The societal importance of assurance and certification

Introduction

Good morning ladies and gentlemen. It's my pleasure to be able to address you this morning. My name is Irene Vettewinkel and I'm the vice chair of NOREA, the professional body for IT auditors in the Netherlands. NOREA is a drafting member of the CSPCert working group. We work closely together with Zeker-OnLine and the Partnering Trust project of the Dutch Ministry of Economic Affairs and Climate to bundle our expertise in defining and validating criteria for online computing.

Today I want to talk to you about the societal importance of assurance and certification. A relevant topic since the new Cybersecurity Act passed the European Parliament including a certification framework for cybersecurity and today the CSPCert group will present a certification scheme for cloud security.

Background on NOREA and the IT audit profession in the Netherlands

Please allow me to take a few moments to tell you a bit about NOREA. NOREA was founded in 1992 by a group of large Dutch multinational organizations including audit firms, financial institutions, government and universities. It was founded based upon a strong belief that the increasing role of information technology required skills that go beyond traditional audit capabilities and that especially in financial audit teams there was need for ICT specialists that could operate at the same level as those responsible for the financial audit.

Today, NOREA is the professional association for over 1.800 registered Dutch IT auditors. They all hold a post master degree in IT auditing. A degree obtained at one of the 4 universities in the Netherlands that offer a specific IT audit program. A program of at least 60 ECTS (which is equivalent to over 1.600 hours of study). NOREA is an affiliate member of IFAC which means that all practitioners have to comply with IFAC standards and guidelines. These include Code of Ethics, education and CPE standards, quality control and applicable standards for the execution of engagements. And what is very important is that NOREA is accredited by the Dutch Association of Certified Public Accountants. This means that registered IT auditors can participate in financial audits and be ultimately responsible for planning and execution of the audit of ICT systems. There is no other country in the world that has this.

The Netherlands has a strong and active IT audit profession. We do need that as the Netherlands as a result of it geographical location has a very sophisticated ICT infrastructure and a strong ICT industry. Most of the transatlantic cables for datacommunication come ashore in the Netherlands. And all global providers have major datacenters located somewhere in the Netherlands. The Netherlands is the second largest colocationprovider in Europe. And after the Brexit we will be the largest. In 2018 the Netherlands was home to 198 multi-tenant datacenters with a total capacity of 1.300 Megawatts and over 308.000 m2 of datafloor. A lot of them are located in a 20 miles radius from where we are now. That's why we say that there is a lot of cloud around Amsterdam and Schiphol. You don't

always see it, but it's there! According to the Dutch Bureau of Statistics over 98% of the people in the Netherlands have internet access which is the highest rate in the European Union.

Of course the IT audit profession has changed significantly since the institution of NOREA in 1992. Over the past 27 years we've seen a growing integration of ICT in our daily lives. Back in 1992 the Internet had only just been invented. Datacommunication was done by means of tapes and floppy disks. Transactions were processed and printed on paper. The Internet and mobile computing brought ICT really into our daily lives. It is now no longer a tool for business; it's part of our personal life. And it doesn't end here. Yesterday's innovations are used today to develop tomorrows innovations. The speed of change is phenomenal. This is what makes this era so fascinating. It took mankind over 500.000 years to stand up and create the first steam machine. It took us 130 years to discover electricity and turn it into artificial intelligence. It took us 23 years to turn a mobile phone into a smart phone. In the development of mankind we're currently in a asymptotic curve. In fact, this exponential growth is what Kurzweil already described back in 1999 in his Law of Accelerating Returns

The societal importance of ICT

The impact of ICT on our society is huge. Cisco predicts that by 2022 there will be 4.8 billion Global Internet users and 28,5 billion networked devices and connections. According to Ericsson 18 billion of them will be IoT devices. Over the past 20 years digital business has moved from an experiment to mainstream. Eurostat calculated that 55% of enterprises were "highly dependent" on cloud computing in 2018. And IDC estimates that the current economic value of digital transformation is 19 trillion US dollars. These figures clearly show the economic impact of ICT. But look around in your daily life. What would your life look like without ICT? Without ICT we would not be in this room today. We probably wouldn't need to be anyway.

This speed of change calls for new control mechanisms. With the change in information technology and its increased use, new threats emerge and their impact increases. This has a significant impact on the risk assessment. We're on an information highway that gets more crowded every day and where the speed gets higher and higher. And to make things more exciting, a substantial part of this highway runs through the clouds. All ingredients for a severe collision are present I would say.

We see this every day. Cyberattacks are in the daily news. In most cases they don't even make the news because organizations are too embarrassed to go public. But in other cases they are big news, for instance when elections are compromised. Or when privacy is compromised and organizations are legally compelled to report data leaks. Cloud computing is an important factor in this. Nowadays we increasingly buy services instead of hard- and software. People expect their cloud provider to be professional and to look after system management and security as a good housefather. What a lot of people don't know is that you seldom buy a single service. The service you buy generally consists of a chain of services that together make it possible for you to use the service. Your SaaS provider will buy capacity from a platform provider; sometimes use hosting services or managed services. For you as a user this in most cases is completely invisible. We call them subservice providers and I promise you that things can go wrong within each subservice provider!

When we do buy a piece of hardware, let's say a new car, we hardly realize that this "thing" is connected to other systems that register our movements and habits. We say it's connected to "the cloud" meaning that we don't know what is happening. Our trust in our providers is seemingly endless. Although we don't know what is happening, we trust that our car will operate reliably in the morning after a nightly download has significantly changed its functionality.

Keeping us safe

Now what should I do to be able to step into my car in the morning in the substantiated trust that it's safe to drive. That the money I wire transfer will arrive in the right account. That my medical records don't get compromised. Given the large number of services I use every day, surely I cannot be expected to take a dive into each and every one of them to see how safe they are!

Clearly there is a task for the government here. In a lot of areas this is already the case. Especially in areas that feature physical risks Governments have already implemented licensing and certification schemes. And with great success! Cars have become much safer because of NCAP testing and MOT testing or APK as we call this in the Netherlands. The new EU regulation on type-approval requirements will again make our cars safer and improve the safety potential of automated and connected vehicles. However this is only possible if the ICT capabilities used are reliable and safe.

Therefore it is logical that the EU is now implementing a certification scheme for security of cloud services. And this is where IT auditors come in.

IT auditors are essentially assurance providers: they deliver trust based upon a thorough examination of the subject. For this they use protocols defined by the International Auditing and Assurance Standards Board (IAASB). These protocols are described in the International Standards on Assurance Engagements (ISAE). Application of these standards is required by among others, regulators and supervisory bodies.

The outcome of an IT audit is usually an attestation report: a comprehensive, long form report including

- a description of the scope of the audit, including the subservice organizations and services involved;
- a description of the "system": the organization, ICT systems used, procedures and controls;
- the control objectives relevant to the objective of the audit;
- the audit procedures performed;
- the results of the audit procedures;
- in some cases a management statement or assertion on the operating effectiveness of the "system";
- and an auditor's opinion on the fair presentation of the management statement and achieving of the objectives.

An assurance report is different from a certificate. The assurance report provides much more information. It is much more detailed and it also contains all exceptions noted during the audit procedures. Financial auditors, regulators and supervisory bodies require this information to be able to integrate this in their work. But normal end users prefer a certificate telling them the cloud service is safe. This implies a big responsibility for the party issuing the certificate to make sure that the requirements are met. In some certification schemes like ISO this is done by not taking the operating effectiveness into account. In practice almost every audit that also tests the operating effectiveness of controls and procedures shows findings and exceptions. Evaluating the impact of these findings and exceptions is one of the most complex tasks of an IT audit. But in our opinion essential for answering the question whether or not a service is reasonably safe.

Furthermore an assurance report requires disclosure of sub service providers and services. In our opinion the scope of a cloud security certificate should not be limited to the organization itself of in

most cases a SaaS provider. The scope should take into account the entire service including the subservices used.

An attestation report can be used as the basis for issuing a cloud security certificate and in our opinion should be used for services that require an assurance level “high”.

Conclusion and recommendations

In conclusion, NOREA strongly supports the cloud security certification initiative. We call upon the European Commission and Dutch Government to expeditiously continue with the implementation of the Cybersecurity Act. And NOREA will provide all support needed to do so. We do have three recommendations.

1. First of all we sincerely hope that the new European Cybersecurity Certificate will not get lost in the jungle of ICT certifications we already see today. Most people rely on a certificate but do not understand its scope or significance. Most people have heard of ISO certificates and some people know that ISO 27001 has got something to do with information security but only very few know the real significance of these certificates. There is a task for the European Commission and ENISA to actively promote and inform the public what the meaning and the value of this certificate is. What does it mean. And why you should choose for cloud services that have this certificate if you have a choice.
2. Secondly a lot of service providers that deliver services to professional organizations already have some form of assurance reporting in place because their clients’ supervisors, regulators and auditors require this. The requirements of the European Cybersecurity Certificate should in our opinion align with these reports in order to reduce the administrative burden and compliance cost for service providers. And safeguard the global competitive position of European providers compared to non-European providers
3. Finally, The Cybersecurity Act features a strong but complex certification framework. But unfortunately complexity equals cost. The Cybersecurity certification framework has the potential to perish in its own success. The European Commission together with ENISA should actively seek for efficient ways to monitor issuance and revoking of certificates in order to reduce the cost for both the European Union, National governments and conformity assessment bodies. And by doing so safeguard the competitive position of European cloud service providers. After all that is one of the objectives of the Digital Single Market.

I thank you for your attention and the opportunity to speak. I am happy to take questions if there is time for that.