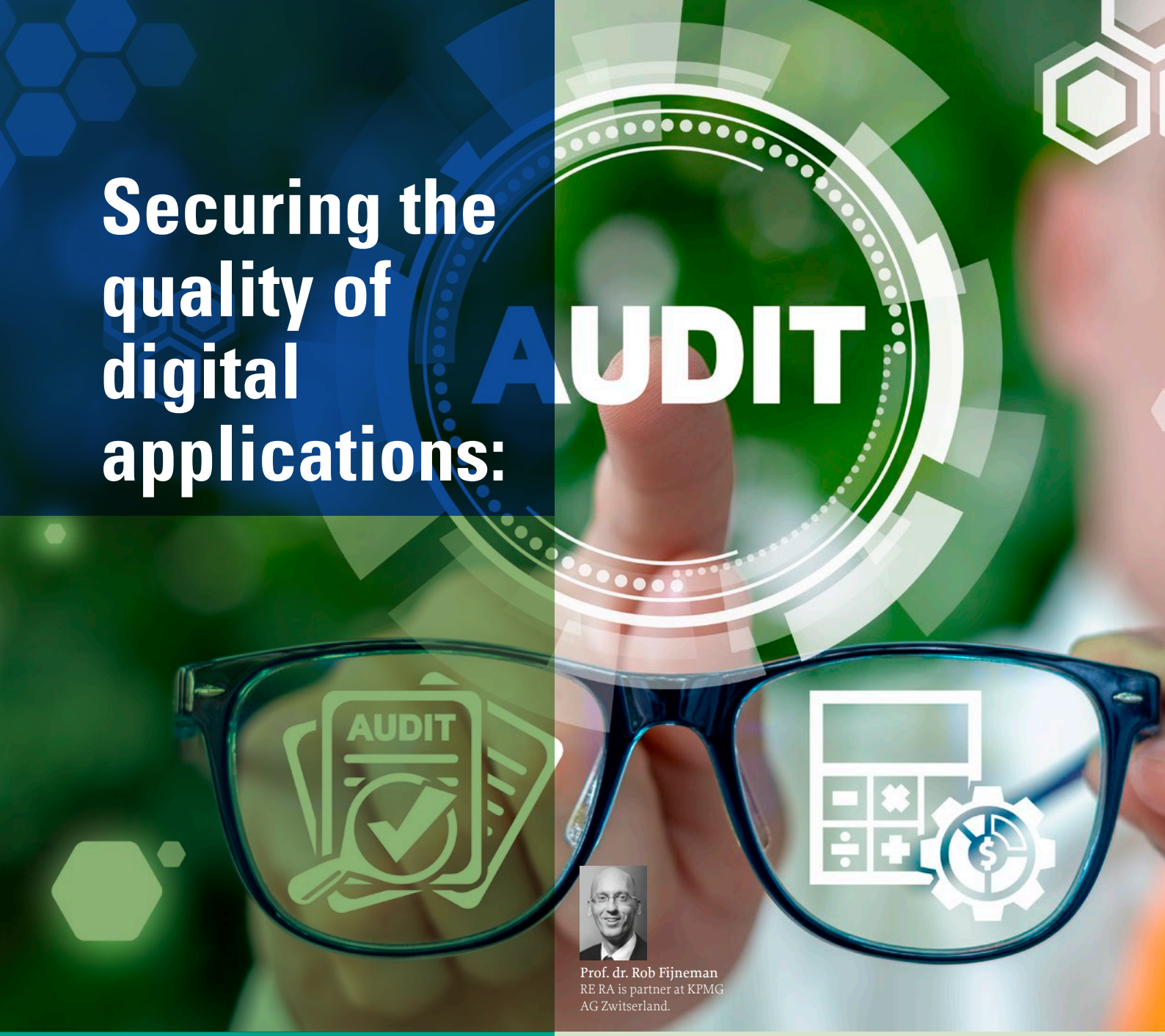
Securing the quality of digital applications:



Prof. dr. Rob Fijneman
RE RA is partner at KPMG AG Zwitserland.

challenges for the IT auditor

Since the advent of digital solutions, the ongoing inquiry into their reliability and security has been a central concern. An increasing number of individuals and companies are asking for assurance. There is a need for standards to report on the quality of the use of digital solutions. Primary responsibility rests with an organization's management; however, incorporating an independent IT auditor can provide additional value.

IT governance requires management to take responsibility for quality

INTRODUCTION

Digital developments are happening at lightning speed. We are all aware of the many digital applications and possibilities in both our business and personal lives. Often, however, we only know and use 10 to 20 percent of the application possibilities of current solutions, and yet we are constantly looking for something new. Or is this all happening to us from an ever-accelerating "technology push"? The covid pandemic that started in 2020 showed us once again that digital tools are indispensable. Digital tools enabled us to remain connected and operational, facilitating ongoing communication among us.

How do we know if digital applications and solutions are sufficiently secure? Do the answers generated by algorithms, for example, reflect integrity and fairness? Are we sufficiently resilient to cyber-attacks and are we spending our money on the right digital solutions? These questions are highly relevant for directors and supervisors of organizations, as they must be able to account for their choices. Externally, the board report provides the basis for policy accountability. It is primarily retrospective in nature and has an annual cycle. The board report could explicitly discuss the digital agenda. The professional association of IT auditors (NOREA) is investigating whether an (external) IT audit 'statement' ([NORE21]) could also be added (see also this article on the new IT audit statement). Accountability for the quality of digital applications and whether everything is done securely, with integrity and effectively takes on new dimensions now that developments are happening at lightning speed, and everyone is connected to everyone else. Administrators, regulators as well as end users and/or consumers are looking for assurance that the digital applications and the resulting data are correct. Validation through assurance by an IT auditor serves as an effective tool for this purpose. A confirmation of quality on the digital highway must and can be found.

These issues are at play not only within organizations, but also in broader society. Protecting privacy is firmly under pressure, the numerous digital solutions are building a continuous personal profile. Also, there are painful examples of the use of algorithms in the public domain ([AR21]) that have seriously harmed a number of citizens. Responsible development toward more complex automated applications requires better oversight and quality control, according to the Court of Audit in its report on algorithms in 2021 ([AR21]). Issues of digital integrity, fairness, reasonableness and security have taken on social significance.

Coupled with the introduction of the Computer Crime Act (WCC I), an explicit link to accountability for computerized data processing emerged for the first time in the 1980s. Meanwhile, the Computer Crime Act III (WCC III) ([Rijk19]) has been in force since 2019, which takes into account many developments in the field of the Internet and privacy. As the final piece in the chain of control and accountability from the WCC I onwards, the auditor must explicitly express an opinion on the reliability and continuity of automated data processing as far as relevant for financial reporting according to Civil Code 2, article 393 paragraph 4. Over four decades have passed, and we now grapple with an expanding array of legislation governing the control of digital solutions. These solutions extend beyond administrative processes to impact all core business functions, bringing with them a shift in the perspective on associated risks.

In short, it's time to consider how quality on the digital highway (such as security, integrity, honesty, efficiency, effectiveness) can be assured. How can accountabilities be formed, what role do managers and supervisors play in this, and how can IT auditing add value? As indicated, these questions play a role not only at the individual organizational level, but also at the societal level. For example, how can the government restore or regain the trust of citizens by explicitly accounting for the deployment of its digital solutions?

IT auditing concerns the independent assessment of the quality of information technology (processes, governance, infrastructure). Quality has many partial aspects; not only does it involve integrity, availability and security, it also involves fairness and honesty. The degree of effectiveness and efficiency can also be assessed. To date, the interpretation of IT auditing is still mostly focused on individual digital applications and still too limited when it comes to the entire coherence of digital applications that fit within the IT governance of an organization. IT auditing can be an important tool in confirming the quality or identifying risks in the development and application of digital solutions if it is used more integrally. This establishes a harmonious interplay between the

organization's responsibility for its IT governance and the validation of its quality by an IT auditor.

TECHNOLOGY DEVELOPMENTS

The COVID crisis has undeniably brought remote work to the forefront and has heightened the significance of adaptable IT. Several emerging trends underscore the landscape of digital solutions and advancements.

What's noteworthy is that a considerable number of organizations exhibit an intricate blend of technology solutions, incorporating both legacy systems and contemporary online (front-office) solutions. Ensuring data integrity, keeping all solutions functioning in continuity, being able to make the right investments and paying for maintenance of legacy solutions, and planning for all of that is certainly not an easy task.

Let's briefly highlight a few trends commonly cited by multiple authors ([KPMG20]; [Wilr20]):

- Flexible work is becoming the norm. Last year, the cloud workplace – more than predicted – grew in popularity. Employees had to work from home, which requires a flexible and secure IT workplace.
- Distributed cloud offers new opportunities for automation. The cloud will also continue to evolve, continuously creating new opportunities that support business growth. According to Gartner analysts ([Gart20]), one of these is the distributed cloud. It can speed up data transfer and reduce its costs. Storing data within specific geographic boundaries – often required by law or for compliance reasons – is also an important reason for choosing the distributed cloud. The provider of the cloud services remains responsible for monitoring and managing it.
- The business use of artificial intelligence (AI) is increasing. Consider, for example, the use of chatbots and navigation apps. This technology will be increasingly prominent in business in the near future. The reason? Computer power and software are becoming cheaper and more widely available. AI will increasingly be used to analyze patterns from all kinds of data.
- Internet of Behaviors. Data is now the lynchpin for much of business processes. Data provides insight and therefore plays an increasingly important role in making strategic decisions. This data-driven approach is also applied to changing human behavior. We also call this the Internet of Behaviors. Based on these analyses, suggestions or autonomous actions can be developed that contribute to issues such as human safety and health. An example is the smartwatch that tracks blood pressure and oxygen levels and provides health tips based on those data.
- Maturity of 5G in practice. In 2020, providers in the Netherlands rolled out their first 5G networks. With 5G, you can seamlessly stay connected on the move or in any location without relying on Wi-Fi. Apart from higher data upload and download speeds, the big changes are mainly in new applications, especially in the field of the Internet of Things. Examples include self-driving cars and a surgeon operating on his patient a thousand kilometers away via an operating robot. Such applications are promising.

MANAGEMENT RESPONSIBILITIES

Driving and overseeing digital solutions is not a given. "Unknown makes unloved" still plays tricks here. The complexity of technology deters, the mix of legacy systems and new digital solutions does not make it very transparent, many parties manage part of the technology chain and the quality requirements are not always explicit.

Still, some form of "good governance" is needed. Fellow Antwerp professor Steven de Haes ([DeHa20]) has gained many insights in his studies on IT governance. In his view, governance needs to address two issues concerning digital solutions. The first is whether digital risks are managed, which requires a standard to test against. In line with the COSO framework (COSO: Committee of Sponsoring Organizations) often used in governance issues, (parts of) the international CoBiT framework (CoBiT: Control Objectives for Information Technology) ([ISAC19]) can be chosen. Management explicitly identifies the applicable management standards for digital solutions, ensuring the clear establishment of both their design and operational processes.

The second question is strategic in nature: are the digital developments correct? Is the strategy concerning the deployment of digital solutions correct and are the investments required correct? Answering this requires a good analysis of the organizational objectives and the digital solutions needed to achieve them. As indicated earlier, the main issues are effectiveness and efficiency.

Establishing a robust organizational foundation begins with a well-structured organizational setup. This often involves using a "layer model" to arrange the various responsibilities. The primary responsibility for ensuring the proper use of digital solutions rests squarely on the shoulders of first-line management. This can be assisted by a "risk & control" function that can act as a "second line" to help set up the right controls and perform risk assessments. The second line can also set up forms of monitoring on the correct implementation and use of the digital solutions. Then, as a third line, an internal audit

function can assess whether the controls in and around the digital solutions are set up and working properly; if desired, the external audit function can confirm this as well. In short, a layered model emerges to collectively ensure the quality of digital solutions.

Given the tremendous speed of digital change, continuous new knowledge of technology is needed. Effectively coordinating this effort while maintaining a focus on the quality of solutions and acknowledging their inherent limitations is the key to successful governance. It is not a static entity, continuously changes in the chain has to be evaluated and adjusted if necessary. Conceivably, the IT function (the CIO or IT management) could organize a structural technology dialogue that starts with knowledge sessions, addressing the quality of digital applications. End users and management share the responsibility of clearly defining quality requirements, overseeing them through change processes, and ensuring the ongoing monitoring, or delegation of monitoring, to guarantee the quality of digital applications and data.

The suppliers of the digital solutions also play an important role. They have to be good stewards and provide better and safer solutions. This does not happen automatically, as is regularly the case; the focus is more on functional innovation than on good management and security. The buyers of the solutions also still question the providers too little about a "secure by design" offering. Proper controls can, and in fact should, already be built in during solution design.

Are the new digital solutions becoming so complex that no one can determine the correctness of the content? From a management perspective, we cannot take such a "black box" approach. We cannot accept, for example, deploying a digital application without knowing whether it works safely. Management should pause and prioritize organizing knowledge or acquiring information about the quality before justifying further deployment.

CHALLENGES FOR THE IT AUDITOR

These quality issues can be answered by IT auditors. In the Netherlands, this field has been organized for more than thirty years, partly through the professional organization NOREA (Dutch Association of EDP Auditors)[1] and university IT audit programs.

The IT auditor has a toolbox to assess digital solutions on various quality aspects. In increasing number of auditing and reporting standards have been developed to provide clients with assurances or a correct risk picture.

On the positive side, current IT auditing standards can already answer many questions from clients about digital solutions. The key is for IT auditors to adequately disclose what they can do and to work with regulators to enrich the tools. The IT auditor has to use simpler language to clarify what is really going on. Clients can and should sharpen their questioning and take responsibility themselves, such as establishing the right level of control.

IT auditors are currently still mainly looking for technically correct answers and methodologies, while a dialogue is needed about the relevant management questions concerning IT governance. What dilemmas do managers and regulators experience when determining the quality level of digital applications and what uncertainties exist? This is what the IT auditor should focus on. Starting from a clear management question, the IT auditor's already available tools listed below can be used in a much more focused way.

From an auditing perspective, when outsourcing, the standard ISAE 3402 (ISAE: International Standards on Assurance Engagements)[2] was developed to keep both the auditor and the client organization informed about the quality of the audits performed by the service organization. The emphasis lies on ensuring the reliability and continuity of financial data processing. The resulting report is called a SOC 1 report (SOC: Service Organization Control).

An ISAE 3402 audit requires proper coordination on the scope of work and the controls to be tested (both in design and in operational operation). The performing IT auditor consults with both the service organization and the receiving customer organization to arrange everything properly. This also involves specific attention to both the "Complementary User Entity Controls" (CUECs), the additional internal control measures that the customer organization must implement, and the "Complementary Subservice Organization Controls" (CSOCs), the control measures that their possibly deployed IT service providers must implement. Frequent consultations occur with the client organization's auditor, who incorporates the ISAE 3402 report as an integral part of the audit process.

The scope of an ISAE 3402 audit can be significant and already provide a solid basis for quality assurance of digital applications. An example from IT audit practice involves a sold division of a company that is now part of

1 See www.norea.nl.

2 See www.iaasb.org, 'Standards and resources'.

another international group. The sold division has plants in over 30 countries, all of which still use the original group's IT services. A test plan has been set up to test the relevant general computer controls (such as logical access security, change control and operations management, also known as "general IT controls"), and all relevant programmed financial controls in the selected financial systems. In this example, this yields a testing of over eighty general computer controls and over two hundred programmed controls by a central group audit team and audit teams in the various countries.

Another assurance report is an ISAE 3000 report, which is prepared to demonstrate that the internal management processes an organization has in place are actually being carried out as described. Basically, this standard was developed for assurances about non-financial information. This may take the form of an ISAE 3000 attestation (3000A), wherein the organization internally defines and reviews standards and controls, with the IT auditor subsequently confirming their effectiveness. Alternatively, it can manifest as a 3000D ("direct reporting"), involving collaborative definition of review standards and controls by both the organization and the IT auditor.

The ISAE 3000 report (also referred to as SOC 2[3]) can focus on many issues and also has multiple quality aspects as angles, such as confidentiality and privacy. Standard frameworks have since been established for conducting privacy audits, for example ([NORE23])[4] based on ISAE 3000. The North American accounting organizations, including AICPA, CPA Canada, and CIMA[5], have collaboratively developed comprehensive standard frameworks, such as SOC 2 modules on Security, Availability, Processing Integrity, and Confidentiality[6]. These are readily applicable to IT and SaaS services and are increasingly being embraced by IT service providers in Europe. For specific IT audit objects, such as specifically delivered online services/functionalities, these can be further focused or expanded with IT (application) controls relevant to the customer organization.

As a final variant, agreed-upon specific work can be chosen, referred to as an ISAE 4400 report. Users of the report then have to form their own opinion about the activities and (factual) findings that are presented by the IT auditor in the report.

In recent years, there has been plenty of innovation within the field of IT auditing to also assess algorithms, for example, and make a statement about them. Consider the issue of fairness and non-biased data. An interplay between multiple disciplines unfolds to comprehend the risk landscape of intricate digital solutions and offer assurances. IT auditors are partnering with data specialists and legal experts to ensure the reliability of algorithms.

Over the past 18 months, there has been a growing discourse regarding the potential inclusion of an IT audit statement within or as an addition to a company's annual report. Specifically, the company would need to articulate its stance on digital solutions, their management, and, for instance, the associated change agenda. An IT auditor could then issue a statement in this regard. The professional association of IT auditors has developed a plan of action to actively develop this IT report and the communication about it in the coming year. There is ongoing consideration regarding the level of assurance achievable through the opinion; currently, we acknowledge a reasonable and limited degree of assurance from the statement system. Clients naturally seek maximum or, perhaps better, optimal assurance. In other words, the assurance they seek is not always found in an IT audit statement. Even better would be if the communication also provides assurance into the future, an area still untrodden by IT auditors.

Standards for IT audits continue to evolve

3 SOC 2 deals primarily with security (mandatory), availability, integrity, confidentiality and/or privacy, as outlined in the SOC 2 guidelines issued by the Assurance Services Executive Committee (ASEC) of the AICPA.

4 There is a Dutch and an English version of the Privacy Control Framework.

5 AICPA: American Institute of Chartered Professional Accountants; CIMA: Chartered Institute of Management Accountants.

6 See [Zwin21] for an article on SOC 2 and [AICP23] for AICPA and CIMA standards.

CONCLUSION

As indicated earlier, tools already exist for the IT auditor to confirm the quality of digital applications. Clients must take responsibility to better understand digital applications and set up the corresponding IT governance. IT auditors can improve their communication, can empathize even more with management's (their clients') questions, and also provide understandable reports.

Addressing pertinent social concerns related to the implementation of digital solutions involves conducting a comprehensive risk inventory and evaluating the effectiveness of the existing controls. In addition to the traditional concerns focused on reliability and security, issues of effectiveness, efficiency, privacy and fairness come into play. The resilience of digital solutions is also an urgent issue. In the EU, the Network and Information Security Directive (NIS2 Directive)[7] and the Digital Operations Resilience Act (DORA)[8] for financial institutions have been established to strengthen digital resilience. The regulator of publicly traded companies in the United States (SEC) has also issued guidelines for annual reporting on cyber security (risk management, governance) and interim reporting of serious incidents. ([SEC23]).

The concept of *secure by design* is anticipated to become increasingly prevalent, as technology vendors recognize the necessity of implementing robust controls during solution deployment. Some suppliers also provide mechanisms to set up continuous monitoring, where the controls put in place are assessed for continuous correct operation and exceptions are reported. Management also plays an important role in this regard; embrace the principles described above. Remember that it is more effective and efficient to design controls during the change of digital solutions than to fix them afterwards.

If more and more continuous monitoring is provided, the IT auditor can move toward a form of *continuous auditing*, providing assurances about the deployment of the digital solution at any time. The "anytime, anyplace, anywhere" principle then becomes a reality in IT auditing. A nice, relaxing prospect within all the digital speeds.

7 See [NCSC23].

8 See [Alam22] for an article on DORA.

About the author

Prof. Rob Fijneman RE RA is a partner at KPMG AG Switzerland, professor of IT auditing at TIAS, Tilburg University, and visiting professor at St. Gallen Universität.

References

[AICP23] AICPA & CIMA (2023). SOC 2® – SOC for Service Organizations: Trust Services Criteria. Consulted at: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

[Alam22] Alam, A., Kroese, A., Fakirou, M., & Chandra, I. (2022). DORA: an impact assessment. Compact 2022/3. Consulted at: https://www.compact.nl/articles/dora-an-impact-assessment/

[AR21] Algemene Rekenkamer (2021, 26 januari). *Aandacht voor algoritmes*. Consulted at: https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes

[DeHa20] De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise Governance of Information Technology* (3rd ed.). Springer.

[Gart20] Gartner (2020, 12 Augus). The CIO's Guide to Distributed Cloud. Consulted at: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-distributed-cloud

[ISAC19] ISACA (2019). COBIT 2019 or COBIT 5. Consulted at: www.isaca.org

[KPMG20] KPMG (2020). Harvey Nash / KPMG CIO Survey 2020: Everything changed. Or did it? Consulted at: https://kpmg.com/dp/en/home/insights/2020/11/harvey-nash-kpmg-cio-survey-2020.html

[NCSC23] Nationaal Cyber Security Centrum (2023). Summary of the NIS2 guideline. Consulted at: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-richtlijn

[NORE21] NOREA (2021). Nieuwe IT check: NOREA ontwikkelt IT-verslag en -verklaring als basis voor verantwoording. Consulted at: www.norea.nl

[NORE23] NOREA (2023). Kennisgroep Privacy. Consulted at: https://www.norea.nl/organisatie/kennis-en-werkgroepen/kennisgroep-privacy

[Rijk19] Rijksoverheid (2019, 28 February). Nieuwe wet versterkt bestrijding computercriminaliteit. Consulted at: https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit

[SEC23] SEC (2023, 26 July). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies [Press Release]. Consulted at: https://www.sec.gov/news/press-release/2023-139

[Wilr20] WilroffReitsma (2020). ICT Trends 2021: dit zijn de 10 belangrijkste. https://wilroffreitsma.nl/nieuws/ict-trends-2021/

[Zwin21] Zwinkels, S. & Koorn, R. (2021). SOC 2 assurance becomes critical for cloud & IT service providers. *Compact* 2021/1. Consulted at: https://www.compact.nl/articles/soc-2-assurance-becomes-critical-for-cloud-it-service-providers/