EURORAI Seminar: “Conducting audits on cyber and information security”

Rotterdam, April 2018

SESSION 1 CONCLUSIONS

Ladies and Gentlemen, dear colleagues,

Session 1 featured three fascinating presentations, including empirical evidence from cyber and information security audits relating to the scope of the audits, the methods and approaches that they use, and the results achieved from them.

I would like to thank the three speakers for their stimulating talks.

The second presentation, by qualified engineer Andreas Preslmayr from the Vienna Court of Audit, highlighted current opportunities and challenges in auditing cyber and information security.

Before he had even finished his introduction, it had become clear that the *Land* Vienna, the city of Vienna, is a region that is very much in the throes of digitalisation and is busy applying state-of-the-art information and communication technologies.

From an audit perspective, therefore, significant impetus is required to deliver innovation as regards identifying information security in terms of defining risk areas and implementing new methods, but also organising the audit itself.

Mr Preslmayr clearly showed the tension created between the type of information system and the type of business process involved.

His additional comments on identifying the risk areas and core issues at play in an information security audit were interesting. It became obvious that the risk areas are connected to the well-known issues from the relevant specialist areas.

He went on to highlight the requirements that have to be met for using new information systems and whose examination represents the starting point for any audit.

The application and continued development of process mining as a data analysis method was also touched on. The questions who?, when?, what? and how? have to be answered in this regard.

As far as organising an information security audit is concerned, the specialist expertise and experience of the auditors in particular are being confronted with new challenges. It was made clear that, although the ongoing further development of skills and knowledge is crucial, there are considerable practical problems in recruiting suitable IT staff.

Information security auditing has repercussions for the bodies audited. Meeting protection targets is now becoming a relevant factor, and users are grappling with the effects head on. For example, authorisations are being scrutinised, as are the actual effectiveness and efficiency and the process steps required, stretching right up to an overhaul of data structures.

The Vienna Court of Audit has solid experience with audits, including IT service management, ICT security regulations for external customers and electronic claims reporting applications through to preparing the accounts for the city of Vienna in SAP.

To close, the experience gained to date was summarised in a few general points:

- Reflecting on the rapid march of new technology
- Access to “security by design”
- Raising awareness of the implementation of audit authorisations
- Taking account of the significant outlay involved
- Rapid growth in the use of ICT systems, including the new requirements that this brings.