The effects of auditing on information security at NRENs and universities

A comparison between a state enforced and a community organised effort.

Type of session: presentation (25 minutes)
Autors/presenters: Rolf Sture Normann (Uninett) and Alf Moens (SURFnet)

KEYWORDS
Information security management, audit, compliance, frameworks, ISO27001

Information security is recognised as a key control area for NRENs and universities. Though legislation has been in place for several decades universities only just now start to implement measures to get in control for information security. The upcoming new European privacy legislation seems to be an important driver to accelerate this process. In several countries NRENs play a key role in boosting and supporting the implementation of information security management within their subsidiaries. The approach can be different per country. In this session we will discuss the approach in Norway and in the Netherlands. They differ widely, but both are successful in reaching the goal of improving information security at the NREN and her subsidiaries.

In the Netherlands the approach is strongly community based. Since 2013 the security professionals of the SURFnet connected institutions have been working together in exchanging experiences and building a comprehensive framework of policies, guidelines and starterkits. Supported by SURF they have set up a control framework and started auditing, firstly with self-assessments and as of 2015 with peer-auditing. Through SURF both the Dutch government and the national supervising bodies are involved to gain broad support for this approach. Key success factor is the involvement of all key players of the organisations, both board and senior management as well as ICT management, security professionals and internal audit. Now, after several years of auditing and assessing and encouraging, improvement is visible in both the maturity of information security and in the quality of the security management process.

In Norway the approach has been driven by compliance. The Norwegian government has given Uninett funds to both assists universities to implement information security management and to audit these implementations. Whereas the larger universities were able to manage these improvements themselves, the smaller ones where assisted by Uninett.
After the Office of the auditor general of Norway was auditing the HE sector, they found that the sector did not comply with the level of security the legislation demanded. Because of lack of compliance with both the privacy law and the ISO27001/2 standards they asked the ministry of education to take actions. The result was that UNINETT was asked to build up a secretary for information security matters in the HE sector. The mandate is to help doing risk assessments, audits, policy work and implement a information security management system based on the ISO27001 standard. The ministry of education is demanding the institutions to use this secretary, and the institutions are measured on this use. That gives the secretary necessary commitment and attention to the institutions.

Uninett also started a research project to find out why the implementation of a information security management system seems to be so difficult. The report was used to create a framework that fits with the institutions organisation and working matters. Because of this approach great improvement in information security is achieved.

Both approaches prove to be successful, both approaches use similar tools and methodologies, funding, realisation and motivation though are opposite.

VITAE

Rolf Sture Normann

Rolf Sture Normann is CISO for the UNINETT, and a manager for the Norwegian secretary for information security. In 1987 Rolf Sture graduated as a bachelor of computer technologies. He has been working with information security since 1996 in both the financial sector and in the public sector. He wrote together with Tommy Tranvik a book “Information security in the public sector” with risk management as a main topic. Rolf Sture is a Certified Information System Auditor (CISA, ISACA) and Certified in Risk and Information Systems Control (CRISC, ISACA), and he is e member of the steering committee of the Terena SIG on Information Security Management.

Alf Moens

Alf Moens is the Corporate security officer of SURF and responsible for information security management at SURF, SURFnet, SURFmarket and SURFsara. He coordinates compliance and control in information security for the SURF and SURFnet subsidiaries. In 2007 Alf graduated as Master of Information Security Management at Tilburg University (TIAS). He has been security manager at Delft university for 8 years and is a board member of the Dutch association of information security professionals (PvIB). Alf is one of the initiators of the TERENA Special Interest Group in information Security Management (SIG-ISM) and is chairman of the steering committee of this SIG.