CS4062-CSF: Information Assurance & Regulatory COmpliance

Summary & Recommended Reading

1 Aims and Objectives

- Gain an understanding of, and doing, Information Assurance (IA).
- Understand the relationship between IA and Regulatory Compliance.
- Gain an understanding of Information Security Management Systems (ISMSs)
- How to achieve and manage IA through use of an ISMS.

2 Summary

- Information Assurance is:: (a) Risk Management;; (b) Defining policies and implementing controls;; (c) Compliance with legislation, regulation, and standards; and; and (d) Ensuring compliance.
- ISMS are used to establish, implement, operate, monitor, review, maintain and improve IA confidence.
- Provide a Plan Do Check Act (PDCA) cycle to do so.
- `ISO 27K` Series provides a set of best practices for achieving and managing Information Assurance.
  - **ISO 27001**: Provides security management
  - **ISO 27002**: Provides security controls

Reading List

Required

[Tas09] Igli Tashi. 'Regulatory Compliance and Information Security Assurance'. In: *Availability, Reliability and Security, 2009. ARES '09. International Conference on.* Mar. 2009, pp. 670–674. DOI: 10.1109/ARES.2009.29.

Recommended

[AW07] Sigurjon Thor Arnason et al. 'Implementing an Information Security Management System: Plan-Do-Check-Act'. In: *How to Achieve 27001 Certification: An Example of Applied Compliance Management.* 2007, pp. 97–162.

[Had+11] S. Haddad et al. ‘Operational Security Assurance Evaluation in Open Infrastructures’. In: *Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference on*. Sept. 2011, pp. 1–6. DOI: 10.1109/CRiSIS.2011.6061831.

[HMG05] HMG. *Risk Management and Accreditation of Information Systems*. English. Online. Centre for the Protection of National Infrastructure (CPNI), Aug. 2005. URL: http://www.cpni.gov.uk/documents/publications/2005/2005003-risk_management.pdf.

[KS06] Bilge Karabacak et al. ‘A Quantitative Method for ISO 17799 Gap Analysis’. In: *Computers & Security* 25.6 (May 2006), pp. 413–419. ISSN: 0167-4048. DOI: 10.1016/j.cose.2006.05.001. URL: http://www.sciencedirect.com/science/article/pii/S0167404806000757.

Further

[CCR12] CCRA. *Common Criteria for Information Technology Security Evaluation*. English. Common Criteria Recognition Arrangement (CCRA) Management Committe. 2012. URL: http://www.commoncriteriaportal.org/.

[Com12a] European Commission. *European Commission on Data Protection*. English. European Commission. 2012. URL: http://ec.europa.eu/justice/data-protection/ (visited on 20/11/2012).

[Com12b] European Commission. *European Union Directives*. English. European Commission. 2012. URL: http://eur-lex.europa.eu/ (visited on 20/11/2012).