**Compact ("computer and accountant") appeared for the first time in 1974. Dries Neisingh was involved right from the very start. He was the editor-in-chief for many years up until 2003. His first publication dealt with "The use of the computer by the accountant". This title denotes the start of a development that could not be predicted. Since his retirement Dries continues to follow the profession at a suitable distance from sunny Spain via the newspaper and via Compact, which he still very much enjoys reading. He sometimes sees old wine in new bottles (such as a mole at the police who is given too many access rights), sometimes fascinating cases (such as Volkswagen's rigged software) and sometimes subject matter that is so technically complex that it even exceeds his powers of imagination. Dries places two fascinating developments within the perspective of the past and looks to the future.**

# For How Long Will IT Auditors Still Audit around Microchips?

**Andries Neisingh**

*In your farewell speech in 2002 as professor of the auditing reliability and security aspect of IT at Groningen University, you said, among other things, about the future:*

"The integration of IT in and across business processes will continue. Logistics and process automation are already the order of the day and integrated with the administrative and financial processes. Robotization has also found its way into the business world. I expect that accountants will be more often confronted with fully automated production processes, logistics and administration. They will therefore be required to assess these processes on reliability measures. Along with the control measures that are taken in those processes, the continuity and the quality of the IT organization will continue to be of increasing significance. User controls are no longer possible or can hardly be used anymore, while the IT organization still needs to provide the necessary guarantees."

This development is still in full swing. The IT function is becoming increasingly embedded in organizations. It has often become the most important link. IT systems must be correctly developed and installed; monitoring this is a task for IT auditors. And this is becoming increasingly difficult. More and more functionality is moved to microchips, printed circuit boards and operating system software. These are important system building blocks and we don't know what is actually installed on them. An update occasionally arrives to seal leaks, but

The rigged software at Volkswagen indicates an audit question for the IT auditor for the coming decades

## A digital safe, only accessible within the organization, is perhaps the future

nobody knows how dangerous these leaks were. The rigged software at Volkswagen shows that functionality in microchips is not adequately monitored. We test the defined functionality and do not expect fraudulent functionality. But we will have to know what is in these microchips, because we can only create an adequate system of internal control and security measures if these building blocks are correct. I cannot imagine that the chip manufacturers and the companies that provide the software for them will voluntarily offer up their company secrets. But the user organizations want "things" to be verifiable. A construction can possibly be thought up where IT auditors provide statements comparable with assurance statements. In 2002, I pointed out that there were still accountants who carried out audits around the computer. This is unthinkable nowadays. But how long can we continue to audit around microchips, printed circuit boards and operating system software? This is the question that confronts us in the coming decades.

*You also wrote the following forecast in your farewell speech:*

> "The use of the Internet will continue to increase even further. Now that the Internet is used for all kinds of purposes, also for matters that cannot bear the light of day, a need will arise to regulate in some way or another the use, respectively the monitoring, of the data transport. Technological solutions will have to be sought to be able to immediately determine the nature of the data transport. I see absolutely no solution in regulation, for example, by prohibiting the use of encryption."

Prohibiting or regulating the use of encryption has happily not occurred. This was also completely unworkable; I warned about this. Regulating the monitoring of data transport is a current topic of discussion. A much less significant factor, at that time, was the emergence of wifi, smartphones, laptops and working from home. Everything is now connected and it is very easy if you can simply log in and access your work at home, on the road or in your hotel. But this also makes an organization vulnerable for hackers and careless or malevolent employees. Company secrets were previously on paper in the safe. You were not allowed to take these papers outside. Why should it now be possible via the computer or the smartphone? Organizations must seriously ask themselves whether they have to deploy all the technological possibilities that make it possible for everybody to access all the information within the organization from any place and at any time. I can imagine that in the future the IT system on which company secrets are stored, is not connected to other systems and that it is only accessible within the organization via carefully thought-out authorizations and, if necessary, in a secured area. A kind of digital safe.

**Andries Wybe Neisingh** (1942) is a retired KPMG Information Risk Management partner in the Netherlands. During his working life he was a chartered accountant, a chartered EDP Auditor and professor of auditing reliability and security aspect of IT at Groningen University. He was involved with Compact right from the first issue in 1974 and was the editor-in-chief for many years.