Information and Cyber Security Assurance in Organisations

ITX8090

VIII

Practical info

01.09.15
08.09.15
15.09.15
22.09.15
~~29.09.15~~
06.10.15
13.10.15
20.10.15
~~27.10.15~~
03.11.15
~~10.11.15~~
17.11.15
24.11.15
01.12.15
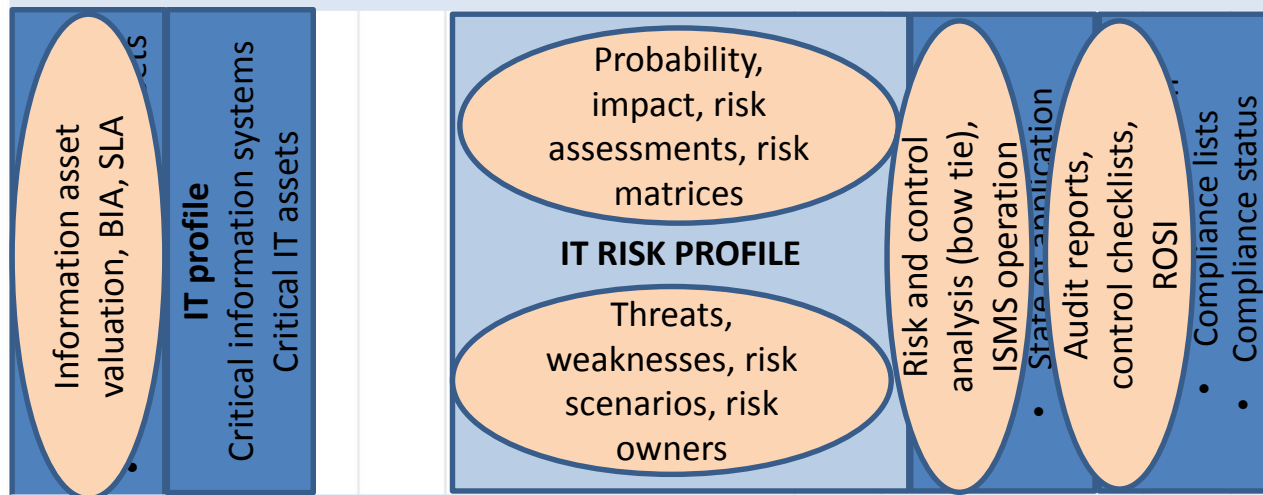08.12.15
15.12.15

Practical info

Course page

https://courses.cs.ttu.ee/pages/ITX8090

Concept progress

Legal obligations for IT security, data protection, business continuity (for example data protection act, emergency act, etc …) and internal goals.

Information asset valuation, BIA, SLA

IT profile
Critical information systems
Critical IT assets

Probability, impact, risk assessments, risk matrices

IT RISK PROFILE

Threats, weaknesses, risk scenarios, risk owners

Risk and control analysis (bow tie), ISMS operation

State or application

Audit reports, control checklists, ROSI

Compliance lists
Compliance status

IT risk and information security management actions (analysis, assessments, overviews; changes in profiles and impact to risks, improvements in controls, need to audit, test etc …)

IS objectives

Set information security objectives:

1. Consistent with the information security policy;

2. Be measurable;

3. Take into account applicable information security requirements, and results from risk assessment and risk treatment;

4. Be communicated;

5. Be updated as appropriate.

IS objectives

When planning security objectives:
1. What will be done?
2. What resources will be required?
3. Who will be responsible?
4. When it will be completed?
5. How the results will be evaluated?

IS controls

A.5 Information security policies

A.5.1 Management direction for information security

A.5.1.1 Policies for information security

A.5.1.2 Review of the policies for information security

IS controls

A.6 Organization of information security

A.6.1 Internal organization

A.6.1.1 Information security roles and responsibilities

A.6.1.2 Segregation of duties

A.6.1.3 Contact with authorities

A.6.1.4 Contact with special interest groups

A.6.1.5 Information security in project management

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy

A.6.2.2 Teleworking

IS controls

A.7 Human resource security

A.7.1 Prior to employment

A.7.1.1 Screening

A.7.1.2 Terms and conditions of employment

A.7.2 During employment

A.7.2.1 Management responsibilities

A.7.2.2 Information security awareness, education and training

A.7.2.3 Disciplinary process

A.7.3 Termination and change of employment

A.7.3.1 Termination or change of employment responsibilities

IS controls

A.8 Asset management

A.8.1 Responsibility for assets

A.8.1.1 Inventory of assets

A.8.1.2 Ownership of assets

A.8.1.3 Acceptable use of assets

A.8.1.4 Return of assets

A.8.2 Information classification

A.8.2.1 Classification of information

A.8.2.2 Labelling of information

A.8.2.3 Handling of assets

A.8.3 Media handling

A.8.3.1 Management of removable media

A.8.3.2 Disposal of media

A.8.3.3 Physical media transfer

IS controls

A.9 Access control

A.9.1 Business requirements of access control

A.9.1.1 Access control policy

A.9.1.2 Access to networks and network services

A.9.2 User access management

A.9.2.1 User registration and de-registration

A.9.2.2 User access provisioning

A.9.2.3 Management of privileged access rights

A.9.2.4 Management of secret authentication information of users

A.9.2.5 Review of user access rights

A.9.2.6 Removal or adjustment of access rights

IS controls

A.9.3 User responsibilities

A.9.3.1 Use of secret authentication Information

A.9.4 System and application access control

A.9.4.1 Information access restriction

A.9.4.2 Secure log-on procedures

A.9.4.3 Password management system

A.9.4.4 Use of privileged utility programs

A.9.4.5 Access control to programm source code

IS controls

A.10 Cryptography

A.10.1 Cryptographic controls

A.10.1.1 Policy on the use of cryptographic controls

A.10.1.2 Key management

IS controls

A.11 Physical and environmental security

A.11.1 Secure areas

A.11.1.1 Physical security perimeter

A.11.1.2 Physical entry controls

A.11.1.3 Securing offices, rooms and facilities

A.11.1.4 Protecting against external and environmental threats

A.11.1.5 Working in secure areas

A.11.1.6 Delivery and loading areas

IS controls

A.11.2 Equipment

A.11.2.1 Equipment siting and protection

A.11.2.2 Supporting utilities

A.11.2.3 Cabling security

A.11.2.4 Equipment maintenance

A.11.2.5 Removal of assets

A.11.2.6 Security of equipment and assets off-premises

A.11.2.7 Secure disposal or reuse of equipment

A.11.2.8 Unattended user equipment

A.11.2.9 Clear desk and clear screen policy

IS controls

A.12 Operations security

A.12.1 Operational procedures and responsibilities

A.12.1.1 Documented operating procedures

A.12.1.2 Change management

A.12.1.3 Capacity management

A.12.1.4 Separation of development, testing and operational environments

IS controls

A.12.2 Protection from malware

A.12.2.1 Controls against malware

A.12.3 Backup

A.12.3.1 Information backup

A.12.4 Logging and monitooring

A.12.4.1 Event logging

A.12.4.2 Protection of log information

A.12.4.3 Administrator and operator logs

A.12.4.4 Clock synchronisation

IS controls

A.12.5 Control of operational software

A.12.5.1 Installation of software on operational systems

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities

A.12.6.2 Restrictions on software installation

A.12.7 Information systems audit considerations

A.12.7.1 Information systems audit controls

IS controls

A.13 Communications security

A.13.1 Network security management

A.13.1.1 Network controls

A.13.1.2 Security of network services

A.13.1.3 Segregation in networks

A.13.2 Information transfer

A.13.2.1 Information transfer policies and procedures

A.13.2.2 Agreements on information transfer

A.13.2.3 Electronic messaging

A.13.2.4 Confidentiality or nondisclosure agreements

IS controls

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

A.14.1.1 Information security requirements analysis and specification

A.14.1.2 Securing application services on public networks

A.14.1.3 Protecting application services transactions

IS controls

A.14.2 Security in development and support processes

A.14.2.1 Secure development policy

A.14.2.2 System change control procedures

A.14.2.3 Technical review of applications after operating platform changes

A.14.2.4 Restrictions on changes to software packages

A.14.2.5 Secure system engineering principles

A.14.2.6 Secure development environment

A.14.2.7 Outsourced development

A.14.2.8 System security testing

A.14.2.9 System acceptance testing

A.14.3 Test data

A.14.3.1 Protection of test data

IS controls

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

A.15.1.1 Information security policy for supplier relationships

A.15.1.2 Addressing security within supplier agreements

A.15.1.3 Information and communication technology supply chain

A.15.2 Supplier service delivery management

A.15.2.1 Monitoring and review of supplier services

A.15.2.2 Managing changes to supplier services

IS controls

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

A.16.1.1 Responsibilities and procedures

A.16.1.2 Reporting information security events

A.16.1.3 Reporting information security weaknesses

A.16.1.4 Assessment of and decision on information security events

A.16.1.5 Response to information security incidents

A.16.1.6 Learning from information security incidents

A.16.1.7 Collection of evidence

IS controls

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

A.17.1.1 Planning information security continuity

A.17.1.2 Implementing information security continuity

A.17.1.3 Verify, review and evaluate information security continuity

A.17.2 Redundancies

A.17.2.1 Availability of information processing facilities

IS controls

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

A.18.1.1 Identification of applicable legislation and contractual requirements

A.18.1.2 Intellectual property rights

A.18.1.3 Protection of records

A.18.1.4 Privacy and protection of personally identifiable information

A.18.1.5 Regulation of cryptographic controls

IS controls

A.18.2 Information security reviews

A.18.2.1 Independent review of information security

A.18.2.2 Compliance with security policies and standards

A.18.2.3 Technical compliance review

Practice

Exercise IX

PhD Andro Kull
CISA, CISM, CRISC, ABCP
E-mail: Andro@consultit.ee
Skype: andro.kull