Digital solutions: How to ensure quality?

Accountability for the quality of digital solutions is taking on new dimensions

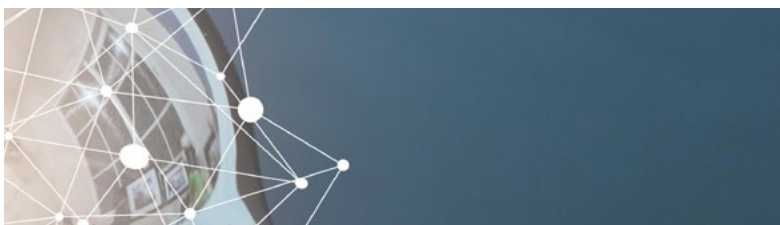
Digital developments are moving at lightning speed – both in our business and private lives. Although oftentimes, we only use a portion of the solutions available, we are always looking for something new. At the same time, the ever-accelerating "technology push" is driving constant change. Starting in 2020, the COVID-19 pandemic demonstrated that digital solutions were the only option to continue to function and communicate in physically distanced setups. But it also came with pressing questions. How do we know whether the digital applications and solutions are sufficiently secure? Are the answers generated by algorithms, for example, honest and fair? Are we sufficiently resilient to cyberattacks? And are we spending our money on the right digital solutions?

These questions are extremely relevant for managers and board members who must also be able to account for their choices in the annual reporting cycle. The board report could explicitly discuss the digital agenda and quality thereof. Indeed, some EU countries have already started to explore whether to require an (external) IT audit "statement". Accountability for the quality of digital solutions is taking on new dimensions as developments move at lightning speed and everyone is linked to everyone. On this digital highway, we are all seeking certainty.

These issues also play a role in society. The protection of privacy is under considerable pressure. There are several painful examples of how using algorithms in the public domain has seriously harmed citizens. Issues of digital integrity, honesty, fairness and security have taken on social significance.

It is interesting to note that a relatively large number of organizations have a complex mix of technology solutions, made up partly of older (legacy) systems and new online (front office) solutions. Ensuring data integrity, functioning and continuity of all solutions and resilience overall is no easy task. It can also be difficult to decide on the right investments and contain costs for maintenance of older solutions, while also having everything run according to plan.

In short, it is time for boards and managers to seek certainties on the digital highway. How can accountability be formalized? What role do board members play in this? And how can IT auditing add value?



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

Good governance as a board imperative

Managing and supervising digital solutions is not something that can be taken for granted. The complexity of technology is clear, with the mixture of legacy systems and new digital solutions blurring transparency efforts. Multiple parties often manage parts of the technology chain, while quality requirements are not always explicit.

A form of good governance is needed. According to Professor Steven de Haes (Antwerp University), who has gained many insights through his studies on IT governance, a board must address two key areas with regard to digital solutions:

- The first area is digital risks, and whether they are managed. To answer this, there needs to be a standard to test against. In line with the framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is often used for governance issues, it is possible to opt for (parts of) the international Control Objectives for Information Technology (CoBiT) framework. In doing so, management makes explicit which control standards are applicable in and around the digital solutions and can determine and monitor their design as well as their operating effectiveness.
- The second area is strategy. Are digital developments the right ones? Is the strategy for deploying digital solutions correct and are the required investments correct? Answering these questions requires a good analysis of the organizational objectives and the required digital solutions, focusing on effectiveness and efficiency.

A layered model is often used to organize the various responsibilities as follows:

- First-line management defines and monitors the correct use of digital solutions. A risk and control function can be helpful as a second line in setting up the right controls and in carrying out risk assessments.
- The second line can also organize forms of monitoring for the correct implementation and use of the digital solutions.
- An internal audit function can then, as a third line, assess whether the controls in and around the digital solutions are properly set up and working effectively; if desired the external (IT) audit function can also confirm this.

The board is responsible for ensuring this layered governance model is set up and monitored and can always ask for independent assessments by (IT) auditors to provide assurance.

In view of the rapid pace of digital change, knowledge of the technology needs to be updated constantly. Good governance involves organizing this aspect while also keeping the quality of the solutions – as well as any inherent limitations – in mind. Governance is not a static exercise – changes in the digital chain will have to be continuously evaluated and adjusted, if necessary. Is the tide turning? In other words, are the new digital solutions becoming so complex that no one can determine the correctness of the content? From a management responsibility perspective, it is not an option to opt for such a "black box" approach. We cannot accept, for example, the use of algorithms that we have not been able to assess for correctness and fairness.

IT auditing and standards

IT auditing is about independently assessing the quality of information technology (processes, governance, infrastructure) or, as mentioned above, digital solutions. This makes IT auditing an important instrument in providing comfort or identifying risks when developing and applying digital solutions. The IT auditor has a set of instruments to assess the digital solutions in terms of various quality aspects. More and more auditing and reporting standards have been developed to provide clients with guarantees or an accurate risk picture. Highlights include:

- International Standards on Assurance Engagements (ISAE) 3402

This standard has been developed from the auditing point of view to inform the accountant of the client organization about the quality of the work performed by a service organization in the case of outsourcing.

- Service Organization Control (SOC) reports

With SOC-1 (or ISAE3402), the focus is on the reliability and continuity of the financial data processing. SOC-2 covers a broader range of quality aspects (like privacy) and data flows.

- ISAE 3000 report

This is another assurance report, which is drawn up to demonstrate that the internal management processes that an organization has set up are carried out as described. The ISAE 3000 report (also referred to as SOC-2) can focus on many topics and covers various quality aspects such as confidentiality and privacy.

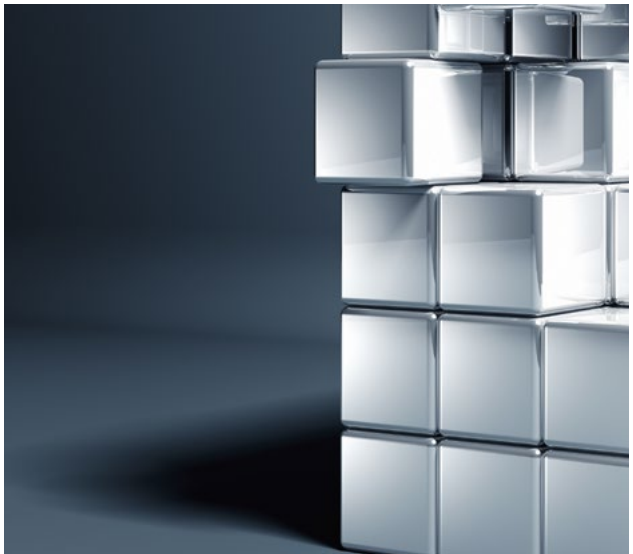
- ISAE 4400 report

The last variant which can be chosen is an agreed-upon procedures report. Users of the report will then have to form their own opinion regarding the activities and findings presented in the report by the IT auditor.

In recent years, a lot of innovation has taken place within the field of IT auditing to, for example, also assess and make a statement about algorithms. Take, for example, the issue of fairness and non-biasedness of data. Interplay between multiple disciplines has to be considered to understand the risk picture of complex digital solutions and to provide certainties. IT auditors work together with data specialists and lawyers on algorithm assurance.

Closing remarks

The current IT audit standards can already answer many boardroom questions about digital solutions. IT auditors should make clear what they can do and opt for collaboration with regulators to enrich the range of instruments. The language and explanation of the IT auditor will sometimes have to be simplified to make it clear what is really going on. Boards can and must refine their questions and take responsibility themselves, for example by setting up the right level of control.



Secure-by-design is expected to become more the norm as technology suppliers also understand that the right controls must be implemented when developing new solutions. Some suppliers also provide mechanisms to set up continuous monitoring, whereby the controls in place are assessed for continuous correct operation and exceptions are reported. Here management also plays an important role in embracing the principles as described above. It is more effective and efficient to adjust the control during implementation of digital solutions than to repair it afterwards.

If more and more continuous monitoring is provided, the IT auditor can move to a form of continuous auditing, in which assurance can be provided on the deployment of the digital solution at any time. This approach would support the board agenda even more in future.

Insights by Professor Dr. Rob Fijneman RE RA

This article is written based on a combination of research insights, results of master theses and practical experience in the field of IT auditing. Rob Fijneman combines being a professor in IT auditing at TIAS School for Business and Society/Tilburg University with being a Technology Audit partner at KPMG AG in Switzerland. His experience covers a wide range of multinational clients which he has audited and advised in the past 36 years. In 2019 he was made officer in the Order of Oranje-Nassau by the Dutch King for his work as professor in IT auditing.

Prof. Dr. Rob Fijneman
Partner, Audit

+41 58 249 23 27
robfijneman@kpmg.com

This article is part of the KPMG Board Leadership News. To receive this newsletter for board members three times a year, you can register here.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2022 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.