nomme les « idoles », c'est-à-dire les préjugés auxquels ils sont attachés et place l'esprit critique au cœur des sciences.

Plus tard, David **Hume** recommande, puisque nous ne pouvons atteindre la certitude, de faire la meilleure estimation possible des réalités qui se trouvent sous nos yeux. Ce n'est pas parce que certaines croyances fondamentales sont naturelles et irrésistibles qu'elles sont vraies ou correctes, le plus souvent, elles sont basées sur des habitudes plutôt que sur des preuves rationnelles.

Les penseurs des **Lumières** avaient comme exigence de ne jamais consentir à la reprise docile de la pensée d'autrui. L'enjeu majeur était de faire reculer l'obscurantisme, les dogmes et les préjugés, ce qui suppose tout à la fois l'autonomie de la pensée et le développement de l'esprit critique.

Troublé par le scepticisme de Hume, **Kant** dira que celui-ci l'a fait sortir de son « sommeil dogmatique ». Toute l'œuvre du grand philosophe allemand est en effet indissociable du terme « critique ». « Je sais que je ne sais pas », disait Socrate. « Que sais-je ? » se demandait Montaigne. « Que puis-je savoir ? » s'interroge Kant qui cherche à établir les conditions de possibilité de la connaissance, en expliquant que nous ne voyons pas le monde tel qu'il est mais tel que nous sommes.

Plus près de nous, **Nietzsche,** qui disait vouloir faire de la philosophie avec un marteau, a fait une critique radicale de la culture occidentale

"methodische" of hyperbolische "twijfel" noemt, waarbij de waarheid van alles wat men aanneemt zonder het te hebben aangetoond, wordt betwist. Zodat sceptische twijfel geen onvermogen is om te weten, tracht Descartes er een stap naar kennis van te maken.

Tegelijkertijd roept **Francis Bacon** wetenschappers op tot het vernietigen van wat hij "afgoden" noemt, d.w.z. de vooroordelen waaraan zij zijn gehecht, en plaatst hij de professioneel-kritische instelling in het hart van de wetenschap.

Later adviseert **David Hume** dat wij, aangezien wij geen zekerheid kunnen bereiken, de best mogelijke inschatting maken van de werkelijkheid die zich voor onze ogen afspeelt. Het is niet omdat bepaalde kernovertuigingen natuurlijk en onweerstaanbaar zijn, dat zij waar of correct zijn. Vaker wel dan niet zijn zij gebaseerd op gewoonten veeleer dan op rationeel bewijs.

Verlichtingsdenkers hadden als vereiste om nooit in te stemmen met het volgzaam overnemen van het denken van anderen. De belangrijkste uitdaging was het terugdringen van obscurantisme, dogma's en vooroordelen, wat zowel de autonomie van het denken als de ontwikkeling van een professioneel-kritische instelling veronderstelt.

Verontrust door het scepticisme van Hume, zal **Kant** zeggen dat Hume hem uit zijn "dogmatische slaap" heeft gehaald. Al het werk van de grote Duitse filosoof is immers onlosmakelijk verbonden met de term "kritisch". "Ik weet dat ik het niet weet", zei Socrates. "Wat weet ik?", vroeg Montaigne zich af. "Wat kan ik weten?", vraagt Kant zich af, die tracht de voorwaarden voor de mogelijkheid van kennis vast te stellen, door toe te lichten dat wij de wereld niet zien zoals die is, maar zoals wij zijn.

En wat dichter bij ons ligt **Nietzsche,** de filosoof met de hamer, leverde radicale kritiek op de moderne westerse cultuur, waarbij hij

moderne, encourageant le questionnement et la remise en cause des valeurs, des dogmes et des vérités établies.

Les enseignements pour les auditeurs

Ces différents philosophes ont contribué chacun à leur façon à établir les fondements de l'esprit critique, à en montrer la voie et nous invitent à exercer et entretenir le nôtre. Leur pensée peut être une source d'inspiration et enrichir la pratique de l'auditeur dans son travail d'analyse, de vérification et d'évaluation.

A la lumière de la maïeutique de Socrate, de l'empirisme sceptique de Hume, du doute méthodique de Descartes ou du questionnement radical de Kant sur les limites de la raison, en quoi devrait consister l'esprit critique en matière d'audit ? A poser et se poser les bonnes questions, à ne pas accepter sans réserve ce qui est présenté comme une évidence, à douter de manière constructive, à prendre conscience de l'influence de sa propre subjectivité dans tout jugement.

De manière plus précise, l'esprit critique ou scepticisme professionnel doit permettre à l'auditeur, dans une perspective indépendante et objective, de remettre en question les informations et les éléments probants qui lui sont soumis. En adoptant une attitude sceptique, il se met en mesure d'identifier les incohérences et les anomalies, de tester la solidité des arguments avancés, de débusquer les stratagèmes et les manipulations, de faire la part entre les faits et l'interprétation des faits.

Faire confiance avec discernement

On pourrait le dire autrement. Exercer son esprit critique pour l'auditeur, c'est chercher à

aanmoedigde om gevestigde waarden, dogma's en waarheden in twijfel te trekken en in vraag te stellen.

De lessen voor de auditors

Deze verschillende filosofen hebben elk op hun eigen manier bijgedragen aan het leggen van de grondslagen van de professioneel-kritische instelling, aan het wijzen van de weg ernaartoe, en nodigen ons uit om een professioneel-kritische instelling aan te nemen en te handhaven. Hun denken kan een inspiratiebron zijn en de praktijk van de auditor bij zijn analyse-, verificatie- en beoordelingswerkzaamheden verrijken.

Waaruit zou de professioneel-kritische instelling bij auditing – in het licht van de maieutiek van Socrates, het sceptisch empirisme van Hume, de methodische twijfel van Descartes of de radicale bevraging van Kant naar de grenzen van de rede – moeten bestaan? Uit het stellen van de juiste vragen, het niet zonder voorbehoud aanvaarden van wat als vanzelfsprekend wordt voorgesteld, het constructief twijfelen, het zich bewust worden van de invloed van de eigen subjectiviteit in elke oordeelsvorming.

Meer in het bijzonder moet de professioneel-kritische instelling of het professioneel scepticisme de auditor in staat stellen om, vanuit een onafhankelijk en objectief perspectief, de aan hem voorgelegde informatie en controle-informatie in vraag te stellen. Door het aannemen van een sceptische houding is de auditor in staat om inconsistenties en afwijkingen te identificeren, de deugdelijkheid van de aangevoerde argumenten te toetsen, strategieën en manipulaties aan het licht te brengen, en onderscheid te maken tussen de feiten en de interpretatie van de feiten.

Vertrouwen hebben met oordeelkundig inzicht

Men zou het anders kunnen zeggen. Het aannemen van een professioneel-kritische

bien calibrer sa confiance, à la baisse ou à la hausse, plus ou moins fortement, en fonction de l'évaluation qu'il aura faite de l'information et de sa source, à l'aide de plusieurs indices : sa plausibilité, la rigueur logique du raisonnement, la qualité et le nombre de preuves à l'appui, etc.

Au-delà de l'analyse des informations et des données, l'auditeur doit pouvoir aussi comprendre les motivations, les biais et les contextes qui sont à l'œuvre, tout en se méfiant de ses propres biais et préjugés. A ce propos, on peut rappeler que c'est à **Kahneman** et **Tversky**, deux psychologues américains, que l'on doit d'avoir montré à quel point les mécanismes mentaux non rationnels, les fameux biais cognitifs, influencent et perturbent le jugement et la prise de décision.

Cette capacité à penser de manière critique est cruciale pour garantir l'intégrité, la transparence et la fiabilité des rapports d'audit. Elle est d'autant plus importante que nous vivons dans un monde où l'information est omniprésente et contradictoire, où les fake news prolifèrent sur internet et brouillent les pistes. L'auditeur doit pouvoir discerner le vrai du faux, s'interroger sur la nature même de la vérité, rejoignant ainsi une des grandes préoccupations de la philosophie.

Les réflexions partagées dans ce texte valent autant pour l'analyse en profondeur des états financiers de l'entreprise et des hypothèses et évaluations qui les sous-tendent que pour l'analyse de ses performances en matière de durabilité qui intéressent les parties prenantes.

Pour conclure, c'est en tant que pratique de la pensée critique que le travail de l'auditeur

instelling houdt in dat de auditor tracht zijn vertrouwen bij te stellen naar beneden of naar boven, in meer of mindere mate, afhankelijk van de beoordeling die hij zal hebben gemaakt van de informatie en de bron ervan, met behulp van een aantal indicatoren: de plausibiliteit ervan, de logische nauwkeurigheid van de redenering, de kwaliteit en kwantiteit van het bewijsmateriaal, enz.

Afgezien van het analyseren van informatie en gegevens moet de auditor ook in staat zijn om een inzicht te krijgen in de betrokken beweegredenen, tendenties en contexten, terwijl hij op zijn hoede is voor zijn eigen tendenties en vooroordelen. In dit verband kan eraan worden herinnerd dat **Kahneman** en **Tversky**, twee Amerikaanse psychologen, hebben aangetoond in welke mate niet-rationele mentale mechanismen, de zogenaamde cognitieve tendenties, de oordeelsvorming en het besluitvormingsproces beïnvloeden en verstoren.

Dit vermogen om kritisch te denken is van cruciaal belang voor het waarborgen van de integriteit, transparantie en betrouwbaarheid van controleverklaringen. Het is des te belangrijker omdat wij leven in een wereld waarin informatie alomtegenwoordig en tegenstrijdig is, waarin nepnieuws zich op het internet verspreidt en de sporen vervaagt. De auditor moet in staat zijn om het ware van het valse te onderscheiden en de aard zelf van de waarheid in twijfel te trekken, en dit in overeenstemming met één van de grote bekommernissen van de filosofie.

De in deze tekst gedeelde overwegingen zijn evenzeer van toepassing op de grondige analyse van de financiële overzichten van de onderneming en de veronderstellingen en evaluaties die eraan ten grondslag liggen, als op de analyse van haar duurzaamheidsprestaties die van belang zijn voor belanghebbenden.

Concluderend kan worden gesteld dat de werkzaamheden van de auditor als een praktijk

revêt une dimension philosophique et dépasse la simple analyse technique. C'est en tant que fondement de la pensée critique que la philosophie, au-delà de la théorie, apporte un éclairage utile sur les exigences et la pratique quotidienne de l'audit.

Anne Mikolajczak

van kritisch denken een filosofische dimensie krijgen en verder gaan dan de louter technische analyse. Het is als de grondslag van kritisch denken dat filosofie, voorbij de theorie, nuttig inzicht biedt in de vereisten en de dagelijkse praktijk van auditing.

Anne Mikolajczak

AUDIT 2.0: IS THE PROFESSION READY FOR A FUTURE WITH AI?

EDDY CARDINAELS

Professor of accounting at Tilburg University and part-time professor at KU Leuven

JUDITH KÜNNEKE

Assistant Professor at Tilburg University

Introduction

While new technologies are often met with skepticism due to their potential to revolutionize accounting practices, the emergence of LLMs (Large Language Models) and AI—with their extensive capabilities—represents an even more significant game-changer. In the past, we have seen the emergence of new techniques such as ERP systems, continuous auditing, XBRL accounting, blockchain technology, automation tools like robotic process automation (RPA), and many more (Eulerich *et al.*, 2024). What sets AI apart is that it is one of the fastest-growing technologies. Applications like Microsoft Copilot, ChatGPT, Bing, and various other platforms make the technology accessible at low cost to many corporations and individuals (Reuters, 2023; Eulerich *et al.*, 2024).

Research by OpenAI and the University of Pennsylvania (Eloundou et al., 2023) highlights that accounting and auditing are among the professions most significantly impacted by AI. The World Economic Forum's Future of Jobs Report (2023) also projects considerable job losses in accounting due to advances in digitalization and automation by 2027. Likewise, Frey and Osborne (2017) place registered auditors within the top 20% of occupations most impacted by computerization. Indeed, the performance of AI cannot be underestimated, and the notion that the computer can replace the registered auditor might not be a myth. For example, Eulerich *et al.* (2024) show that ChatGPT 4.0 can pass all the CPA exams with a score of 85.1% when using additional training and calculation tools. So, time to let the robot do the work, right?

We, however, argue that the future of registered auditors "with AI" still looks bright. Though AI models demonstrate impressive capabilities, human intervention and professional skepticism

remain essential. Registered auditors who embrace these tools and integrate them thoughtfully into their work will not only enhance audit quality but also redefine the profession's future. While AI tools will not replace humans, registered auditors who ignore or disregard their potential might find themselves replaceable. The challenge lies not in resisting AI but in leveraging it to transform audit practices.

Embracing the tools and capabilities of AI

Before describing what AI can offer to registered auditors, it is helpful to define what AI encompasses. Several definitions have been put forward. In broad terms, artificial intelligence (AI) refers to the development of computer systems or machines that can perform tasks that typically require human intelligence (IBM, 2024; Medium, 2023). The idea of AI is to create technologies and applications that can mimic, augment, or even outperform humans in many domains. AI is designed to analyze large patterns of data, recognize patterns in the data, and sometimes even make autonomous decisions with various degrees of discretion.

AI appears in many disciplines. Healthcare professionals use it to check patient records, medical tests, and X-rays, detecting certain patterns and anomalies to help physicians diagnose conditions like cancer much earlier in the process. Robotic surgery is another revolutionary example. As a result, AI enables healthcare professionals to focus more on tasks that need the "human touch". For example, patients often feel that doctors do not spend sufficient time with them to interact closely and build trust, and indeed, due to the shortage of doctors, they often do not have time. With AI taking over some tasks, human time is freed up and can be used where humans add more value than AI—for instance, in guiding and comforting patients in difficult times (Levels, 2020). In transportation, AI-powered route optimization tools analyze traffic, weather, package volume, and delivery constraints in real-time

EMBRACING EVEN THE SIMPLE FORMS OF TECHNOLOGY CAN MAKE A NOTABLE DIFFERENCE TO THE PROFESSION.

to determine more efficient routes. Shops like Target and online stores like Amazon analyze purchasing history of their customers, using big data to predict their next big purchase. This allows them to engage in tailored marketing strategies that try to satisfy customer needs but ultimately boost sales. Even simple tools like personal assistants or using Copilot in meetings help employees gain efficiency in their daily work—for example, by taking notes, providing summaries of the meeting, and sending the summary to all participants. Recruiters also use AI to select the best candidates for the job, and machine learning tools are often capable of selecting the candidates that will excel in future jobs (Chen and Ke, 2024).

A. What's in it for the registered auditor?

CPA Canada and AICPA (2019) argue that AI has different levels of maturity (see Figure 1). Simple technologies of AI do not always require deep learning. At the more advanced stages, AI, machine learning, and deep learning techniques enter the scene. Yet, we argue that embracing even the simple forms of technology can make a notable difference to the profession.

In stage 1, decision-makers focus on basic or routine tasks that, with limited intelligence, can be performed by computers and algorithms. With limited investment, numerous audit tasks can already be supported through the use of technology.

Robotic processes can assist registered auditors in the profession. Robotic process automation (RPA) tools have been implemented early on in digital auditing platforms such as KPMG Clara or EY Canvas. These RPAs can streamline

financial processes by automating repetitive tasks such as data entry, reconciliation, report generation, and processing of information. Natural Language Processing (NLP) or AI-driven NLP technologies can extract insights from unstructured textual data, such as audit reports, emails, and legal documents, facilitating efficient information retrieval and analysis.

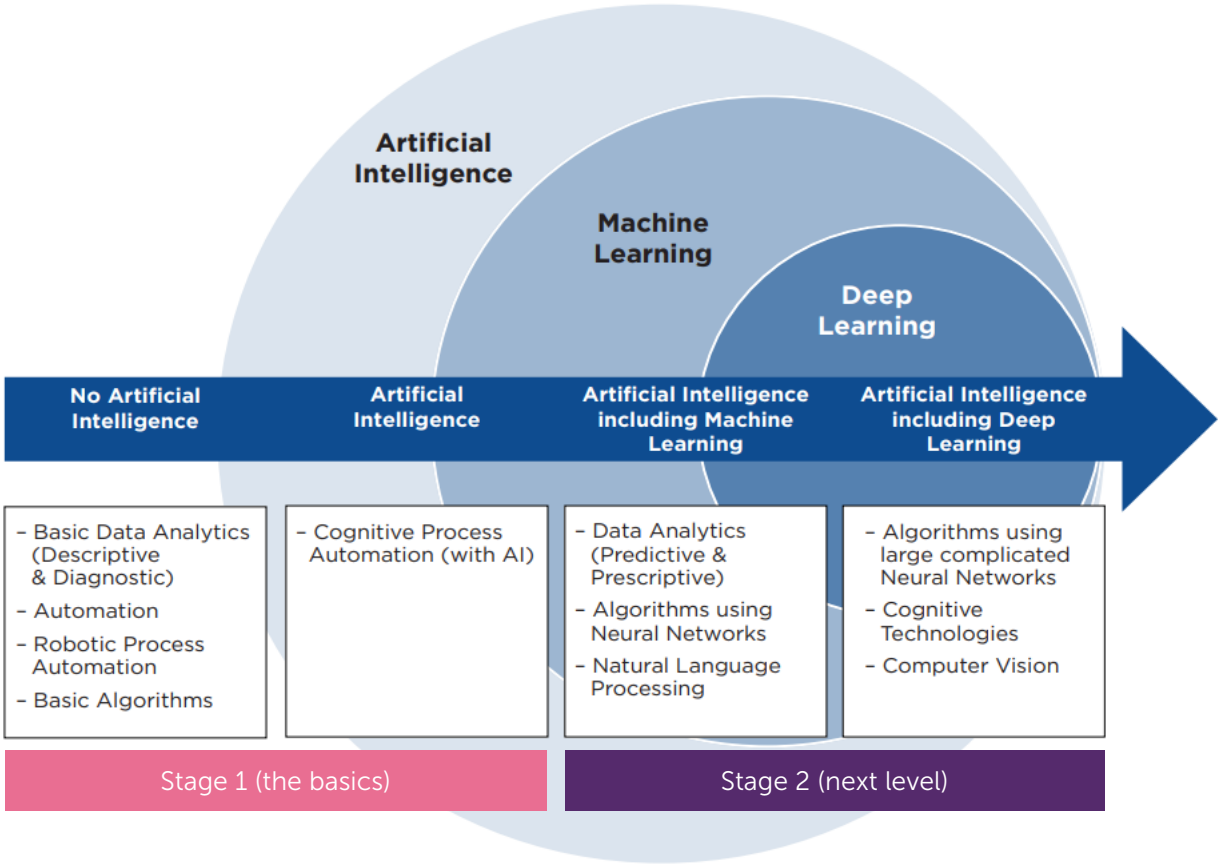

Figure 1: Stages in AI applications (CPA and AICPA, 2019).

Inventory counting, for example, is a process that can be automated. Christ *et al.* (2021) show that drones can help auditors with this time-consuming task. New technologies can decrease count time from 681 hours to 19 hours while at the same time counting more accurately. Error rates in the study decreased significantly from 0.15% to 0.03%. Such technologies may come with sizeable costs, a topic to which we return later. At the same time, this significant reduction in time can help auditors focus back on the core business of providing sense and context to documentation that helps support their findings. Invoicing, payroll administration, gathering evidence, and extracting data from several source documents can be automated. Similar to healthcare professionals, auditors can resort to automation of collecting evidence and help to gather initial diagnostic information about potential red flags or cues that require further investigation.

Natural Language Processing (NLP) offers additional benefits. Researchers from Chicago (Kim *et al.*, 2024) have shown that AI performs remarkably well in offering risk reports for companies. Their models help to train ChatGPT in extracting risk information from conference calls. They show that the AI-generated risk reports predict economic outcomes of companies more efficiently. Auditors can mimic this process. With specific prompts, they can extract crucial information from the companies' filings and documentation and assess whether companies are at risk. Another example is provided by Cardinaels *et al.* (2019). A simple algorithm can summarize earnings releases from companies. The big benefit of AI is that it provides summaries with less bias, directing the decision-maker to the fundamental cues that matter for future performance. It helps to undo the biases that managers introduce in their summaries, offering greater insight to the decision-maker.

When gathering evidence, the use of AI is also important. Recently, many companies, including audit firms, design their internal chatbots to assist auditors (WSJ, 2023; Deloitte, 2023) or help auditors to plan better on how to approach audit tasks. In their working paper, Bhaskar et al. (2024) show that such bots help decision-makers. The use of such tools leads to more speaking-up behavior as auditors feel more confident about raising red flags and important issues during meetings. While such internal bots are not always available at smaller firms, simpler tools like summarization, automatic gathering of evidence, or instructing ChatGPT to calculate ratios and analyze some of the fundamentals can be fruitful for saving efficiency in the initial phases of the audit.

B. Upscaling the sampling procedure

A significant aspect of the audit profession involves checking transactions and procedures to detect anomalies or potential red flags. Due to the often large amounts of records, auditors often resort to sampling. Sampling is an auditing technique that provides supporting evidence that allows auditors to issue audit opinions without having to audit every single item and transaction. While this technique makes a lot of sense, AI offers a drastic shift in approaching the testing phase. If you can test the entire population with computing power, why not apply it?

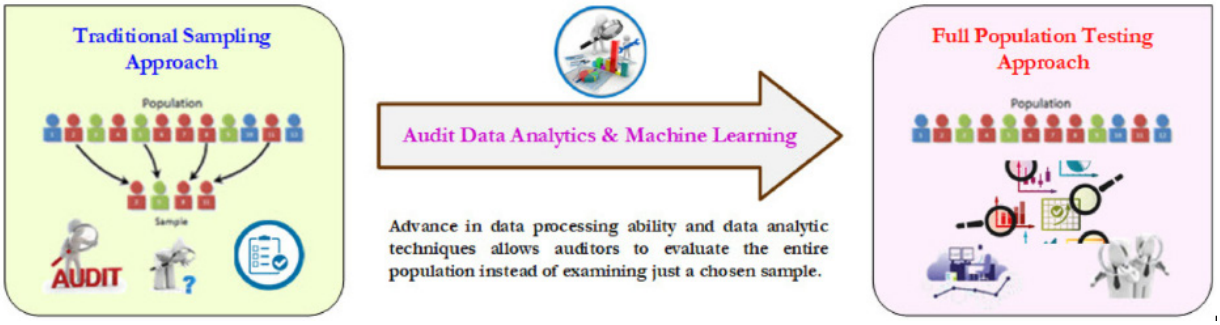

Figure 2: Upscaling sampling (Huang et al., 2022)

While small-scale sampling has its value, stage 2 models of AI (see Figure 1), using more advanced machine learning techniques, allow the testing of the full set of transactions that a company conducts, making it more economical. Consider giants like Amazon or Bol.com, which produce millions or even billions of transactions annually. Drawing up a representative sample of transactions here is nearly impossible or subject to errors. Even if one would test 500,000 transactions, it still represents much less than 1% of the transactions of Amazon. The issue

with sampling is that it is hard to achieve a representative sample, and error rates are large as auditors tend to rely on fairly small samples as they were traditionally restricted by time and computing power. The conclusions that one draws from a small sample might not be representative of the entire population. This runs the risk that certain anomalies might not be flagged and remain undetected.

With AI, the entire population can be screened. Audit data analytics and machine learning can play a critical role in identifying abnormal transactions (Huang et al., 2022). For instance, it may list that from the full set of invoices, about 5% did not follow the standard routing, and 2% had strange anomalies. AI can be further trained to prioritize exceptions based on the severity of violations and the dollar amounts involved. This initial evidence gathering leads to a complete picture and ensures that many of the anomalies that may go unnoticed via small sampling are now put on the table. In the Belgian audit profession, for example, these tools are employed for tasks such as journal entry testing in compliance with ISA 240. However, the use of such tools remains heavily dependent on the resources and infrastructure of specific audit networks.

This is just one example of more advanced techniques that auditors can use. Machine learning (Stage 2) can also be used for fraud detection. It further allows auditors to predict future trends and significant changes in earnings, again allowing the auditor to identify potential going concern issues earlier. This can also be informative for management of the company to see where further action is required. The risk analyses of the previous section can also be upscaled with machine learning techniques.

Upscaling will be increasingly important, as with the introduction of CSRD, the company's efforts on environmental, social, and governance (ESG) aspects need to be assured. Here, given the amount of data, AI can play an even bigger role in gaining efficiency and helping the auditors in assuring that the company's disclosures are reasonably accurate.

Investments in the future

As the integration of Artificial Intelligence (AI) into the auditing profession moves forward, many firms weigh the costs against the benefits. While initial expenditures and the learning curve associated with adopting AI tools are unavoidable, these costs should be viewed not merely as expenses but as strategic investments in the future of auditing.

A. The investment perspective on AI implementation

The costs of AI integration vary widely depending on the desired outcomes and the scale of implementation. For firms seeking a comprehensive, customized AI solution, the investment can be substantial. Developing an advanced AI system may involve hiring data scientists, investing in advanced data processing infrastructure, and allocating resources for ongoing maintenance and updates. Such an endeavor can easily escalate into hundreds of thousands of euros. Deloitte serves as a prime example; by consolidating its AI initiatives into the Artificial Intelligence Center of Expertise (AICE), the firm has made a significant investment, employing hundreds of experts to drive innovation, particularly in the consulting domain.

Conversely, there are more accessible AI options available that offer robust capabilities without the hefty price tag. Off-the-shelf tools like Caseware AnalyticsAI provide powerful data analysis functions on a subscription basis, often costing just a few thousand euros annually. These solutions can automatically run extensive tests on all transactions—far beyond the capabilities of traditional sampling methods—identifying outliers and grouping items to give auditors a comprehensive risk overview. More affordable tools like ChatGPT,

available for around 20 euros per month, can assist with tasks such as drafting reports based on bullet points, though caution is advised when handling sensitive data. Typically, firms cannot simply paste clients' proprietary or confidential data into these systems, as LLMs process data externally, potentially exposing it to risks of misuse or breaches. This raises concerns regarding data security, client confidentiality, and compliance with regulatory requirements. It may be advisable to deploy LLMs within secure, private environments where data control is maintained. At the same time, also cost-efficient AI offers solutions for organizations facing confidentiality challenges by creating simulated data that mirrors real-world scenarios. This capability enables auditing professionals to perform comprehensive analyses and simulations without compromising privacy or data security.

These examples illustrate that AI integration is scalable and adaptable to various budget constraints. Firms can start with smaller investments and expand their AI capabilities as demand and resources grow.

B. Upskilling employees for an AI-enhanced future

Integrating AI into auditing is not solely about adopting new tools; it also necessitates a shift in the skill sets of auditing professionals. Employees may need to upskill to effectively utilize AI technologies, even if they do not become expert programmers. A fundamental understanding of AI and data analytics is crucial. This includes comprehending how AI systems function, the types commonly used in auditing, and recognizing both the potential outputs and limitations of these technologies. The reliance on training data and the implications of any inherent biases are critical to understand. LLMs rely on vast amounts of publicly available data, which may include outdated, biased, or inaccurate information. As a result, they can inadvertently produce outputs that reflect these limitations. This underscores the need for

A FUNDAMENTAL UNDERSTANDING OF AI AND DATA ANALYTICS IS CRUCIAL.

auditors not only to be aware of these risks but also to develop the skills necessary to critically assess AI-generated outputs.

For instance, understanding how a machine learning model identifies and predicts audit risks enables auditors to interpret results more effectively and apply them correctly. Auditors must review AI-generated insights, determine relevance, and make informed decisions. This capability is essential not only for integrating AI findings into the audit process but also for confidently explaining these findings during client negotiations. Moreover, legal responsibilities dictate that auditors cannot attribute their audit opinions solely to AI outputs; understanding the genesis of the information is a fundamental part of the job.

A recent academic study (Law and Chen, 2024) examining job postings reveals a prominent shift in the demand for auditor skills. In firms where AI is applied, there is a decreased demand for traditional software skills, such as proficiency in Excel. Simultaneously, there is an increased demand for cognitive skills or client skills. The use of AI reduces the need for routine technical tasks, allowing auditors to focus more on non-routine tasks that require human judgment and interaction. The emphasis on the human factor also mirrors the audit regulator's view. Human intervention remains critical to ensure that these outputs are properly interpreted and contextualized. Auditors must apply their professional judgment to analyze and validate AI-driven findings, as interpretation is a core component of the audit process. Without this critical layer of human expertise, AI outputs may be deemed insufficient by regulators. This reinforces the complementary nature of AI in auditing: it is a tool to enhance, not replace, the auditor's role in delivering high-

quality, regulator-compliant audit work. This shift suggests that while auditors do not need to become technical experts in AI, there is a growing space for AI in auditing.

C. Strategic implications and workforce considerations

From a strategic standpoint, the adoption of AI could help address the chronic shortage of skilled personnel in the auditing profession. By automating routine tasks, AI technologies enable existing staff to concentrate on higher-value activities, effectively expanding workforce capacity without increasing headcount. This not only helps manage personnel shortages but may also enhance job satisfaction by allowing auditors to engage in more meaningful work.

However, there are potential workforce implications to consider. In their study, Fedyk et al. (2022) suggest that investment in AI could lead to a reduction in accounting staff over time. For example, the authors observed a 7.1% decrease in accounting employees four years after an AI investment. While other factors may contribute to this reduction, the trend highlights the need to consider how AI adoption may impact staffing levels. Nonetheless, the study indicates a 5% reduction in the likelihood of a audit restatements, suggesting enhanced accuracy in information processing and potential elimination of human error.

Strategically, investing in AI is becoming less of an option and more of a necessity. The rapid evolution of AI in auditing presents significant challenges, particularly for small audit firms. While large firms often have the resources to invest in AI tools, training programs, and IT infrastructure, smaller firms may struggle to keep pace. Larger auditing firms with ample resources are quickly integrating AI, setting new industry standards. This disparity risks widening the gap in efficiency and service quality between smaller firms and their larger counterparts. Clients of smaller firms may soon expect similar efficiencies, particularly if they become aware of the advantages such as faster information processing and overall improved efficiency. Firms that fail to adopt AI risk signaling inefficiency, potentially driving clients toward competitors who have embraced the technology. On the flip side, AI can level the playing field by allowing smaller firms to compete more effectively. Affordable AI tools enable these firms to enhance their services, demonstrating to clients and the market that they are committed to staying at the forefront of industry advancements. This commitment is crucial not only for attracting and retaining clients but also for inspiring confidence among stakeholders that the firm is equipped to handle future challenges.

Professional skepticism in using AI is key

While the initial literature argued that humans are skeptical about AI and seem to have an algorithm aversion (Dietvorst et al., 2015), the mindset of people has shifted more and more toward appreciation of these algorithms. When humans are kept in the loop or when tasks are increasingly complex, they are more likely to resort to algorithms. Also, with increased literacy and the adaptability of algorithms allowing humans to adjust parameters, reliance on AI increases. Compared to the early stages of in-car navigation systems, we now fully trust these systems for guidance. This trust has grown so strong that people blindly follow directions without questioning if the guidance is correct—which can occasionally lead to unintended consequences, like driving into pedestrian lanes or restricted roads.

However, reliance is only helpful to the extent that we remain skeptical. In many cases, reliance on algorithms improves decision-making. Commerford and Ulla (2023) document that auditors propose better audit adjustments in cases of high uncertainties, particularly if algorithms are adaptable and have learning capabilities. The broader implication of this study is that reliance on algorithmic advice is contextually dependent. It is influenced by an

algorithm's features and capabilities, and it is important to understand the features of the AI to help registered auditors make better use of them.

Indeed, blindly following algorithms can be dangerous. Peters (2024) offers evidence of an automation bias—that is, auditors may use automated cues as a heuristic replacement for seeking information to the extent that it reduces their professional skepticism. In his study, Peters (2024) shows that registered auditors are less critical of structured audit tasks when they are performed by technology (which makes mistakes) than when they are performed by a colleague. With AI assistance, auditors tend to spend less time on tasks and often place blind trust in the algorithm, which leads to underperformance in the task. Also, Cardinaels and Zureich (2024) show that decision-makers are less skeptical in making difficult decisions. They rely heavily on an algorithm and offload difficult decisions to it, which can be dangerous when the algorithm lacks sufficient quality.

A notorious case where reliance on algorithms went wrong was the Dutch "toeslagen affaire" or the Dutch childcare benefit scandal (UvA, 2023). Many parents were falsely accused of fraud by the Dutch tax authorities due to discriminatory and biased algorithms. The consequences for these families were devastating. AI poses risks and is still prone to errors and biases. If the data used to train an AI system contains bias, such as stereotypes related to gender or ethnicity, AI incorporates these biases and reflects them in its decision-making.

A. Transparency and explainability of AI

The issue with AI is that, as decision-makers, we are not always aware of the data on which the AI was trained. Often, we allow algorithms to make initial decisions and trust the output without question, taking their results for granted. That is why research now starts to emphasize the role of transparency and explainability when

BLINDLY FOLLOWING ALGORITHMS CAN BE DANGEROUS.

AI is taken into action (Balasubramaniam *et al.*, 2023). Explainability, or the question "How does this work?" is a key factor in AI use.

When AI becomes more advanced, it is often hard to comprehend how AI came to a result. The whole process of going from input to output often remains a black box, sometimes even to the designers of such systems. Here is where the term explainable AI comes in (IBM, 2024). Explainable AI refers to methods and tools that make an AI model's decisions understandable and interpretable. It allows for a clear assessment of the model's impact, anticipated outcomes, and possible biases, thereby helping to evaluate its accuracy, fairness, and transparency. It is closely connected to transparency. Users should get insight into the data that is used to train the model. The role of algorithms in these models and what was considered to make predictions need to be disclosed. Openness about the capabilities, the data sources, but also the limitations and context of its use is crucial to avoid people using AI in contexts for which it is not designed. AI transparency should offer insights into the inner workings of these systems, enabling people to understand and trust how they operate so that they can apply these tools with skepticism.

AI can help auditors become more efficient, but insights into the process should still trigger sufficient skepticism so that auditors also apply sufficient human judgment in the process. We would advocate that AI be seen as a companion, which, similar to other actors, may provide advice—albeit faster, more efficiently, and more accurately. Yet, as with any actor, we should still apply our own judgment and assess whether the model's insights align with the specific context to which AI is applied.

B. Towards Audit 2.0

Once AI is in place, the auditor will receive a new role. For instance, more and more companies use advanced technologies to track their emission behavior. Firms ask their suppliers, customers, and employees to participate in tracking systems that can measure emission behavior. While the systems make use of AI and generate many statistics and insights, auditors should be skeptical about the output they generate. What rules does the algorithm use to track behavior? Does it make errors? What estimates does it use? How many people participate in these tools such that outcomes generated via AI are reliable? AI might be based on a sample of people which does not represent the true population.

As one can see, these questions raise the issue of whether or not auditors in the future also need to audit the algorithms behind AI. As organizations increasingly base their decisions on algorithms, the need to audit them becomes larger (Sandu *et al.*, 2022). It is problematic if the data used to train the algorithm is not representative of the group where the algorithm will be applied. Second, if designers cannot explain well or have to admit that they do not fully understand how algorithms work, we should maybe not put them in place. Indeed, these questions are fundamental to the new audit profession. Auditors may need to audit the training data to ensure that AI is free from bias. AI algorithms that are trained on biased data that do not represent the true population may need to be replaced. Auditors also should put checks and balances in place and talk to various stakeholders to ensure that decisions AI make are acceptable to various stakeholder groups (Oyinkansola Adelakun, 2022). Sandu *et al.* (2022) also refers to the life cycle of algorithms. Once in use, it needs to be continuously monitored and reviewed, and auditors need to question whether the algorithm or AI is still performing what it has been designed for. If new trends pop up, certain training sets are outdated, or new parameters are required, we might need to develop a new method for analyzing the problem. Implementing frameworks that include good governance of AI becomes an issue that controllers need to consider in the future, and that auditors need to check in practice.

Figure 3: Stages in the life cycle of AI (Sandu et al., 2022).

Therefore, apart from understanding the new technology, auditors need to be aware of issues like data privacy, biases, and fairness concerns of AI. They can work in close cooperation with firms and remind them about their responsibilities and obligations to be transparent about AI. They can highlight areas for improvement such that AI-driven decision-making is used in the best way to inform decision-makers.

Conclusion

AI represents a paradigm shift for the audit profession, offering tools to automate routine tasks, analyze large data sets, and detect anomalies, thereby creating new efficiencies. However, the true potential of AI in accounting lies in its partnership with human intelligence.

Registered auditors who embrace AI tools, applying them with sufficient professional skepticism and judgment, will gain unique advantages that can enhance the quality of their audits. The role of a registered auditor will have to expand as AI tools become increasingly complex. Auditors should acquaint themselves with AI and need to acquire new skills, including the audit of AI. Relatedly, auditors further need to understand issues about transparency and explainability to exploit its full advantage and secure a competitive advantage.

Samenvatting

Recente ontwikkelingen in kunstmatige intelligentie (AI) en grote taalmodellen (LLM's) bieden aanzienlijke nieuwe uitdagingen en kansen voor de accountancysector. In dit artikel bespreken we hoe AI het landschap van audits verandert. AI kan de efficiëntie van audits verbeteren door repetitieve taken te automatiseren, gegevensanalyse te verbeteren, de steekproefmogelijkheden uit te breiden, onregelmatigheden op te sporen en voorspellende inzichten te genereren. Desondanks stellen we dat professionele scepsis onmisbaar blijft wanneer auditors AI-tools gebruiken. AI-tools ondersteunen de besluitvormer, maar nemen de beslissingen zelf niet over, noch de verantwoordelijkheid voor de gevolgen daarvan. De nuances tijdens het auditproces en de interactie met klanten en collega's vereisen menselijke input. Hoewel AI bedrijfsrevisoren niet zal vervangen, moeten ze nieuwe vaardigheden ontwikkelen om audit-algoritmen effectief te evalueren en te valideren. Dit waarborgt dat AI-tools de betrouwbaarheid van besluitvorming vergroten zonder de effectiviteit te ondermijnen.

Résumé

Les progrès récents de l'intelligence artificielle (IA) et des grands modèles de langage présentent de nouveaux défis et de nouvelles opportunités pour les professionnels du chiffre. Dans cet article, nous examinons comment l'IA transforme le paysage de l'audit. Elle a le potentiel d'accroître l'efficacité des audits en automatisant les tâches répétitives, en améliorant l'analyse des données, en élargissant les capacités d'échantillonnage, en identifiant les irrégularités et en générant des informations prédictives. Cependant, nous affirmons que le scepticisme professionnel reste essentiel lorsque les auditeurs utilisent des outils d'intelligence artificielle. Certes, ces outils soutiennent le preneur de décisions, mais ils ne reprennent pas en soi la prise de décision ou la responsabilité des conséquences découlant des décisions. Les nuances apparaissant au cours du processus d'audit et l'interaction avec les clients et les collègues nécessitent l'intervention de l'homme. L'IA ne remplacera pas les réviseurs d'entreprises, mais ceux-ci doivent acquérir de nouvelles compétences pour évaluer et valider efficacement les algorithmes d'audit, en veillant à ce que les outils d'intelligence artificielle renforcent la fiabilité de la prise de décision sans en compromettre l'efficacité.

References

Balasubramaniam, N., M. Kauppinen, A. Rannisto, K. Hiekkanen, and S. Kujala. 2023. Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, 159(C), 1-15. https://doi.org/10.1016/j.infsof.2023.107197

Bhaskar, L. S., A. K. Jones, and K. Kadous. 2024. You've Got a Chatbot Friend in Me: Do Generative AI Chatbots Improve the Quality of Auditors' Voice Decisions? *Working Paper, Indiana University and Emory University*.

Cardinaels, E., S. Hollander, and B. White. 2019. Automatic summarization of earnings releases: Attributes and effects on investors' judgments. *Review of Accounting Studies,* 24(3), 860-890. https://doi.org/10.1007/s11142-019-9488-0

Cardinaels, E., and J. Zureich. 2024. Do algorithms make people harsher. *Working Paper, Tilburg University and Lehigh University*.

Christ, H., S. A. Emett, S. L. Summers, and D. A. Wood. 2021. Prepare for takeoff: improving asset measurement and audit quality with drone-enabled inventory audit procedures. *Review of Accounting Studies*, 26(4): 1323-1343. https://doi.org/10.1007/s11142-020-09574-5

Chen, C., and B. Ke. 2024. Machine Learning as a Management Control Mechanism: The Case of Employee Selection. *Working Paper, Shanghai Univeristy of Finance and Economics and National University of Singapore*. https://ssrn.com/abstract=4789953

Commerford B., and J. Ulla. 2023. Reliance On Algorithmic Estimates: The Joint Influence of Algorithm Adaptability and Measurement Uncertainty. *Working Paper, University of Illinois at Urbana-Champaign and University of Kentucky*.

CPA and AICPA. 2019. A CPA's Introduction to AI: From Algorithms to Deep Learning, What You Need to Know. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cpas-introduction-to-ai-from-algorithms.pdf

Deloitte. 2023. Deloitte Launches Innovative 'DARTbot' Internal Chatbot. https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloittelaunches-innovative-dartbot-internal-chatbot.html

Dietvorst, B. J., J. P. Simmons, and C. Massey. 2015. Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General*, 144(1): 114-126. https://doi.org/10.1037/xge0000033

Eulerich, M., A. Sanatizadeh, H. Vakilzadeh, and D. A. Wood. 2024. Is it All Hype? ChatGPT's Performance and Disruptive Potential in the Accounting and Auditing Industries. *Review of Accounting Studies*, 29(3): 2318-2349. https://doi.org/10.1007/s11142-024-09833-9

Eloundou T., S. Manning, P. Mishkin, and D. Rock. 2024. GPTs are GPTs: An early look at the labor market impact potential of large language models. *Science*, 384(6702): 1306-1308. https://doi.org/10.1126/science.adj0998

Fedyk A., J. Hodson, N. Khimich, and T. Fedyk. 2022. Is artificial intelligence improving the audit process?. *Review of Accouningt Studies*, 27(3): 938-985. https://doi.org/10.1007/s11142-022-09697-x

Frey, C. B., and M. A. Osborne. 2017. The future of employment: How susceptible are jobs to computerization? *Technological Forecasting and Social Change*, 114(C): 254-280. https://doi.org/10.1016/j.techfore.2016.08.019

Kim, A., M. Muhn, and N. Nikolaev. 2024. From Transcripts to Insights: Uncovering Corporate Risks Using Generative AI. *Working Paper, University of Chicago*. https://doi.org/10.2139/ssrn.4593660

Law, K., and M. Shen. 2024. How Does Artificial Intelligence Shape Audit Firms?. *Management Science Forthcoming*. https://doi.org/10.1287/mnsc.2022.04040

Levels, M. 2020. Hoe voorkom jij dat je werkloos wordt? https://www.universiteitvannederland.nl/college/hoe-voorkom-jij-dat-je-werkloos-wordt

Huang, F., W. Gyun, M. Vasarhelyi, and Z. Yan. 2023. Audit data analytics, machine

learning, and full population testing. *Journal of Finance and Data Science*, 8: 138-144. https://doi.org/10.1016/j.jfds.2022.05.002

IBM. 2024. Artificial intelligence (AI) solutions. https://www.ibm.com/artificial-intelligence

IBM. 2024. What is explainable AI? https://www.ibm.com/topics/explainable-ai

Medium. 2023. https://medium.com/@wengitonyegodswill/artificial-intelligence-ai-refers-to-the-development-of-computer-systems-that-can-perform-tasks-40c1a19ed53d

Oyinkansola Adelakun, B. 2022. Ethical Considerations in the Use of AI for Auditing: Balancing Innovation and Integrity. *European Journal of Accounting, Auditing and Finance Research*, 10(12): 91-108. https://doi.org/10.37745/ejaafr.2013/vol10n1291108

Peters, C. 2024. Auditor Automation Usage and Professional Skepticism. *Working Paper, Nanyang Technological University*. https://ssrn.com/abstract=4309348

Reuters. 2023. ChatGPT sets record for fastest-growing user base - analyst note. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Sandu, I., M. Wiersma, and D. Manichand. Time to audit your AI algorithms. *Maandblad voor Accountancy and Bedrijfseconomie*, 96(7/8): 253-265. https://doi.org/10.5117/mab.96.90108

UvA. 2023. The Dutch childcare benefit scandal shows that we need explainable AI rules. https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-rechtsgeleerdheid/news/2023/02/childcare-benefit-scandal-transparency.html

World Economic Forum. 2023. The Future of Jobs Report 2023. Available at: https://www.weforum.org/publications/the-future-of-jobs-report-2023/

WSJ (Wall Street Journal). 2023. EY Unveils Fruits of $1.4 Billion Artificial-Intelligence Investment. https://www.wsj.com/articles/ey-unveils-fruits-of-1-4-billion-artificialintelligence-investment-ab8d5b5a

LA GESTION DE LA SÉCURITÉ DE L'INFORMATION DANS LES BUREAUX D'AUDIT

INFORMATIEBEVEILIGINGSMANAGEMENT IN AUDITKANTOREN

AURÉLIE VAN DER PERRE

Head of Privanot et experte en protection des données et sécurité de l'information

NILS QUAIRIAT

Information Security Officer

1. Préambule

Le réviseur d'entreprises traite quotidiennement un grand volume de données et d'informations, que ce soit pour ses missions d'audit ou la gestion de sa propre organisation.

Dans un contexte de dématérialisation croissante, les risques d'atteinte à ces données et à ces informations sont de plus en plus nombreux compte tenu, entre autres, du degré de complexité des systèmes d'information et de la sophistication des méthodes utilisées par les acteurs malicieux (hackeurs, fraudeurs, etc.). Dans les cas les plus graves, les conséquences peuvent impliquer l'arrêt définitif des activités du cabinet.

1. Woord vooraf

De bedrijfsrevisor verwerkt dagelijks een grote hoeveelheid gegevens en informatie, hetzij voor zijn controleopdrachten, hetzij voor de aansturing van zijn eigen organisatie.

In een context van toenemende dematerialisatie nemen de bedreigingen voor deze gegevens en informatie meer en meer toe, onder meer gezien de mate van complexiteit van de informatiesystemen en de verfijning van de methoden die door kwaadwillende actoren (hackers, fraudeurs, enz.) worden gehanteerd. In de ernstigste gevallen kunnen de gevolgen de definitieve stopzetting van de activiteiten van het kantoor inhouden.

En outre, un certain nombre de risques liés à la protection des données peuvent influencer l'évaluation des risques définis par le système de gestion de la qualité des cabinets d'audit en application de la norme ISQM-1. Des contrôles supplémentaires doivent, le cas échéant, être mis en place au sein du système de gestion de la qualité des cabinets, dont l'organisation est impactée.

Il est par ailleurs essentiel pour le réviseur d'entreprises de gérer les risques liés à l'intégrité des données, non seulement pour l'organisation de son propre cabinet, mais aussi en raison de l'impact potentiel sur l'entité contrôlée. De tels risques peuvent en effet mettre à mal la crédibilité de l'entité lorsque les données sont utilisées dans les systèmes internes en vue, notamment, de la préparation des rapports financiers. Un jugement erroné sur l'image fidèle d'un client de premier plan pourrait également nuire à la réputation du cabinet. Dans ce contexte, on peut également se référer à la norme ISA 315 (révisée), qui exige que le réviseur d'entreprises évalue les risques liés aux technologies de l'information ; les aspects liés à la cybercriminalité et à l'intégrité des données en font partie intégrante.

L'impact potentiel de ces risques sur l'organisation du cabinet et sur l'exécution de la mission du réviseur d'entreprises soulignent l'importance de cet article qui vise à offrir au lecteur une analyse de mesures utiles qu'il peut adopter afin de mitiger les risques de cyberattaques et d'atteintes aux données à caractère personnel.

Ces mesures découlent tant des préceptes en matière de sécurité de l'information que de ceux en matière de protection des données à caractère personnel.

Daarnaast kunnen een aantal gegevensbeschermingsrisico's van invloed zijn op de inschatting van risico's die door het kwaliteitsmanagementsysteem van auditkantoren zijn gedefinieerd in toepassing van ISQM 1. Indien nodig moeten aanvullende interne beheersingsmaatregelen worden geïmplementeerd binnen het kwaliteitsmanagementsysteem van de kantoren waarvan de organisatie wordt beïnvloed.

Het is ook essentieel voor de bedrijfsrevisor om de risico's die gepaard gaan met gegevensintegriteit te beheren, niet alleen voor de organisatie van zijn eigen kantoor, maar ook als gevolg van de potentiële impact op de gecontroleerde entiteit. Dergelijke risico's kunnen immers de geloofwaardigheid van de entiteit ondermijnen wanneer de gegevens worden gebruikt in interne systemen voor onder meer het opstellen van de financiële verslagen. Een verkeerde oordeelsvorming over het getrouw beeld van een toonaangevende cliënt zou ook de reputatie van het kantoor kunnen schaden. In dit verband kan ook worden verwezen naar ISA 315 (herzien), die vereist dat de bedrijfsrevisor de risico's in verband met informatietechnologie beoordeelt; aspecten die verband houden met cybercriminaliteit en gegevensintegriteit maken er integraal deel van uit.

De potentiële impact van deze risico's op de organisatie van het kantoor en op de uitvoering van de opdracht van de bedrijfsrevisor beklemtonen het belang van dit artikel dat tot doel heeft de lezer een analyse te bieden van nuttige maatregelen die hij kan vaststellen om de risico's op cyberaanvallen en inbreuken in verband met persoonsgegevens te beperken.

Deze maatregelen vloeien voort uit zowel de voorschriften inzake informatiebeveiliging als die inzake de bescherming van persoonsgegevens.

LA SÉCURITÉ DE L'INFORMATION EST AVANT TOUT UN OUTIL PERMETTANT AU RÉVISEUR D'ENTREPRISES DE LIMITER LES RISQUES D'ATTEINTES AUX DONNÉES ET DE CYBERATTAQUES.

2. Remparts aux cyberattaques et aux atteintes aux données

A. Sécurité de l'information

La sécurité de l'information est une notion vaste définie comme étant « *la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information* »[1].

> ***Confidentialité*** *: propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, entités ou processus non autorisés*[1].
> ***Intégrité*** *: propriété selon laquelle l'information est exacte et complète*[1].
> ***Disponibilité*** *: propriété selon laquelle l'information est accessible et utilisable à la demande par une entité autorisée*[1].

Elle implique l'implémentation d'un processus de gestion des risques et l'adoption de mesures techniques et organisationnelles pour mitiger les risques identifiés. La sécurité de l'information est donc avant tout un outil permettant au réviseur d'entreprises de limiter les risques d'atteintes aux données et de cyberattaques.

1 *Traduit à partir de ISO/IEC 27000:2014 - Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*

INFORMATIEBEVEILIGING IS VOORAL EEN HULPMIDDEL WAARMEE DE BEDRIJFSREVISOR DE RISICO'S OP GEGEVENSINBREUKEN EN CYBERAANVALLEN KAN BEPERKEN.

2. Bolwerk tegen cyberaanvallen en gegevensinbreuken

A. Informatiebeveiliging

Informatiebeveiliging is een breed begrip dat wordt omschreven als zijnde *"de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie"*[1].

> ***Vertrouwelijkheid****: de eigenschap dat informatie niet wordt verspreid of vrijgegeven aan niet-gemachtigde personen, entiteiten of processen*[1].
> ***Integriteit****: de eigenschap dat de nauwkeurigheid en de volledigheid van de informatie is gewaarborgd*[1].
> ***Beschikbaarheid****: de eigenschap dat informatie op verzoek van een gemachtigde entiteit toegankelijk en bruikbaar is*[1].

Informatiebeveiliging omvat het implementeren van een risicomanagementproces en het vaststellen van technische en organisatorische maatregelen om de geïdentificeerde risico's te beperken. Informatiebeveiliging is daarom vooral een hulpmiddel waarmee de bedrijfsrevisor de risico's op gegevensinbreuken en cyberaanvallen kan beperken.

1 *Vertaald uit ISO/IEC 27000:2014 - Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Overzicht en woordenlijst.*

Parmi les références en matière de sécurité de l'information dont s'inspire le présent article, citons le standard international ISO (*International Organization for Standardization*) 27001 *« sécurité de l'information, cybersécurité et protection de la vie privée »*. Ce standard décrit les exigences d'un système de gestion de la sécurité de l'information et s'accompagne d'une liste de mesures de sécurité types. Le réviseur peut par ailleurs s'inspirer du standard américain NIST (*National Institute of Standards and Technology*) 800-53 « *security and privacy controls for information systems and organizations* », qui propose un catalogue exhaustif de mesures types. Au titre des standards de référence, nous pouvons encore citer le « *CyberFundamentals »,* établi par le *Centre for Cyber Security Belgium* (CCB), qui propose des listes de mesures concrètes adaptées au contexte de l'organisation.

B. Préceptes en matière de protection des données à caractère personnel

Par ailleurs, les traitements de données à caractère personnel sont à effectuer conformément aux principes du Règlement général sur la protection des données[2] (ci-après le RGPD) et des autres lois applicables, telles que la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[3].

Notons que les amendes pénales et administratives – en cas de non-respect des règles en vigueur relatives à la protection des données à caractère personnel – sont sévères. Ainsi, le RGPD prévoit des amendes

2 Règlement (EU) 2016/679 du 27 avril 2016 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la Directive 95/46/CE.

3 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.* 5 sept. 2018, 68616.

Een van de referenties voor informatie-beveiliging waarop dit artikel is gebaseerd, is de internationale standaard ISO (*International Organisation for Standardisation*) 27001, "*Informatiebeveiliging, cybersecurity en bescherming van de privacy*". Deze standaard beschrijft de eisen voor een management-systeem voor informatiebeveiliging en gaat vergezeld van een lijst van standaard beveiligingsmaatregelen. De bedrijfsrevisor kan zich ook laten inspireren door de Amerikaanse standaard NIST (*National Institute of Standards and Technology*) 800-53 *"Security and Privacy Controls for Information Systems and Organizations"*, die een uitgebreide reeks standaardmaatregelen aanbiedt. Tot slot kunnen wij ook de *"Cyberfundamentals"* vermelden, een referentiekader ontwikkeld door het Centrum voor Cybersecurity België (CCB), dat lijsten bevat van concrete maatregelen afgestemd op de context van de organisatie.

B. Voorschriften inzake de bescherming van persoonsgegevens

Bovendien moet de verwerking van persoonsgegevens worden uitgevoerd in overeenstemming met de beginselen van de "Algemene Verordening Gegevensbescherming"[2] (hierna "de GDPR") en andere toepasselijke wetten, zoals de wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens[3].

Er dient te worden opgemerkt dat de strafrechtelijke en administratieve geldboeten – in geval van niet-naleving van de geldende regels inzake de bescherming van persoonsgegevens – streng zijn. Zo voorziet

2 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

3 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018, 68616.

administratives pouvant s'élever jusqu'à 10.000.000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

C. Mesures complémentaires

La sécurité de l'information prévoit des mesures qui tendent au respect des normes, lois et régulations précitées. Le RGPD a érigé l'intégrité et la confidentialité des données à caractère personnel en principes essentiels à la protection des données (art. 5.1, f) RGPD) et impose la mise en place de mesures de sécurité techniques et organisationnelles adaptées aux risques d'atteintes aux données à caractère personnel (art. 32 RGPD). Plus le risque d'atteintes à la confidentialité et à l'intégrité des données à caractère personnel est élevé, en raison par exemple de leur utilité concrète dans le cadre de fraudes, plus les mesures de protection à adopter sont strictes.

Les mesures qui découlent de la sécurité de l'information et de la protection des données à caractère personnel sont tout à fait complémentaires.

Une liste de mesures nécessaires afin de limiter le risque de cyberattaques et d'atteintes aux données à caractère personnel est repris dans le chapitre suivant. En fonction du contexte, de la taille et de la maturité de l'organisation, toutes les mesures ou seulement certaines d'entre elles sont à mettre en œuvre. Le réviseur d'entreprises qui le souhaite pourrait également en appliquer d'autres et, potentiellement, tendre vers la certification à un standard tel qu'ISO 27001, suite à un audit réalisé par un organisme indépendant.

3. Mesures techniques et organisationnelles

Certaines mesures de sécurité organisationnelles impliquent des aspects

de GDPR in administratieve geldboeten tot 10.000.000 EUR of, voor een onderneming, tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

C. Aanvullende maatregelen

Informatiebeveiliging voorziet in maatregelen gericht op naleving van voornoemde normen, wet- en regelgeving. De GDPR heeft de integriteit en vertrouwelijkheid van persoonsgegevens vastgelegd als essentiële beginselen voor gegevensbescherming (art. 5.1, f) GDPR) en vereist de implementatie van technische en organisatorische beveiligingsmaatregelen afgestemd op de risico's op inbreuken in verband met persoonsgegevens (art. 32 GDPR). Hoe hoger het risico op inbreuken op de vertrouwelijkheid en integriteit van persoonsgegevens, bijvoorbeeld vanwege de praktische bruikbaarheid ervan in het kader van fraude, hoe strenger de vast te stellen beschermingsmaatregelen.

Maatregelen die voortvloeien uit informatiebeveiliging en de bescherming van persoonsgegevens zijn volkomen complementair.

In het volgende punt worden de maatregelen uiteengezet die nodig zijn om het risico op cyberaanvallen en inbreuken in verband met persoonsgegevens te beperken. Afhankelijk van de context, omvang en maturiteitsgraad van de organisatie moeten alle of slechts sommige van deze maatregelen worden uitgevoerd. De bedrijfsrevisor die dat wenst, kan ook andere maatregelen toepassen en eventueel toewerken naar certificering volgens een standaard zoals ISO 27001, na een audit uitgevoerd door een onafhankelijke instantie.

3. Technische en organisatorische maatregelen

Sommige organisatorische beveiligingsmaatregelen omvatten technische aspecten

techniques et, inversement, des mesures de sécurité techniques peuvent nécessiter la prise en compte d'aspects organisationnels. Afin de faciliter la lecture, le présent article propose une division simplifiée des mesures de sécurité. À titre d'exemple, le contrôle d'accès et le principe du moindre privilège (voir *infra*) ne se limitent pas à l'implémentation technique des droits d'accès et des privilèges au niveau de la configuration du système d'information. Ils incluent également la vérification que les octrois sont adéquats ainsi qu'une réévaluation régulière de ces derniers.

A. Mesures organisationnelles

1- Politique de sécurité de l'information

Par souci d'une gouvernance optimale de la sécurité de l'information au sein de son cabinet, le réviseur d'entreprises documente formellement les règles et le contexte de la sécurité de son organisation. Le document décrit l'objectif, les rôles et responsabilités, le champ d'application de la politique ainsi que les mesures prévues par l'organisation, telles que celles décrites dans cet article.

La politique est communiquée au sein de l'organisation. Elle est revue de manière régulière ou lors de changement significatif. Elle sert de pierre angulaire pour assurer la protection des données et la conformité au sein de l'organisation.

2- Gestion des risques et évaluation du niveau de risque

Les normes relatives à la sécurité de l'information impliquent pour le réviseur d'entreprises d'évaluer le risque en cas d'atteinte à la confidentialité, à l'intégrité et/ou à la disponibilité des données/informations traitées par son cabinet. Cette évaluation couvre notamment les risques inhérents aux traitements de données à caractère

en omgekeerd kunnen technische beveiligingsmaatregelen vereisen dat rekening wordt gehouden met organisatorische aspecten. Voor het leesgemak wordt in dit artikel een vereenvoudigde indeling van beveiligingsmaatregelen voorgesteld. Toegangscontrole en het beginsel van het minste voorrecht *(cf. infra)* zijn bijvoorbeeld niet beperkt tot de technische implementatie van toegangsrechten en voorrechten op het niveau van de configuratie van het informatiesysteem. Deze omvatten ook het controleren of de toekenningen adequaat zijn en het regelmatig herbeoordelen ervan.

A. Organisatorische maatregelen

1- Informatiebeveiligingsbeleid

Ten behoeve van een optimale governance van informatiebeveiliging binnen zijn kantoor documenteert de bedrijfsrevisor formeel de regels en de context van de beveiliging van zijn organisatie. Het document beschrijft de doelstelling, de rollen en verantwoordelijkheden, de reikwijdte van het beleid en de door de organisatie geplande maatregelen, zoals deze beschreven in dit artikel.

Het beleid wordt binnen de organisatie gecommuniceerd. Het wordt op gezette tijdstippen of tijdens significante wijzigingen beoordeeld. Het dient als een hoeksteen voor het waarborgen van gegevensbescherming en naleving binnen de organisatie.

2- Risicomanagement en beoordeling van het risiconiveau

Informatiebeveiligingsnormen houden in dat de bedrijfsrevisor het risico beoordeelt in het geval van een inbreuk op de vertrouwelijkheid, integriteit en/of beschikbaarheid van de door zijn kantoor verwerkte gegevens/informatie. Deze beoordeling heeft meer bepaald betrekking op de risico's die inherent zijn aan de verwerking van persoonsgegevens (*cf.*

personnel (cf. art. 32. 2. du RGPD). Le risque de violation de données, que celui-ci soit accidentel ou intentionnel, doit être pris en compte. Les mesures de sécurité techniques et organisationnelles sont dites adéquates lorsqu'elles sont adoptées en fonction du niveau de risque identifié pour les informations et données. Le risque doit être maintenu sous un seuil acceptable.

Par exemple, si le réviseur place dans son cabinet des caméras connectées dont il peut consulter les images depuis internet, il augmente le risque d'intrusion sur son réseau et donc, par conséquent, de violation de données. Il prend donc des mesures liées à ce traitement, telles que l'installation régulière des mises à jour de sécurité de l'équipement (cf. *infra*).

Les organismes qui accèdent à des sources de données fédérales ou qui utilisent le numéro d'identification du registre national sont, en outre, tenus de prendre des mesures supplémentaires[4] comme par exemple la désignation d'un délégué à la protection des données (DPO, *Data Protection Officer*).

L'évaluation des risques, y compris l'identification de nouveaux risques ou le changement du niveau des risques préalablement identifiés, se fait en continu et, en particulier, en cas de changements significatifs dans l'organisation tel que le changement de l'infrastructure informatique.

3- Gestion des incidents de sécurité de l'information

Le réviseur d'entreprises met en place une procédure de gestion des incidents ou un *breach response plan*. La procédure décrit comment détecter rapidement les incidents, fournir une réponse efficace pour limiter leurs impacts, documenter et analyser les causes

4 *Cf.* de manière non-exhaustive la loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.* 21 avril 1984, 5247.

art. 32.2. GDPR). Er moet rekening worden gehouden met het risico op gegevensinbreuk, hetzij per ongeluk of opzettelijk. Technische en organisatorische beveiligingsmaatregelen worden passend geacht wanneer zij worden vastgesteld op basis van het geïdentificeerde risiconiveau voor de informatie en gegevens. Het risico moet onder een aanvaardbare drempel worden gehouden.

Als de bedrijfsrevisor bijvoorbeeld in zijn kantoor verbonden camera's plaatst waarvan hij de beelden via internet kan bekijken, verhoogt hij het risico op inbraak op zijn netwerk en dus op gegevensinbreuk. Daarom treft hij maatregelen in verband met deze verwerking, zoals het regelmatig installeren van beveiligingsupdates voor de apparatuur (*cf. infra*).

Instanties die toegang hebben tot federale gegevensbronnen of het identificatienummer van het Rijksregister gebruiken, zijn bovendien verplicht om verdere maatregelen[4] te treffen, zoals het aanstellen van een functionaris voor gegevensbescherming (DPO, *Data Protection Officer*).

Risicobeoordeling, inclusief de identificatie van nieuwe risico's of de verandering in het niveau van eerder geïdentificeerde risico's, wordt continu uitgevoerd en, in het bijzonder, in het geval van significante veranderingen in de organisatie, zoals de verandering in de IT-infrastructuur.

3- Beheer van informatiebeveiligingsincidenten

De bedrijfsrevisor implementeert een *incident management procedure* of een *breach response plan* (inbreukresponsplan). De procedure beschrijft de wijze waarop incidenten snel kunnen worden gedetecteerd, een effectieve reactie kan worden geboden om hun impact te beperken, de oorzaken en

4 *Cf.* onder meer de wet van 8 augustus 1983 tot regeling van een Rijksregister van natuurlijke personen, *BS* 21 april 1984, 5247.

et conséquences et, le cas échéant, veiller au rétablissement des services impactés. Les rôles et responsabilités liés aux incidents sont définis. Par exemple, un point de contact interne unique à l'organisation (comme une boite e-mail partagée) peut y être indiqué et communiqué au personnel afin que chaque incident soit signalé de manière centralisée, facilitant ainsi la gestion et le suivi des incidents par la personne ou l'équipe responsable.

En cas d'incident, il est également recommandé de consulter la police d'assurances du cabinet, de prendre contact avec son DPO ou avec son responsable des systèmes de sécurité de l'information et, dans les cas les plus graves, avec la police.

Lorsqu'un incident provoque une violation de données à caractère personnel au sens du RGPD, une analyse des risques d'atteintes aux droits et libertés des personnes concernées doit être effectuée. Une notification à l'Autorité de protection des données s'avèrera obligatoire si un risque a été identifié (art. 33 RGPD). De même, une notification à l'égard des personnes concernées sera requise si le risque a été jugé élevé (art. 34 RGPD). Une méthodologie d'évaluation du niveau de risque est mise en place afin de rendre cette analyse la plus objective possible. Le réviseur peut se tourner, par exemple, vers les *Recommendations for a methodology of the assessment of severity of personal data breaches*[5] de l'ENISA (*European Union Agency for Cybersecurity*) pour guidance.

5 Autorités de protection des données de Grèce et Allemagne, *Recommendations for a methodology of the assessment of severity of personal data breaches, – Auteurs : Clara Galan Manso, ENISA, Sławomir Górniak, ENISA – 20 décembre 2013, https*://www.enisa.europa.eu/publications/dbn-severity

gevolgen kunnen worden gedocumenteerd en geanalyseerd en, indien nodig, het herstel van de getroffen diensten kan worden gewaarborgd. De rollen en verantwoordelijkheden in verband met incidenten worden vastgelegd. Er kan bijvoorbeeld een intern centraal contactpunt binnen de organisatie (zoals een gedeelde e-mailbox) worden aangegeven en gecommuniceerd naar het personeel, zodat elk incident centraal wordt gemeld, waardoor het managen en monitoren van incidenten door de verantwoordelijke persoon of het team wordt vergemakkelijkt.

In geval van een incident is het ook raadzaam om de verzekeringspolis van het kantoor te raadplegen, contact op te nemen met de DPO of met de verantwoordelijke persoon voor de informatiebeveiligingssystemen en, in de meest ernstige gevallen, met de politie.

Wanneer een incident leidt tot een inbreuk in verband met persoonsgegevens in de zin van de GDPR, dient een analyse te worden gemaakt van de risico's op inbreuken op de rechten en vrijheden van betrokkenen. Een melding aan de Gegevensbeschermingsautoriteit zal verplicht zijn indien een risico is geïdentificeerd (art. 33 GDPR). Evenzo zal een melding aan de betrokkenen vereist zijn als het risico hoog werd geacht (art. 34 GDPR). Om deze analyse zo objectief mogelijk te maken, wordt een methodologie voor de beoordeling van het risiconiveau ontwikkeld. De bedrijfsrevisor kan bijvoorbeeld de *Recommendations for a methodology of the assessment of severity of personal data breaches*[5] van ENISA (Agentschap van de Europese Unie voor cyberbeveiliging) raadplegen als leidraad.

5 Gegevensbeschermingsautoriteiten van Griekenland en Duitsland, *Recommendations for a methodology of the assessment of severity of personal data breaches, – Auteurs: Clara Galan Manso, ENISA, Sławomir Górniak, ENISA – 20 december 2013, https*://www.enisa.europa.eu/publications/dbn-severity.

Violation de données à caractère personnel : *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (art. 4, al. 1er, 12) RGPD).*

Inbreuk in verband met persoonsgegevens*: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (art. 4, eerste lid, 12) GDPR).*

4- Contrats

Le réviseur d'entreprises prend des mesures à l'égard de son sous-traitant. Il s'assure que le contrat qui le lie à celui-ci contient des mesures à l'égard des collaborateurs de celui-ci ou à l'égard du sous-traitant lui-même s'il agit en tant que consultant indépendant (cf. art. 32.4 RGPD).

5- Instructions à l'égard des personnes physiques agissant sous son autorité

Le réviseur d'entreprises donne des instructions par rapport à la sécurité et à la protection des données aux personnes qui agissent sous son autorité (cf. art. 32.4 RGPD). À titre d'exemples, les instructions suivantes peuvent être imposées :

- les accès aux données ne sont autorisés que dans les circonstances où cela s'avère indispensable à l'exercice des missions professionnelles du collaborateur ;
- les données ne peuvent être utilisées, copiées, reproduites sous aucune forme et ne peuvent être communiquées à autrui que lorsque cela s'avère strictement nécessaire à la réalisation des missions professionnelles du collaborateur ;
- en cas de doute, des précisions sont demandées auprès du réviseur d'entreprises ;
- la confidentialité des données traitées doit être garantie ;
- aucune donnée confidentielle n'est conservée en local (sur le disque dur de l'ordinateur) sauf si cela s'avère strictement

4- Overeenkomsten

De bedrijfsrevisor treft maatregelen ten aanzien van zijn verwerker. Hij vergewist zich ervan dat de overeenkomst die hem aan de verwerker bindt maatregelen bevat ten aanzien van de medewerkers van de verwerker of ten aanzien van de verwerker zelf indien hij optreedt als onafhankelijk adviseur (*cf.* art. 32.4 GDPR).

5- Instructies ten aanzien van de natuurlijke personen die onder zijn gezag handelen

De bedrijfsrevisor geeft instructies met betrekking tot gegevensbeveiliging en -bescherming aan de personen die onder zijn gezag handelen (*cf.* art. 32.4 GDPR). Bij wijze van voorbeeld kunnen de volgende instructies worden opgelegd:

- de toegang tot de gegevens is enkel toegelaten in omstandigheden waarin dit noodzakelijk is voor de uitvoering van de beroepstaken van de medewerker;
- de gegevens mogen enkel gebruikt, gekopieerd of in enige vorm gereproduceerd worden en mogen enkel aan anderen medegedeeld worden wanneer dat strikt noodzakelijk blijkt voor de uitvoering van de beroepstaken van de medewerker;
- in geval van twijfel worden bijzonderheden gevraagd bij de bedrijfsrevisor;
- de vertrouwelijkheid van de verwerkte gegevens moet worden gewaarborgd;
- geen enkel vertrouwelijk gegeven wordt ter plaatse bewaard (op de harde schijf van de computer), tenzij dit strikt noodzakelijk blijkt

DES RÈGLES PARTICULIÈRES PEUVENT ÊTRE PRÉCISÉES DANS UNE PROCÉDURE D'UTILISATION DE L'INTERNET EN GÉNÉRAL, DE LA MESSAGERIE ÉLECTRONIQUE OU D'OUTILS TELS QUE LES TRADUCTEURS AUTOMATIQUES OU L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE.

SPECIFIEKE REGELS KUNNEN WORDEN GESPECIFICEERD IN EEN PROCEDURE VOOR HET GEBRUIK VAN INTERNET IN HET ALGEMEEN, E-MAILS OF HULPMIDDELEN ZOALS AUTOMATISCHE VERTALERS OF GENERATIEVE KUNSTMATIGE INTELLIGENTIE.

nécessaire à l'accomplissement de la mission professionnelle du collaborateur ;
- aucune donnée confidentielle n'est enregistrée sur un support mobile (clé USB, PC portable, tablette, etc.), sauf si cela s'avère strictement nécessaire à l'accomplissement de la mission professionnelle du collaborateur, et/ou si elles sont préalablement chiffrées.

Des règles particulières peuvent être précisées dans une procédure d'utilisation de l'internet en général, de la messagerie électronique ou d'outils tels que les traducteurs automatiques ou l'intelligence artificielle générative.

6- Sensibilisation du personnel

Le réviseur d'entreprises sensibilise ses collaborateurs internes et externes aux concepts et bonnes pratiques en matière de sécurité de l'information et de protection des données à caractère personnel. À cette occasion, les instructions précitées sont expliquées en des termes simples.

D'autres matières sont utilement présentées telles que l'ingénierie sociale et en particulier l'hameçonnage (ci-après « *phishing* »), la bonne gestion des mots de passe ou les réflexes à adopter dans des circonstances particulières telles que la découverte d'une clé USB suspecte ou l'accueil d'un client dans un lieu non surveillé.

voor het vervullen van de beroepstaak van de medewerker;
- geen enkel vertrouwelijk gegeven wordt opgeslagen op een mobiele drager (USB-stick, laptop, tablet, enz.), tenzij dit strikt noodzakelijk blijkt voor het vervullen van de beroepstaak van de medewerker, en/of de gegevens vooraf zijn versleuteld.

Specifieke regels kunnen worden gespecificeerd in een procedure voor het gebruik van internet in het algemeen, e-mails of hulpmiddelen zoals automatische vertalers of generatieve kunstmatige intelligentie.

6- Sensibilisering van het personeel

De bedrijfsrevisor maakt zijn interne en externe medewerkers bewust van de concepten en goede praktijken op het gebied van informatiebeveiliging en de bescherming van persoonsgegevens. Bij deze gelegenheid worden voornoemde instructies in eenvoudige bewoordingen toegelicht.

Andere onderwerpen worden op nuttige wijze gepresenteerd, zoals *social engineering* en in het bijzonder phishing, goed wachtwoord-beheer of de reflexen die moeten worden toegepast in specifieke omstandigheden zoals het ontdekken van een verdachte USB-sleutel of het ontvangen van een cliënt op een onbewaakte locatie.

Idéalement, la sensibilisation est continue. Notons que certains logiciels offrent la possibilité de sensibiliser le personnel par l'envoi de simulations d'emails de *phishing* et par la diffusion de courtes sessions de sensibilisation de quelques minutes à échéance régulière.

Ingénierie sociale – L'ingénierie sociale, telle que définie au sens de cet article et à ne pas confondre avec un « Master en Ingénierie et Action sociales », est une activité malicieuse impliquant des interactions humaines et des manipulations psychologiques, dans le but d'obtenir de l'information (telle que des mots de passe ou des données sensibles) ou de faire commettre une erreur de sécurité (telle que l'installation de logiciels malveillants ou l'ouverture d'une porte menant à une zone sécurisée pour une personne non autorisée). Elle se manifeste très souvent sous la forme d'attaque par *phishing*, où un email malveillant pousse la victime à la faute.

Dans le cadre de la mise en œuvre d'ISQM-1 au sein d'un cabinet d'audit, on pourrait s'attendre à ce qu'une politique et des procédures pertinentes – parfois complexes – soient établies et communiquées aux collaborateurs.

7- Utilisation du matériel informatique du cabinet

Le réviseur d'entreprises veille à ce que les membres du personnel utilisent exclusivement le matériel fourni par l'organisation, y compris en cas de télétravail. L'organisation maintient alors le contrôle sur les flux de données et limite les risques d'intrusion qu'implique l'usage d'appareils en dehors du contrôle de l'organisation.

Les systèmes traitant les données et informations de l'organisation ne sont par ailleurs accessibles que par des appareils

In het ideale geval gebeurt de sensibilisering continu. Er dient te worden opgemerkt dat sommige software de mogelijkheid biedt om het personeel te sensibiliseren door gesimuleerde phishing e-mails te versturen en door regelmatig korte bewustmakingssessies van enkele minuten uit te zenden.

Social engineering – *Social engineering*, zoals gedefinieerd in dit artikel en niet te verwarren met een "*Master in Social Engineering and Action*", is een kwaadaardige activiteit waarbij menselijke interactie en psychologische manipulatie een rol spelen, met als doel informatie te verkrijgen (zoals wachtwoorden of gevoelige gegevens) of een beveiligingsfout te veroorzaken (zoals het installeren van malware of het openen van een deur naar een beveiligde zone voor een niet-gemachtigde persoon).
Dit manifesteert zich heel vaak in de vorm van een phishingaanval, waarbij een kwaadaardige e-mail het slachtoffer ertoe aanzet de fout te maken.

Als onderdeel van de implementatie van ISQM-1 binnen een auditkantoor zou men kunnen verwachten dat relevante – soms complexe – beleidslijnen en procedures worden opgesteld en medegedeeld aan de medewerkers.

7- Gebruik van het informaticamateriaal van het kantoor

De bedrijfsrevisor ziet erop toe dat de personeelsleden uitsluitend gebruikmaken van de door de organisatie ter beschikking gestelde hardware, ook in geval van telewerken. De organisatie behoudt zo de controle over de gegevensstromen en beperkt de risico's op inbraak die gepaard gaan met het gebruik van apparatuur die buiten de controle van de organisatie valt.

De systemen die de gegevens en informatie van de organisatie verwerken, zijn bovendien alleen toegankelijk met apparatuur die technisch

techniquement sous son contrôle, par exemple en installant un certificat sur les ordinateurs fournis aux membres du personnel, ce qui permet de vérifier techniquement l'origine de diverses requêtes. Ces mesures permettent de bloquer l'accès aux données et aux informations à un pirate informatique qui se serait emparé du compte d'un utilisateur.

8- Protection physique de la salle serveur

Si le réviseur d'entreprises dispose de son propre serveur au sein de son cabinet, il prend les mesures suivantes :

- l'accès à la salle serveur est sécurisé ou, si le serveur est dans une armoire dédiée, celle-ci est fermée à clé ;
- une alimentation électrique de secours est couplée au serveur ;
- un détecteur d'incendie ou de fumée est placé à proximité du serveur ;
- la salle (ou le rack) est suffisamment ventilé(e) ;
- si le serveur est au rez-de-chaussée ou dans un étage inférieur, des mesures réduisant l'impact d'une inondation sont prises. Par exemple, le serveur n'est pas installé sur le sol et une pompe à eau est prévue dans la pièce.

9- Destruction sécurisée du matériel informatique

Faire don de matériel usagé sans prendre les mesures de sécurité adéquates, même si l'initiative est louable, peut être à l'origine d'une violation de données à caractère personnel.

Détruire physiquement un disque dur permet de mitiger les risques de violation. Si un réviseur d'entreprises souhaite réutiliser ou donner du matériel usagé, il s'assure que les données ont été effacées à l'aide d'une technique appropriée, par exemple via l'intermédiaire de son fournisseur informatique. Il est par ailleurs

onder de controle van de organisatie staat, bijvoorbeeld door een certificaat te installeren op de computers die aan de personeelsleden worden verstrekt, waardoor het mogelijk is om de oorsprong van verschillende verzoeken technisch te verifiëren. Deze maatregelen maken het mogelijk om de toegang tot gegevens en informatie te blokkeren voor een hacker die een gebruikersaccount zou hebben overgenomen.

8- Fysieke beveiliging van de serverruimte

Indien de bedrijfsrevisor binnen zijn kantoor over een eigen server beschikt, treft hij de volgende maatregelen:

- de toegang tot de serverruimte is beveiligd of, als de server zich in een specifiek daarvoor bestemde kast bevindt, is deze vergrendeld;
- een noodstroomvoorziening is gekoppeld aan de server;
- een brand- of rookmelder is in de buurt van de server geplaatst;
- de serverruimte (of het serverrack) is voldoende geventileerd;
- als de server zich op de begane grond of op een lagere verdieping bevindt, worden er maatregelen getroffen om de impact van een overstroming te beperken. De server is bijvoorbeeld niet op de vloer geïnstalleerd en er is een waterpomp voorzien in de ruimte.

9- Beveiligde vernietiging van hardware

Het doneren van gebruikte hardware zonder passende beveiligingsmaatregelen te treffen, zelfs als het initiatief prijzenswaardig is, kan de oorzaak zijn van een inbreuk in verband met persoonsgegevens.

Het fysiek vernietigen van een harde schijf biedt de mogelijkheid om de risico's op een inbreuk te beperken. Als een bedrijfsrevisor gebruikte hardware wil hergebruiken of doneren, zorgt hij ervoor dat de gegevens met behulp van een geschikte techniek zijn gewist, bijvoorbeeld via zijn IT-provider. Het wordt ook aanbevolen om

DÉTRUIRE PHYSIQUEMENT UN DISQUE DUR PERMET DE MITIGER LES RISQUES DE VIOLATION. SI UN RÉVISEUR D'ENTREPRISES SOUHAITE RÉUTILISER OU DONNER DU MATÉRIEL USAGÉ, IL S'ASSURE QUE LES DONNÉES ONT ÉTÉ EFFACÉES À L'AIDE D'UNE TECHNIQUE APPROPRIÉE, PAR EXEMPLE VIA L'INTERMÉDIAIRE DE SON FOURNISSEUR INFORMATIQUE.

HET FYSIEK VERNIETIGEN VAN EEN HARDE SCHIJF BIEDT DE MOGELIJKHEID OM DE RISICO'S OP EEN INBREUK TE BEPERKEN. ALS EEN BEDRIJFSREVISOR GEBRUIKTE HARDWARE WIL HERGEBRUIKEN OF DONEREN, ZORGT HIJ ERVOOR DAT DE GEGEVENS MET BEHULP VAN EEN GESCHIKTE TECHNIEK ZIJN GEWIST, BIJVOORBEELD VIA ZIJN IT-LEVERANCIER.

recommandé de garder la preuve de l'acte de destruction du matériel informatique ou des données qui y sont contenues afin d'éviter toute mise en cause de la responsabilité du réviseur d'entreprises. Il y a lieu de garder à l'esprit que supprimer un fichier informatique et/ou vider la corbeille de l'ordinateur n'implique en aucune manière la suppression des données du disque et qu'un simple formatage rapide ne rend pas la récupération des données impossible. Des programmes dédiés existent pour effacer les données de manière exhaustive.

B. Mesures techniques

1- Backups

Le réviseur d'entreprises veille à ce que les données et informations critiques soient sauvegardées de manière régulière. Effectivement, en cas de défaillance de disques durs, de désastre environnemental, ou d'attaque de type *ransomware*, les backups feront office de filet de secours ultime afin de rétablir les opérations du cabinet.

het bewijs van de daad van vernietiging van de hardware of de daarin opgenomen gegevens te bewaren om elke aansprakelijkheidsstelling van de bedrijfsrevisor te voorkomen. Er moet rekening mee worden gehouden dat het verwijderen van een elektronisch bestand en/of het leegmaken van de prullenbak van de computer geenszins inhoudt dat de gegevens van de schijf worden verwijderd en dat een eenvoudige snelle formattering gegevensherstel niet onmogelijk maakt. Er bestaan speciale programma's om gegevens volledig te wissen.

B. Technische maatregelen

1- Back-ups

De bedrijfsrevisor ziet erop toe dat regelmatig een back-up wordt gemaakt van kritische gegevens en informatie. In het geval van een harde schijf-storing, een milieuramp of een *ransomware*-aanval, zullen back-ups immers fungeren als het ultieme vangnet om de transacties van het kantoor te herstellen.

Ransomware – un *ransomware*, *cryptolocker* ou encore *rançongiciel* est un logiciel malveillant utilisé par des acteurs malicieux afin de chiffrer les données d'une organisation, la mettant à l'arrêt. Les criminels demandent ensuite une large somme d'argent en échange des clés de déchiffrement, prenant ainsi l'organisation en otage. Typiquement, les criminels exfiltrent également toutes les données compromises, et menacent de les publier sur internet en cas de non-paiement. Une bonne gestion des backups permet de remettre son organisation sur pied en cas d'attaque de ce type. Il est toujours recommandé de ne jamais céder à ce genre de chantage, le paiement n'offrant aucune garantie et incitant les criminels à reproduire leurs actions répréhensibles.

Le réviseur veille à ce que les backups soient correctement sécurisés :

- les backups sont chiffrés. Ainsi, en cas de compromission du système hôte des backups, la fuite de données est limitée ;

- les backups sont soit *offline*, soit immutables. En stockant ses backups *offline*, c'est-à-dire sur un support déconnecté de tout réseau informatique, les backups sont hors de portée d'un hackeur qui essaierait de les effacer ou de les chiffrer dans le cadre d'une attaque de type *ransomware*, afin de forcer l'organisation à effectuer le paiement. Si les backups ne sont pas *offline*, il est également acceptable de les rendre immutables, c'est-à-dire qu'il est possible de les créer et de les lire, mais pas de les modifier ou de les effacer. La majorité des services de backups dans le cloud disposent de cette fonctionnalité ;

- les backups sont délocalisés. Ainsi, en cas de désastre environnemental, tel qu'un incendie dans la salle serveur, les backups peuvent encore être récupérés ;
- la restauration des backups est testée régulièrement, typiquement une fois par an.

Ransomware – een *ransomware* of *cryptolocker* is een malware die door kwaadwillende actoren wordt gebruikt om de gegevens van een organisatie te versleutelen, waardoor deze stil komt te liggen. De criminelen eisen vervolgens een grote som geld in ruil voor de decoderingssleutels, waardoor de organisatie gegijzeld wordt. Meestal exfiltreren de criminelen ook alle gecompromitteerde gegevens en dreigen ze deze op internet te publiceren in geval van niet-betaling. Goed back-upbeheer maakt het mogelijk om uw organisatie weer op de been te krijgen in geval van een dergelijke aanval. Het wordt altijd aanbevolen om nooit toe te geven aan dit soort chantage, omdat betaling geen garantie biedt en criminelen aanmoedigt om hun verwerpelijke acties te herhalen.

De bedrijfsrevisor ziet erop toe dat de back-ups goed beveiligd zijn:

- de back-ups zijn versleuteld. Dit betekent dat in geval van compromittering van het back-up hostsysteem, het lekken van gegevens wordt beperkt;
- de back-ups zijn hetzij offline, hetzij onveranderlijk. Door de back-ups offline op te slaan, d.w.z. op een medium dat is losgekoppeld van een computernetwerk, zijn de back-ups buiten het bereik van een hacker die, in het kader van een *ransomware*-aanval, zou proberen ze te wissen of te versleutelen teneinde de organisatie te dwingen de betaling uit te voeren. Als de back-ups niet offline zijn, is het ook aanvaardbaar om ze onveranderlijk te maken, d.w.z. dat het mogelijk is om ze te maken en te lezen, maar niet om ze te wijzigen of te verwijderen. De meeste cloudback-updiensten hebben deze functionaliteit;
- de back-ups worden verplaatst. Zo kunnen de back-ups bij een milieuramp, zoals een brand in de serverruimte, alsnog worden teruggehaald;
- back-upherstel wordt regelmatig getest, meestal één keer per jaar. Deze tests maken

Ces tests permettent de s'assurer de leur bon fonctionnement en cas de besoin ;
- des notifications régulières sont envoyées afin de confirmer la réussite ou l'échec des backups et de détecter les erreurs le plus tôt possible. Alternativement, un monitoring est mis en place par le fournisseur IT ;
- si les backups contiennent des données à caractère personnel, ils sont stockés de préférence dans l'Espace économique européen et, dans la mesure du possible, auprès d'une société dont la souveraineté est européenne, afin de faciliter la conformité au RGPD.

2- Contrôle d'accès

Le réviseur d'entreprises veille à ce que les accès aux données et informations de son organisation ne soient octroyés qu'aux personnes autorisées. Ce contrôle d'accès inclut l'utilisation de comptes nominatifs authentifiés de manière forte (idéalement à l'aide d'une authentification à facteurs multiples). Les accès sont liés à des personnes ou à des groupes et sont revus à intervalles réguliers (typiquement, une fois par an).

Le réviseur utilise le principe du *need-to-know*, c'est-à-dire que les utilisateurs ont uniquement accès aux données dont ils ont besoin pour pouvoir exercer leurs fonctions.

het mogelijk om de goede werking ervan te garanderen in geval van nood;
- regelmatige meldingen worden verzonden om het succes of falen van back-ups te bevestigen en om fouten zo vroeg mogelijk op te sporen. Als alternatief wordt monitoring opgezet door de IT-provider;
- als de back-ups persoonsgegevens bevatten, worden deze bij voorkeur opgeslagen in de Europese Economisch Ruimte en, voor zover mogelijk, bij een vennootschap met Europese soevereiniteit, om de naleving van de GDPR te vergemakkelijken.

2- Toegangscontrole

De bedrijfsrevisor ziet erop toe dat alleen bevoegde personen toegang krijgen tot de gegevens en informatie van zijn organisatie. Deze toegangscontrole omvat het gebruik van sterk geverifieerde accounts op naam (in het ideale geval met behulp van multifactor-authenticatie). De toegang is gekoppeld aan personen of groepen en wordt op geregelde tijdstippen (meestal eenmaal per jaar) beoordeeld.

De bedrijfsrevisor hanteert het *"need-to-know"*-beginsel, wat betekent dat gebruikers alleen toegang hebben tot de gegevens die ze nodig hebben om hun functies te kunnen uitvoeren.

Authentification à facteurs multiples *– souvent abrégé en MFA est un processus de sécurité qui nécessite plusieurs facteurs de vérification pour prouver l'identité d'un utilisateur de manière suffisante.*
La MFA combine des informations sur ce que l'utilisateur sait, comme un mot de passe, mais aussi sur un facteur supplémentaire, tel que ce qu'il possède, comme un smartphone, qu'il peut typiquement utiliser pour valider l'ouverture d'une session ou obtenir un code d'authentification unique. Ainsi, un acteur malicieux disposant uniquement du mot de passe d'une victime ne pourra pas s'authentifier en son nom si la MFA est activée.
Cette mesure présente malgré tout quelques limites. Effectivement, des attaques de phishing plus avancées et de plus en plus courantes contournent ce type de protection. La MFA permet malgré tout d'éviter un grand nombre de violations de données.

3- Principe du moindre privilège

Le réviseur d'entreprises implémente le principe du moindre privilège, c'est-à-dire que les membres du personnel disposent du niveau de droits minimum nécessaire à l'exercice de leurs fonctions.

À titre d'exemples :
- les membres du personnel ont uniquement un accès en lecture seule pour les documents et dossiers qu'ils ne devront pas modifier ni supprimer ;
- les membres du personnel ne disposent pas des droits d'administrateur local de leur machine, ce qui réduit considérablement les risques d'installation de logiciels malveillants. Si, pour une raison quelconque, les droits d'administrateur local sont nécessaires, ceux-ci sont utilisés uniquement au moment opportun via un compte séparé (par exemple, pour mettre à jour un logiciel nécessitant de tels droits).

Multifactor-authenticatie *– vaak afgekort als MFA – is een beveiligingsproces dat meerdere verificatiefactoren vereist om de identiteit van een gebruiker voldoende te bewijzen.*
MFA combineert informatie over wat de gebruiker weet, zoals een wachtwoord, maar ook over een bijkomende factor, zoals wat hij bezit, zoals een smartphone, die hij meestal kan gebruiken om het inloggen te valideren of een eenmalige authenticatiecode te verkrijgen. Zo zal een kwaadwillende actor die uitsluitend beschikt over het wachtwoord van een slachtoffer zich niet namens hem kunnen authenticeren als MFA is ingeschakeld.
Toch kent deze maatregel enkele beperkingen. Meer geavanceerde en steeds vaker voorkomende phishingaanvallen omzeilen immers dit soort bescherming. Desondanks kan MFA een groot aantal gegevensinbreuken voorkomen.

3- Beginsel van het minste voorrecht

De bedrijfsrevisor hanteert het beginsel van het minste voorrecht, dat wil zeggen dat personeelsleden het minimumniveau van rechten hebben dat nodig is voor de uitvoering van hun taken.

Voorbeelden hiervan zijn:
- de personeelsleden hebben alleen leestoegang tot documenten en dossiers die ze niet hoeven te wijzigen of te verwijderen;
- de personeelsleden hebben geen lokale beheerdersrechten op hun computer, wat het risico op het installeren van malware aanzienlijk verkleint. Als om welke reden dan ook lokale beheerdersrechten vereist zijn, worden deze alleen op het juiste moment gebruikt via een aparte account (bijvoorbeeld om software bij te werken die dergelijke rechten vereist).

4- Cycle de vie des mises à jour de sécurité

Le réviseur d'entreprises veille à ce que les mises à jour de sécurité des composants du système d'information soient régulièrement appliquées.

Typiquement, et à une fréquence qui varie en fonction de différents facteurs tels que le niveau de classification du composant ou de son exposition aux menaces, les mises à jour sont installées lorsqu'elles sont disponibles ou en suivant un cycle récurrent.

Ces mises à jour ne se limitent pas aux « Windows Updates » des postes de travail bien connues, mais incluent aussi celles des logiciels, des serveurs, du *VPN*, du routeur, du pare-feu, du *firmware* des postes de travail, etc.

Le ***VPN*** *– pour « Virtual Private Network » ou « Réseau Privé Virtuel » en français, permet aux employés de se connecter à distance et de manière sécurisée au réseau interne de l'organisation, leur donnant ainsi accès à certaines ressources comme les disques réseaux ou à un intranet, sans devoir exposer celles-ci au monde extérieur.*

Un système qui ne dispose pas de mises à jour de sécurité peut généralement être compromis très facilement par un acteur malicieux. Le réviseur d'entreprises veille donc tout particulièrement à ce que les systèmes exposés à/ou interagissant avec l'internet disposent de l'installation de mises à jour de manière régulière. Soulignons que tout système exposé au monde extérieur, comme un *VPN*, est régulièrement scanné par les hackeurs. Lorsqu'une vulnérabilité est identifiée, le service est rapidement compromis par ces derniers qui pénètrent ainsi dans le réseau de l'entreprise. En général, ces étapes sont entièrement automatisées.

4- Levenscyclus van beveiligingsupdates

De bedrijfsrevisor ziet erop toe dat er regelmatig beveiligingsupdates van de informatiesysteemcomponenten worden toegepast.

Meestal, en met een frequentie die varieert afhankelijk van verschillende factoren, zoals het classificatieniveau van de component of de blootstelling ervan aan bedreigingen, worden updates geïnstalleerd wanneer ze beschikbaar zijn of volgens een terugkerende cyclus.

Deze updates beperken zich niet tot de bekende *"Windows Updates"* voor werkposten, maar omvatten ook updates voor software, servers, VPN, router, firewall, *firmware* voor werkposten, enz.

Het ***VPN*** *– voor Virtual Private Network of Virtueel Privénetwerk – stelt werknemers in staat om op afstand en veilig verbinding te maken met het interne netwerk van de organisatie, waardoor ze toegang krijgen tot bepaalde bronnen zoals netwerkschijven of tot een intranet, zonder dat ze deze aan de buitenwereld hoeven bloot te stellen.*

Een systeem zonder beveiligingsupdates kan over het algemeen heel gemakkelijk worden gecompromitteerd door een kwaadwillende actor. De bedrijfsrevisor ziet er daarom in het bijzonder op toe dat systemen die worden blootgesteld aan en/of interageren met internet, regelmatig worden bijgewerkt. Er dient te worden beklemtoond dat elk systeem dat aan de buitenwereld wordt blootgesteld, zoals een VPN, regelmatig wordt gescand door hackers. Wanneer een kwetsbaarheid wordt geïdentificeerd, wordt de dienst snel gecompromitteerd door de hackers, die zo het ondernemingsnetwerk binnendringen. Over het algemeen zijn deze stappen volledig geautomatiseerd.

Idéalement, un processus de monitoring des vulnérabilités est mis en place. Ainsi, lorsqu'une vulnérabilité critique est identifiée, le processus d'installation de mise à jour peut être lancé immédiatement, sans attendre le prochain cycle. En effet, lorsqu'une vulnérabilité critique affecte un système interagissant avec le monde extérieur, chaque moment est précieux pour éviter sa compromission.

5- Protections anti-malware

Le réviseur d'entreprises veille à installer des logiciels anti-malware sur les composants du système d'information, tels que les postes de travail et les serveurs. Les mises à jour de sécurité de ces logiciels sont régulièrement installées, tout comme les mises à jour de leurs bases de données de connaissances. Notons qu'aucune solution anti-malware n'est capable de détecter tous les logiciels malveillants ou de détecter l'ensemble des attaques en cours.

6- Utilisation de la cryptographie

Le réviseur d'entreprises s'assure que des mesures de cryptographie adéquates sont mises en place. Par exemple, tous les échanges de données devraient en principe être chiffrés, en particulier lorsqu'ils passent à travers des réseaux non fiables comme l'internet. Le réviseur évalue notamment l'utilisation du chiffrement de bout en bout qui réduit les risques de violations de données, en empêchant la lecture des données par le fournisseur de service. Les protocoles de chiffrement des données respectent les standards, qui évoluent au fil du temps.

Pour citer quelques exemples et comme explicité en amont, les backups et les supports de données mobiles sont chiffrés. D'autres exemples sont l'échange de flux de données/informations en business to business (B2B) ainsi que les e-mails.

In het ideale geval wordt er een proces voor het monitoren van kwetsbaarheden opgezet. Dit betekent dat wanneer een kritische kwetsbaarheid wordt geïdentificeerd, het update-installatieproces onmiddellijk kan worden gestart, zonder te wachten op de volgende cyclus. Wanneer een kritische kwetsbaarheid een systeem beïnvloedt dat met de buitenwereld interageert, is elk moment immers waardevol om te voorkomen dat het systeem wordt gecompromitteerd.

5- Antimalwarebeveiliging

De bedrijfsrevisor ziet erop toe dat antimalwaresoftware wordt geïnstalleerd op de informatiesysteemcomponenten, zoals werkposten en servers. Beveiligingsupdates voor deze software worden regelmatig geïnstalleerd, evenals updates voor hun kennisdatabases. Er dient te worden opgemerkt dat geen enkele antimalware-oplossing alle malware of lopende aanvallen kan detecteren.

6- Gebruik van cryptografie

De bedrijfsrevisor vergewist zich ervan dat er passende cryptografische maatregelen worden getroffen. Zo zouden bijvoorbeeld alle gegevensuitwisselingen in principe moeten worden versleuteld, in het bijzonder wanneer ze via onbetrouwbare netwerken zoals het internet verlopen. De bedrijfsrevisor beoordeelt meer bepaald het gebruik van *end-to-end*-encryptie die het risico op gegevensinbreuk vermindert, door te voorkomen dat de serviceprovider de gegevens leest. Gegevensversleutelingsprotocollen houden zich aan standaarden, die in de loop van de tijd evolueren.

Om een paar voorbeelden te noemen en zoals hierboven toegelicht, worden back-ups en mobiele gegevensdragers versleuteld. Andere voorbeelden zijn de uitwisseling van gegevens-/informatiestromen in *business-to-business* (B2B) en e-mails.

Nous devons toutefois ajouter que le cryptage des données n'est pas toujours évident en ce qui concerne la profession de réviseur d'entreprises. En Asie, par exemple, il existe une interdiction quasi totale du cryptage[6].

7- Réseau séparé pour les visiteurs

Lorsque le réviseur d'entreprises offre une connexion internet à ses visiteurs, généralement via un réseau wifi, il veille à ce que ce réseau soit séparé de celui de l'organisation afin de réduire les risques d'intrusions.

4. Mesures spécifiques liées à la protection des données à caractère personnel

Certaines mesures supplémentaires à celles déjà décrites en amont sont requises spécifiquement pour assurer la protection des données à caractère personnel et assurer la conformité des traitements de données au RGPD.

Afin de les identifier, le réviseur d'entreprises prendra soin d'élaborer son registre des activités de traitements de données à caractère personnel. Le registre décrit les opérations de traitements réalisées par l'organisation. La tenue du registre est imposée par l'article 30 du RGPD et doit contenir les coordonnées du responsable du traitement et, le cas échéant, de son délégué à la protection des données, la description des finalités poursuivies, le détail des catégories de données à caractère personnel traitées, la liste des destinataires des données, etc. Ce registre est à la disposition de l'Autorité de protection des données qui peut y demander accès à tout moment.

6 Cf. *World Map of Encryption* : https://www.gp-digital.org/world-map-of-encryption/

Er dient echter te worden opgemerkt dat gegevensversleuteling niet altijd vanzelfsprekend is als het gaat om het beroep van bedrijfsrevisor. In Azië is er bijvoorbeeld een bijna volledig verbod op versleuteling[6].

7- Apart netwerk voor bezoekers

Wanneer de bedrijfsrevisor een internetverbinding aanbiedt aan zijn bezoekers, over het algemeen via een wifi-netwerk, ziet hij erop toe dat dit netwerk gescheiden is van het netwerk van de organisatie om het risico op inbreuken te verkleinen.

4. Specifieke maatregelen met betrekking tot de bescherming van persoonsgegevens

Bepaalde maatregelen naast de hierboven reeds beschreven maatregelen zijn specifiek vereist om de bescherming van persoonsgegevens te waarborgen en ervoor te zorgen dat de gegevensverwerking in overeenstemming is met de GDPR.

Om deze maatregelen te identificeren, zal de bedrijfsrevisor zorgen voor het opstellen van zijn register van de verwerkingsactiviteiten van persoonsgegevens. Het register beschrijft de door de organisatie uitgevoerde verwerkingen. Het houden van het register is vereist op grond van artikel 30 van de GDPR en moet de volgende gegevens bevatten: de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van zijn functionaris voor gegevensbescherming, de beschrijving van de nagestreefde verwerkingsdoeleinden, de bijzonderheden van de categorieën van verwerkte persoonsgegevens, de lijst van ontvangers van de gegevens, enz. Dit register is beschikbaar voor de Gegevensbeschermingsautoriteit, die er te allen tijde toegang toe kan vragen.

6 *Cf. World Map of Encryption*: https://www.gp-digital.org/world-map-of-encryption/.

AVEC L'UTILISATION CROISSANTE DES NOUVELLES TECHNOLOGIES, LES RÈGLES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ET DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL COMPLÈTENT L'OBLIGATION DE SECRET AFIN D'ASSURER LEUR CONFIDENTIALITÉ, LEUR INTÉGRITÉ ET LEUR DISPONIBILITÉ.

En prenant conscience des traitements effectués au sein de son cabinet, le réviseur d'entreprises est capable d'identifier les mesures spécifiques qu'il doit mettre en œuvre afin de garantir la protection des données à caractère personnel (mesures d'informations à l'égard des personnes concernées, rédaction d'une politique de gestion des cookies, réalisation d'une analyse d'impact à la protection des données lorsque des technologies innovantes sont utilisées, etc.). Ces mesures spécifiques sont utilement reprises dans un plan d'actions de mise en conformité.

5. Conclusions

Tout au long de cette contribution, des mesures indispensables à prendre pour assurer la sécurité de l'information et la protection des données à caractère personnel ont été décrites. L'adoption de ces mesures permet au réviseur d'entreprises de limiter les risques de cyberattaques et d'atteintes aux données à caractère personnel. Le réviseur veille à identifier les mesures supplémentaires nécessaires en fonction des traitements qu'il effectue.

MET HET TOENEMENDE GEBRUIK VAN NIEUWE TECHNOLOGIEËN VULLEN VOORSCHRIFTEN VOOR INFORMATIEBEVEILIGING EN BESCHERMING VAN PERSOONSGEGEVENS DE GEHEIMHOUDINGSPLICHT AAN OM DE VERTROUWELIJKHEID, INTEGRITEIT EN BESCHIKBAARHEID ERVAN TE WAARBORGEN.

Door zich bewust te worden van de binnen zijn kantoor uitgevoerde verwerkingen, kan de bedrijfsrevisor de specifieke maatregelen identificeren die hij moet implementeren om de bescherming van persoonsgegevens te waarborgen (informatiemaatregelen ten aanzien van de betrokkenen, het opstellen van een cookiebeheerbeleid, het uitvoeren van een gegevensbeschermingseffectbeoordeling wanneer innovatieve technologieën worden gebruikt, enz.). Deze specifieke maatregelen worden op nuttige wijze opgenomen in een compliance-actieplan.

5. Conclusies

In deze publicatie zijn essentiële maatregelen beschreven die moeten worden getroffen om de informatiebeveiliging en de bescherming van persoonsgegevens te waarborgen. Het vaststellen van deze maatregelen stelt de bedrijfsrevisor in staat om de risico's op cyberaanvallen en inbreuken in verband met persoonsgegevens te beperken. De bedrijfsrevisor ziet erop toe dat hij de aanvullende maatregelen identificeert die nodig zijn op basis van de verwerkingen die hij uitvoert.

Avec l'utilisation croissante des nouvelles technologies, les règles en matière de sécurité de l'information et de protection des données à caractère personnel complètent l'obligation de secret afin d'assurer leur confidentialité, leur intégrité et leur disponibilité. En effet, le secret professionnel n'a pas pour vocation de protéger le réviseur d'entreprises contre le piratage informatique ou les incidents informatiques involontaires ayant des impacts sur les données.

Les obligations légales en termes de sécurité sont utilement complétées avec les mesures et exigences que l'on retrouve dans les standards tels que ISO 27001, NIST 800-53 ou le *CyberFundamentals* de la CCB, dont le réviseur peut largement s'inspirer et dont les grands principes sont repris dans la présente contribution. Comme indiqué en amont, les risques liés à la protection des données peuvent également avoir un impact sur l'organisation du cabinet, en particulier sur l'évaluation de certains risques liés à la qualité et sur la nécessité de mettre en place des contrôles supplémentaires pour atténuer ces risques. Tous les risques liés à la protection des données ne conduisent pas nécessairement à des risques de qualité découlant de la norme ISQM-1. À cet égard également, il convient de faire preuve de discernement professionnel.

Précisons encore que l'Institut des Réviseurs d'Entreprises soutient les cabinets dans leur démarche de mise en place des mesures techniques et organisationnelles appropriées. Ainsi, l'Institut propose les services d'un délégué à la protection des données mutualisé pour le secteur, dont les services permettent de s'assurer de la bonne conformité au RGPD.

Met het toenemende gebruik van nieuwe technologieën vullen voorschriften voor informatiebeveiliging en bescherming van persoonsgegevens de geheimhoudingsplicht aan om de vertrouwelijkheid, integriteit en beschikbaarheid ervan te waarborgen. Het beroepsgeheim is immers niet bedoeld om de bedrijfsrevisor te beschermen tegen computerhacking of onopzettelijke computerincidenten die een impact hebben op de gegevens.

De wettelijke verplichtingen op het vlak van beveiliging worden op nuttige wijze aangevuld met de maatregelen en vereisten die voorzien zijn in standaarden zoals ISO 27001, NIST 800-53 of de *Cyberfundamentals* van het CCB, waarop de bedrijfsrevisor zich grotendeels kan inspireren en waarvan de belangrijkste beginselen in deze publicatie zijn opgenomen. Zoals hierboven vermeld, kunnen gegevensbeschermingsrisico's ook een impact hebben op de organisatie van het kantoor, in het bijzonder op de inschatting van bepaalde kwaliteitsrisico's en de noodzaak om aanvullende interne beheersingsmaatregelen te implementeren om deze risico's te beperken. Niet alle gegevensbeschermingsrisico's leiden noodzakelijkerwijs tot kwaliteitsrisico's die voortvloeien uit ISQM 1. Ook in dit opzicht dient professionele oordeelsvorming te worden toegepast.

Ook moet worden opgemerkt dat het Instituut van de Bedrijfsrevisoren de kantoren ondersteunt bij hun proces voor het implementeren van passende technische en organisatorische maatregelen. Zo biedt het Instituut de diensten aan van een gemeenschappelijke functionaris voor gegevensbescherming voor de sector met het oog op het waarborgen van de overeenstemming met de GDPR.

Le service d'un délégué à la protection des données mutualisé est ouvert aux cabinets de révision, sur une base volontaire et pour un prix avantageux.
Les avantages pour la profession sont nombreux :
- *image de la profession : moderne, axée sur les nouvelles technologies, sécurité juridique & informatique ;*
- *prise en charge centralisée des tâches à accomplir ;*
- *mise en place de processus harmonisés pour la profession ;*
- *garantie d'avoir un DPO indépendant ;*
- *point de contact unique avec l'Autorité de protection des données ;*
- *point de contact unique pour les personnes concernées (citoyens, clients, employés) ;*
- *support concernant toutes les questions liées à la protection des données à caractère personnel.*

Pour toute information complémentaire à ce sujet, n'hésitez pas à vous adresser dès à présent à info@privanot.be.

La protection des données et la sécurité de l'information ne doivent donc pas être considérées comme un frein au développement de la profession du réviseur d'entreprises ou comme une perte de temps mais doivent, au contraire, être perçues comme la garantie de sa pérennité et de son évolution dans le monde dématérialisé qui l'entoure.

De diensten van een gemeenschappelijke functionaris voor gegevensbescherming is opengesteld voor bedrijfsrevisorenkantoren op vrijwillige basis en tegen een voordelige prijs.
De voordelen voor het beroep zijn talrijk:
- *imago van het beroep: modern, gericht op nieuwe technologieën, rechtszekerheid en IT-beveiliging;*
- *gecentraliseerde afhandeling van de uit te voeren taken;*
- *vastlegging van geharmoniseerde processen voor het beroep;*
- *garantie van een onafhankelijke DPO;*
- *één enkel contactpunt met de Gegevensbeschermingsautoriteit;*
- *één enkel contactpunt voor de betrokkenen (burgers, cliënten, bedienden);*
- *steun in alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.*

Voor meer informatie over dit onderwerp kunt u contact opnemen met info@privanot.be.

Gegevensbescherming en informatiebeveiliging mogen daarom niet worden beschouwd als een obstakel voor de ontwikkeling van het beroep van bedrijfsrevisor of als tijdverspilling, maar dienen integendeel te worden opgevat als het vrijwaren van het voortbestaan en de evolutie ervan in de gedematerialiseerde wereld die het beroep omringt.

Summary

The registered auditor processes large volumes of data and information on a daily basis, whether for his audit engagements or for the management of his own organisation.

In a context of increasing dematerialisation, the risks of data and information breaches are increasing, given, among other things, the degree of complexity of information systems and the sophistication of the methods used by malicious actors (hackers, fraudsters, etc.). In the most serious cases, the consequences may entail the permanent cessation of the firm's activities.

This article aims to provide the reader with an analysis of useful measures he can adopt in order to mitigate the risks of cyberattacks and personal data breaches within his firm. These measures derive both from information security precepts and those relating to the protection of personal data.