

**datum**                    **onderwerp**  
1 mei 2018                Summaries presentations session 2 - Eurorai April 2018

**pagina**                    **auteur**  
1 van 3                    Paul Hofstra, Court of Audit of Rotterdam (Netherlands)

*Mr Kersting* - Summary: Audit of IT security: from niche to necessity.

- Mr Kersting started with an overview of the basic conditions in relation to IT security: there is a very big variety of IT networks and there is no obligation to comply with uniform minimum IT safety standards. There is also a legal problem because of the general prohibition of shared administration.
- Then Mr Kersting focuses on the audit standards of the court of audit on state and federal level. The paper of courts of audit offices information security management requires among others the existence of risk analyses; independent IT security officer and management responsibility for IT security.
- But at the same time there is a very big lack of skilled professionals up to 55.000 in 2017.
- Finally mr Kersting stated that on base of the findings of the Court of Audit of Brandenburg there has to be more IT resources, more cooperation between courts of audit and permanent internal awareness of “good cyber hygiene”.

-----

*Mr Cunningham* - Summary: Cyber Security in Wales.

- Mr Cunningham starts his presentation with a very clear definition of cyber security and concludes that cyber security is more about people and management processes attitude and approach than technical IT solutions. The current approach in Wales is focused on IT risk assessments for each audited body (National Health Service; local government; Welsh Government and others). The advantages of this approach is as mr Cunningham emphasizes; simpler and less resource intensive than traditional audit work.
- Some of the findings in 2003 for NHS and local government were: unclear responsibility for datasets and incomplete risk registers. These findings were compared with 2011 and 2017. Mr Cunningham concludes in the journey of audited bodies an increasing lack of direction, awareness and cohesion on strategic level.
- In that context the Wales audit office made risk assessments that highlight the key issues and organized events to raise awareness with very positive feedback.
- Finally mr Cunningham indicates some exiting work in the pipeline on data analytics and promises next time more.

-----

*Mrs Diamond* - Summary: Auditing cyber security.

- Mrs Diamond started her presentation with some displeasing cyber facts: almost 60% of councils in Scotland were hit by cyberattacks and NHS trusts hit by cyberattacks asks patients not to come to hospital. It is as Mrs Diamond put it a matter of life and death!
- Audit Scotland is especially focusing on assessing cyber security risks and emphasizes the importance of culture and behaviours. Cyber resilience is as much a cultural issue as a technical one.
- At working level there is according to Mrs Diamond much interaction between Audit Scotland and internal audit, Scottish Government and other scrutiny bodies and where the main skills of Audit Scotland are focused primarily on auditing digital and digital auditing.

**datum**

1 mei 2018

-----

**pagina**

2 van 3

*Mr Minguillón and Mr Salom* - Summary: Information security and cyber security in the working methods of the audit office of the Valencian community.

- Mr Minguillón starts his presentation with a short outline of the threats and challenges to be faced by the audit institutions: cybercrime is one of them. The digital revolution requires action in different areas and as Mr Minguillón underlines: The challenges of the immediate future require a proactive response from auditors. Furthermore public auditors have to develop new skills specializing in data analytics, big data and cyber security. In relation to cyber security there is a new Practical Audit Guide (GPF-OCEX 5311). The purpose of this guideline is to raise the awareness of cyber security in the activities performed by auditors.
- And Mr Salom has showed us finally some examples of cyber security testing in relation to administrative privileges as part of the CIS controls.

-----

*Mrs Tulyakova* - Summary: State financial control and audit in digital reality.

- Mrs Tulyakova starts her presentation with an overview of the worldwide cyber threats where she emphasizes the possible effects of inefficient security of systems and networks in terms of loss and theft of assets and funds and destination of critical infrastructure.
- In the Vladimir region the state administration has invest more than € 30 mio in ICT and 347.000 households received an access to high speed internet. In that context Mrs Tulyakova underlines that there is a big need for auditors with knowledge on cyber security, risk management and data processing and data analytics.
- And from the perspective of the account chamber she emphasize the importance of measures on providing information security. For example adaption of internal documents on information security; briefing of users and program-technical tools providing information security.

-----

Mr Cotton - Summary: Cyber security and information security: the French experience.

- Mr Cotton started his presentation with an overview of early state interventions in the fight against cybercrime and emphasizes the importance of awareness of the treats, especially in relation to the critical infrastructure.
- Then mr Cotton made clear that in the context of new challenges owing to growing number of networks and servers and to widespread use of encryption and trace obfuscation there is a big need for effective laws to repress them.
- And where the law is providing for security and certification rules, it is the National Cyber Security Authority (created in 2009) that will perform the audits on records and on the spot.
- In that perspective mr Cotton asked himself the question if there is new competition for the traditional audit institutions. He noticed that regional audit institutions have no specialized methods for cyber security audits to date and emphasizes the high costs for a basic cyber security audit (more than € 60.000,00).  
Mr Cotton points out that French audit institutions have to play a role in assessments audit.
- Finally he underlines the importance of the new GDPR in relation to personal data security.

**datum**

1 mei 2018

**pagina**

3 van 3