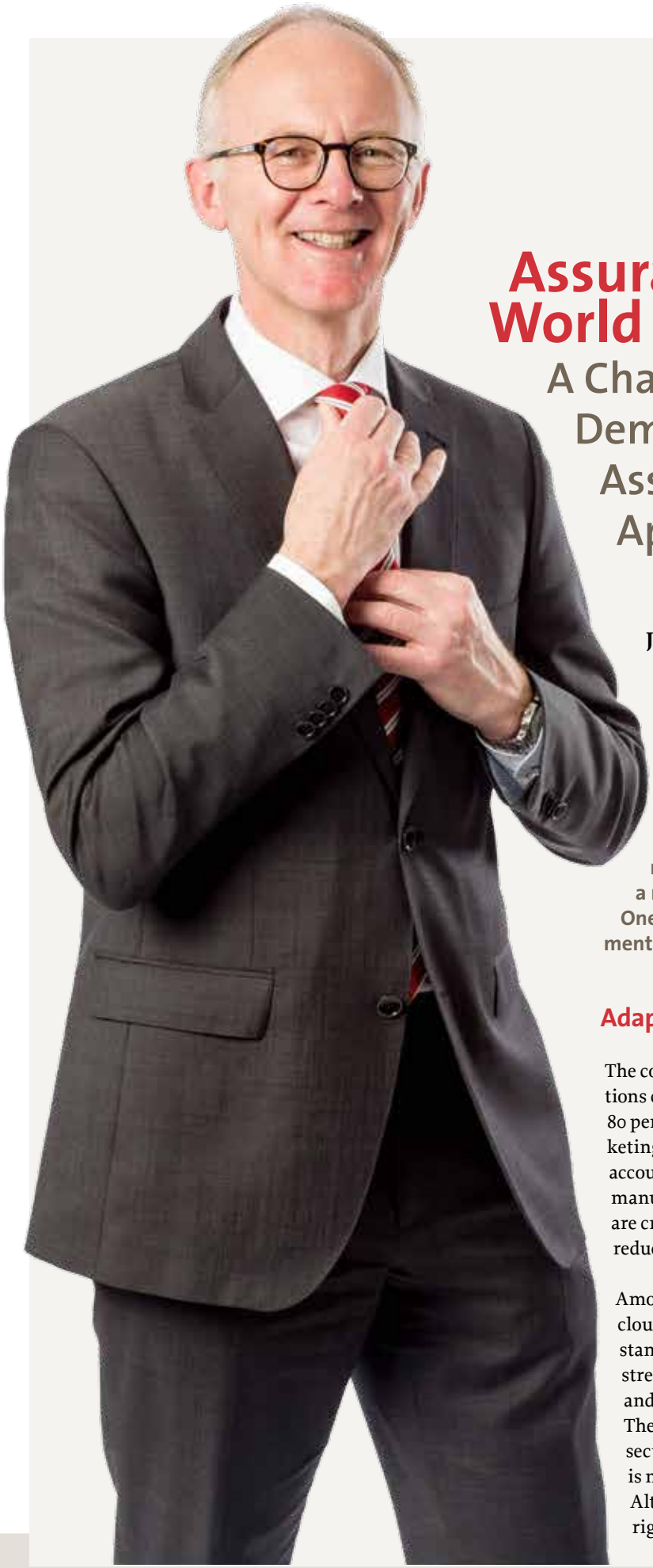

# Assurance in the Digital World of the Future

## A Changing World Creates New Demands When It Comes to Assurance Standards and Approach

**Jaap van Beek**

**The continuous developments within IT such as cloud computing, the Internet of Things and e-commerce (24/7 services) mean that a shift is taking place in the risks and controls necessary to manage security, reliability and confidentiality of data and data processing. Will it continue to be possible for users to adequately control the risk of unauthorized data access or data manipulation and what will this mean for the assurance providers? In this interview we discuss a number of developments and reflect on possible solutions. One thing is clear: assurance must develop along with IT developments to remain relevant for companies and users of IT services.**

### Adapting to New Standards (SOC2) for Cloud Assurance

The corporate use of cloud-enabled services for important business functions continues to grow, according to KPMG research. In 2016, more than 80 percent of companies will be using cloud-enabled tools for sales and marketing, HR, e-mail/collaboration. Other business functions such as finance/accounting, security management, business intelligence and operations/manufacturing are not far behind. Evidently, more and more cloud services are critical to business operations and are now vital when it comes to cost reduction and efforts to accelerate business services.

Among IT and business executives, security, availability and privacy of cloud services are seen as key challenges. In the USA a new assurance standard, SOC2 (Service organization control report 2), is used as a tool to streamline the costs of assessing and monitoring the security, availability and confidentiality practices of their cloud service providers ([Torc13]). The SOC2 is a thorough, predefined standard that closely aligns with security industry standards like ISO27001. In Europe the SOC2 standard is not universally applied as yet, but this will change in the coming years. Although this process of adapting to the new standard is taking place right now, IT auditors still issue reports on paper which are giving assur-

ance on a yearly basis and covering the situation of a year ago, sometimes. Will that really be an adequate situation in the future? In the ultimate cloud solution everything is flexible and dynamic, which can hardly be said of the traditional assurance reports.

## Driving the Developments

With regard to global trends in technology risks as described in the Global Risk 2015 Insight Report of the World Economic Forum, large scale cyberattacks are on the increase in terms of the sophistication of the attacks and the rise of hyperconnectivity (more objects connected with the internet). Analytics on large data sources can drive through insights, but also raise questions about expectations of privacy and data security. At the same time the number of legal and regulatory requirements is increasing. IT developments like Cloud, the Internet of Things, Big Data and the rise of the 24/7 economy seem to lead to a paradigm shift. It is an illusion to think that (cyber) security incidents can be avoided. Controls in current frameworks are usually based on preventive measures which no longer suffice in themselves. More attention needs to be paid to detection and response measures such as incident management. At the same time it is important to strengthen pro-active risk management with components like threat management and vulnerability management. In the famous Target and Diginotar cases the auditors did report on security measures, but yet overlooked important topics ([Diem15]). What will be the response to the ever-changing demands? Is the current way to deal with auditing for assurance purposes still up to standard? And will the receiver of the assurance report accept "generic process-based" assurance reports or will he demand dedicated client-based reports based on factual technical (real time) findings?

## What Will Happen?

It is expected that in three years' time the process of adapting to the new SOC2 standard will be complete and more dynamic reporting will be taking place. Potentially this could take the form of quarterly reporting. If there are issues in a certain quarter, the auditor could report on follow-up and indicate when the issues will be solved. In line with financial reporting this could take the form of more frequent public unaudited service-level reports from the IT provider or more transparent dashboards on the internet. The auditor will include the process of providing the clients with information in the scope of the assurance report.

In 10 years' time continuous auditing is expected to be mature. Currently the focus is on control processes and not on the actual key performance indicators based on technical facts in the service-level reports. IT providers have more and more data and systems available related to the quality of the services delivered, which will be published in this period of transparency. The auditor can use process mining and data analytic tools to analyze the available information and to draw up his ongoing report. The report is no longer based on samples but on 100% of the available data, often client-based! The IT service provider has permanent monitoring in place and the auditor can provide continuous assurance through frequently updated quality-control dashboards.

In 20 to 30 years' time, assurance should no longer be based on controls but should be included in the relevant dataset. Ultimate flexibility! Such datasets can be identified uniquely and are stored safely so that unauthorized attempts to access and effect changes can be made detectible in no time. Technical security measures based on encryption are already available and in use for the blockchain development in the payment industry. In addition, assurance will become part of the monitoring system of the IT provider. IT providers need this monitoring system to keep track of where the data in the cloud is stored. If security and privacy are built into this system, the provision of assurance will also be integrated and not added on top, as in the current situation. I strongly believe that, to remain relevant, IT auditors should play an active role in these developments, both on the advisory and the audit side. There will always be a need for assurance when there are new developments. If IT providers become more transparent, the job will become easier. Still, continuous audits remain necessary to make sure the information can be trusted. The form may change, but we still need humans to interpret results!

### References

[Diem15] T. Diemont, M. van Veen and R. Warmoeskerken, *Cyber in the audit*, Compact 2015/3.

[Torc13] S. Torchia and M. Lundin, *SOC2: Thorough reports critical to Cloud Service Provider Assurance*, KPMG.com, 2013.

**Jaap van Beek** is a partner with KPMG Advisory N.V. and has nearly 30 years of experience with performing assurance engagements. His client focus is on the financial services sector. He is the EMA service line leader IT attestation for KPMG.