Knowledge Requirements for ISMS Auditors

The following requirements apply to the audit team as a whole, or to the auditor if working individually.

In each of the following areas at least one audit team member shall take responsibility within the team:

- managing the team, planning the audit, and audit quality assurance processes;
- audit principles, methods and processes;
- management systems in general and ISMS in particular;
- legislative and regulatory requirements for information security applicable to the organization being audited;
- information security related threats, vulnerabilities and incidents, particularly in relation to the organization being audited and comparable organizations, for example an appreciation of the likelihood of various types of information security incident, their potential impacts and the control methods used to mitigate the risks;
- ISMS measurement techniques;
- related and/or relevant ISMS standards, industry best practices, security policies and procedures;
- information assets, business impact assessment, incident management and business continuity;
- the application of information technology to business and hence the relevance of and need for information security; and
- information security risk management principles, methods and processes.

The audit team must be competent to trace indications of security incidents in the ISMS back to the appropriate elements of the ISMS, implying that the auditors have appropriate work experience and practical expertise in relation to the items noted above.

This does not mean that every auditor needs the complete range of experience and competence in all aspects of information security, but the audit team as a whole should have a sufficiently broad range of experience and sufficiently deep competencies to cover the entire scope of the ISMS being audited.