TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

IX

Practical info

06.09.2016 – Lecture 1 (introduction, CSMS)
13.09.2016 – Lecture 2 (context, regulations, assets, BPM, BIA)
20.09.2016 – Lecture 3 (asset valuation, CIA, IT mapping, governance)
~~27.09.2016 – Lecture 4 (self reading - OCTAVE)~~
04.10.2016 – Lecture 5 (IT risk assessment, methodology, ISO 27005)
11.10.2016 – Lecture 6 (IT risk management, KRI, CE)
~~18.10.2016 – Lecture 7 (IS management, ISO 27001)~~
~~25.10.2016 – Lecture 8 (self reading – IS roles)~~
01.11.2016 – Lecture 9 (IS measures planning, ISO 27002, IEC 62443)
08.11.2016 – Lecture 10 (risk+countermeasures analysis, bowtie, CMM)
15.11.2016 – Lecture 11 (IT auditing)
~~22.11.2016 – Lecture 12 (IS management metrics, IS economics)~~
29.11.2016 – Lecture 13 (Business continuity, testing)
06.12.2016 – Seminar 1 (around 10 HW presentations)
13.12.2016 – Seminar 2 (around 10 HW presentations)
20.12.2016 – Seminar 3 (around 10 HW presentations)
27.12.2016 – Exam (need confirmation)

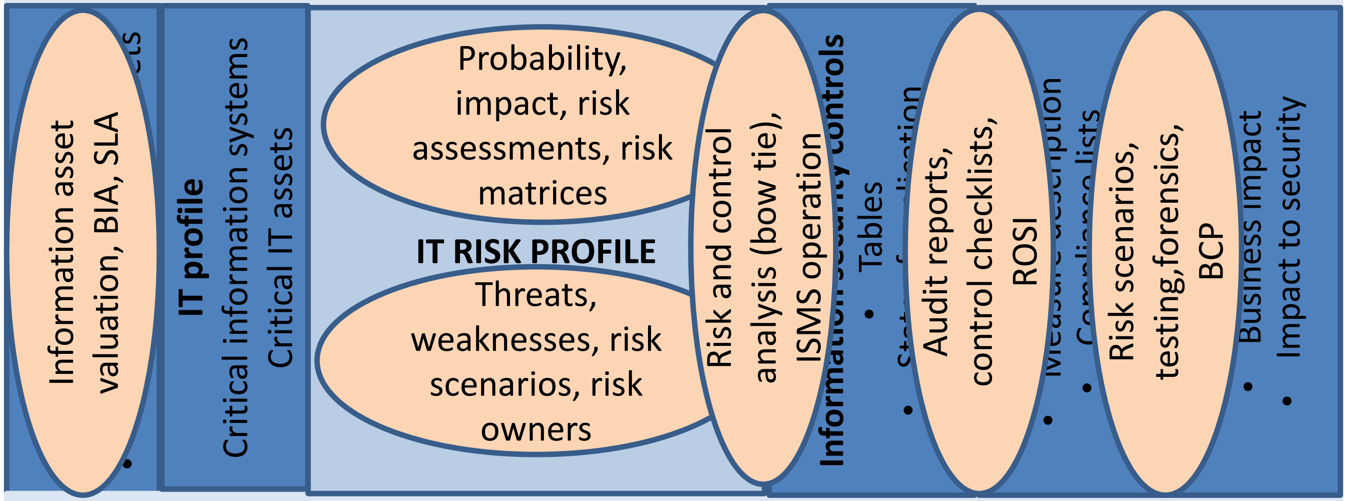
Practical info

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
Tables
Audit reports, control checklists, ROSI
Risk scenarios, testing,forensics, BCP
Business impact
Impact to security

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 …)

Course - evaluation

Evaluation criteria

1) The course contains obligatory homework assignment. Maximum summary points for assignment: 20.
2) Homework assignment deadline 02.12 (via e-mail Andro@consultit.ee)
3) In order to pass the course, each student has to pass the written exam. Maximum points: 80.
4) Final evaluation The final grade for each student is calculated using a summary score of the homework assignments and the exam, ie. 20% for the homework, 80% for the exam.

Course - evaluation

The grades are assigned as follows:

score >= 90 -- grade 5 (excellent)

80 < score ≤ 90 -- grade 4 (very good)

70 < score ≤ 80 -- grade 3 (good)

60 < score ≤ 70 -- grade 2 (satisfactory)

50 < score ≤ 60 -- grade 1 (pass)

score < 50 -- grade 0 (failed)

Business continuity

Normal management	Crisis management
Strategically-driven	Driven by current situation
Long analyzed and planned activities	Fast and tactical decisions
Company manager	Crisis manager
Organization structure	Crisis teams
Main location and ordinary solutions	Spare parts and office solutions
Fomal communication	Crisis communication

Business continuity

Business Continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

/ISO 22301:2012/

Disaster recovery

Disaster Recovery (DR) is the ability of an organization to provide critical Information Technology (IT) and telecommunications capabilities and services, after it is disrupted by an incident, emergency or disaster.
/BCM Institute/

Key elements

Resilience: critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions, for example through the use of redundancy and spare capacity;

Recovery: arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.

Contingency: the organization establishes a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen.

BC terms

Maximum Acceptable Outage (MAO)

The duration after which an organization’s viability will be threatened if an IT system or service cannot be resumed.

Recovery Time Objective (RTO)

The target time for resuming the delivery of a product or service to an acceptable level following its disruption.

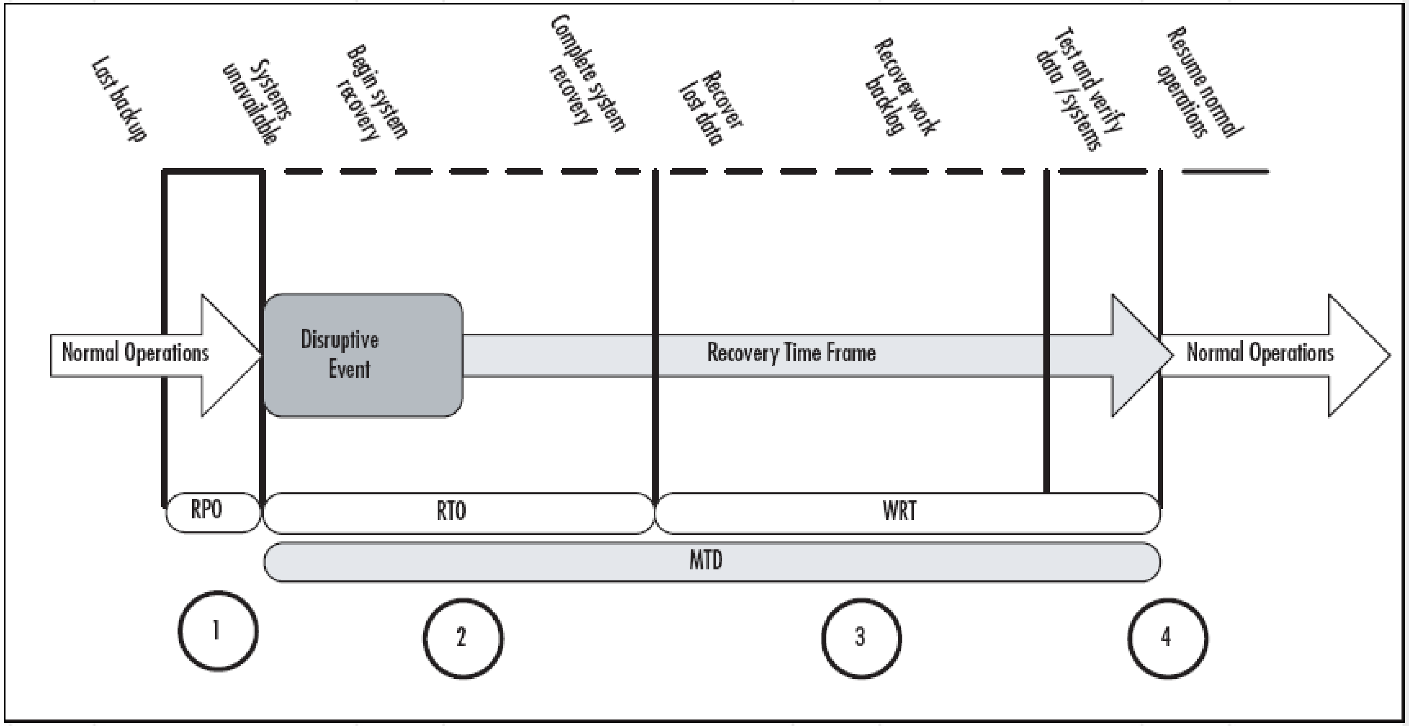
BC terms

Recovery Point Objective (RPO)

The target set for the status and availability of data (electronic and paper) at the start of a recovery process.

It is a point in time at which data or capacity of a process is in a known, valid state and can safely be restored from.

BC terms


Last backup
Systems unavailable
Begin system recovery
Complete system recovery
Recover lost data
Recover work backlog
Test and verify data /systems
Resume normal operations
Normal Operations
Disruptive Event
Recovery Time Frame
Normal Operations
RPO
RTO
WRT
MTD
1
2
3
4

Standards

ISO 22301:2012

Societal security -- Business continuity management systems --- Requirements

ISO/IEC 27031:2011

Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity

ISO/IEC 24762:2008

Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

BCP (DRII)

Preplanning

1. Program Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis

Planning

4. Developing Business Continuity Strategies
5. Emergency Preparedness and Response
6. Developing and Implementing Business Continuity Plans

Postplanning

7. Awareness and Training Programs
8. Business Continuity Plan Exercise, Audit, and Maintenance
9. Crisis Communications
10. Coordination with External Agencies

Practice 1

Program Initiation and Management: Summary

Establish the need for a Business Continuity Management (BCM) Program including resilience strategies, recovery objectives, business continuity, operational risk management considerations and crisis management plans. The prerequisites within this effort include obtaining management support and organizing and managing the formulation of the functions or processes required to construct the BCM framework.

Process

Link

Practice 2

Risk Evaluation and Control

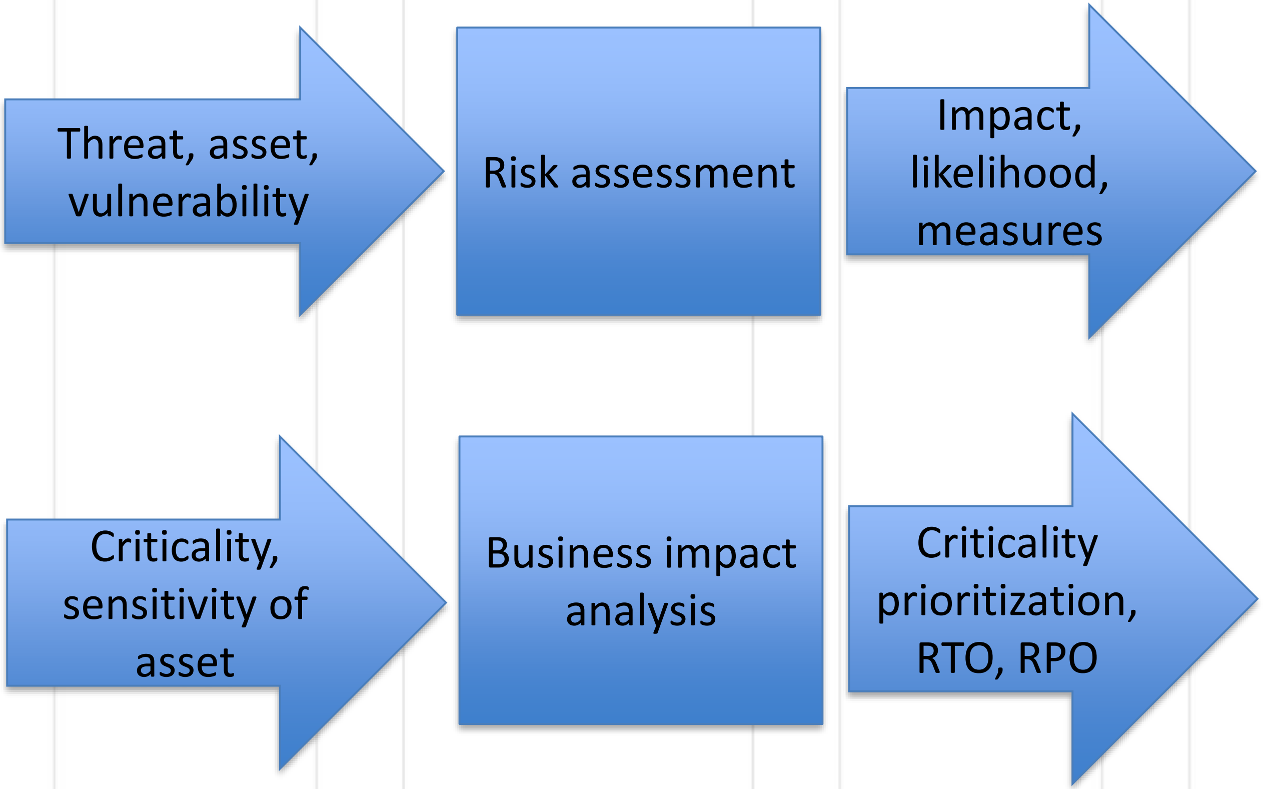
Determine the risks (events or surroundings) that can adversely affect the organization and its resources (people, facilities, technologies) due to business interruption. Determine the potential loss the risks can cause and the controls needed to avoid or mitigate the effects of those risks. Complete a cost benefit analysis to justify the investment in the controls necessary to mitigate the effect of the risks.

Practice 3

Business Impact Analysis

Identify the impacts resulting from business interruptions that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and interdependencies so that recovery time objectives can be established and approved.

BIA



Threat, asset, vulnerability

Risk assessment

Impact, likelihood, measures

Criticality, sensitivity of asset

Business impact analysis

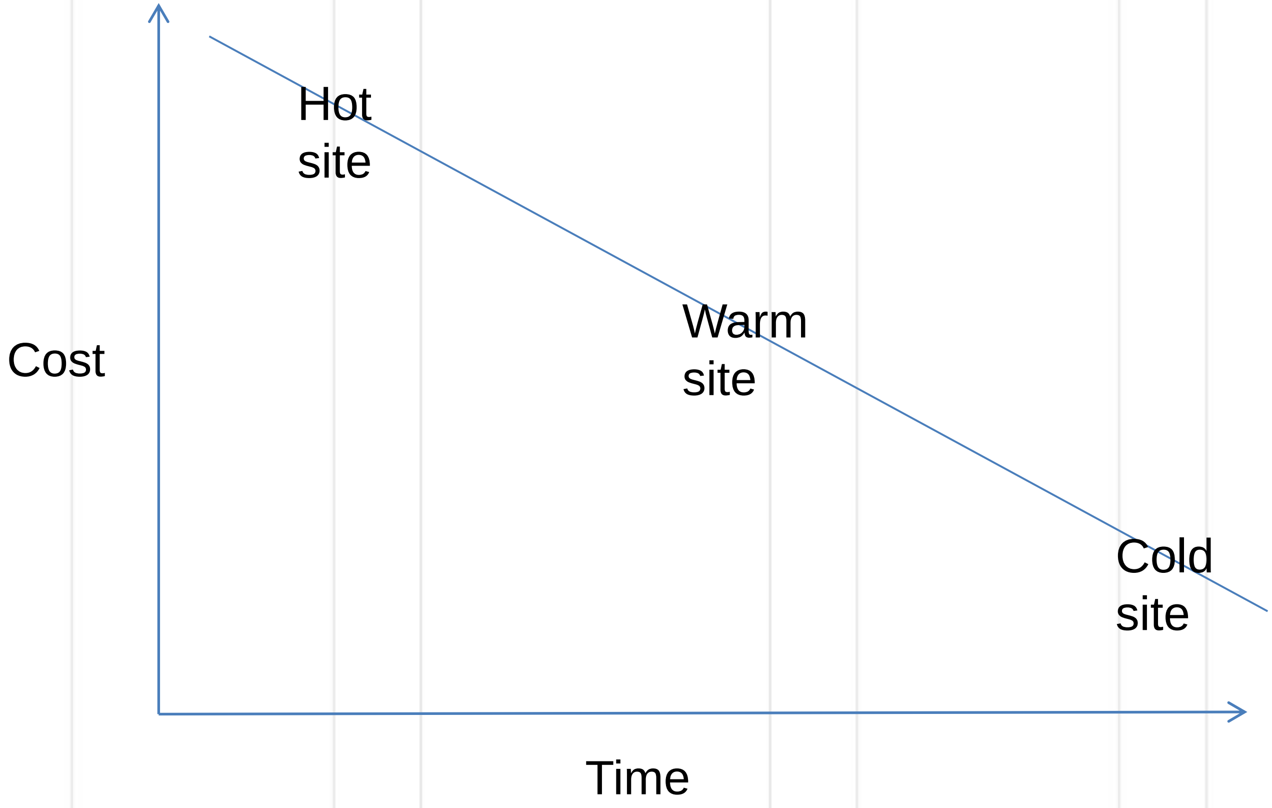
Criticality prioritization, RTO, RPO

Practice 4

Business Recovery Strategies

Leverage the outcome of the BIA and Risk Evaluation to develop and recommend effective business continuity strategies. The basis for these strategies includes the consideration of both the recovery time objectives and the recovery point objectives. This will assist you in assessing and planning for the support of the organization’s critical functions.

Strategy



Hot site

Warm site

Cold site

Cost

Time

Practice 5

Emergency Preparedness and Response

Identify the organization’s readiness to respond to an emergency in a coordinated, timely and effective manner. Develop and implement the procedures for the initial response and stabilization of a situation until the arrival of the authorities which have jurisdiction (if/when).

Practice 6

Developing and Implementing Business Continuity Plans

Design, develop, and implement Business Continuity Plans that will provide continuity and/or recovery as identified by the organization’s requirements.

Documentation

Determining the context of the organization

List of legal, regulatory and other requirements

...

Scope of the BCMS (Business Continuity Management System)

Business continuity policy

Business continuity objectives

Competences of personnel

Communication with interested parties

...

Business continuity procedures

Incident response procedures

Procedures for restoring and returning business from temporary measures

...

Results of internal audit

Practice 7

Awareness and Training Programs

Prepare a program to establish and maintain corporate awareness that Business Continuity Management (BCM) is a part of normal business management, and to develop and enhance the skills required to create and implement Business Continuity Management.

Practice 8

Business Continuity Plan Exercise, Audit, and Maintenance

Establish an exercise/testing program which documents plan exercise requirements including the planning, scheduling, facilitation, communications, auditing and post review documentation. Establish a maintenance program to keep the plans current and relevant. Establish an audit process which will validate compliance with standards, review solutions, verify appropriate levels of maintenance and exercise activities, and validate the plans are correct, accurate and complete.

Testing

Test types

- Checklist Test
- Paper Test
- Tabletop Test
- Partial Walkthrough Test
- Walkthrough Test

Practice 9

Crisis Communication

Establish applicable procedures and policies for coordinating the continuity and restoration activities with external agencies (local, regional, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes and regulations.

Practice 10

Coordination with External Agencies

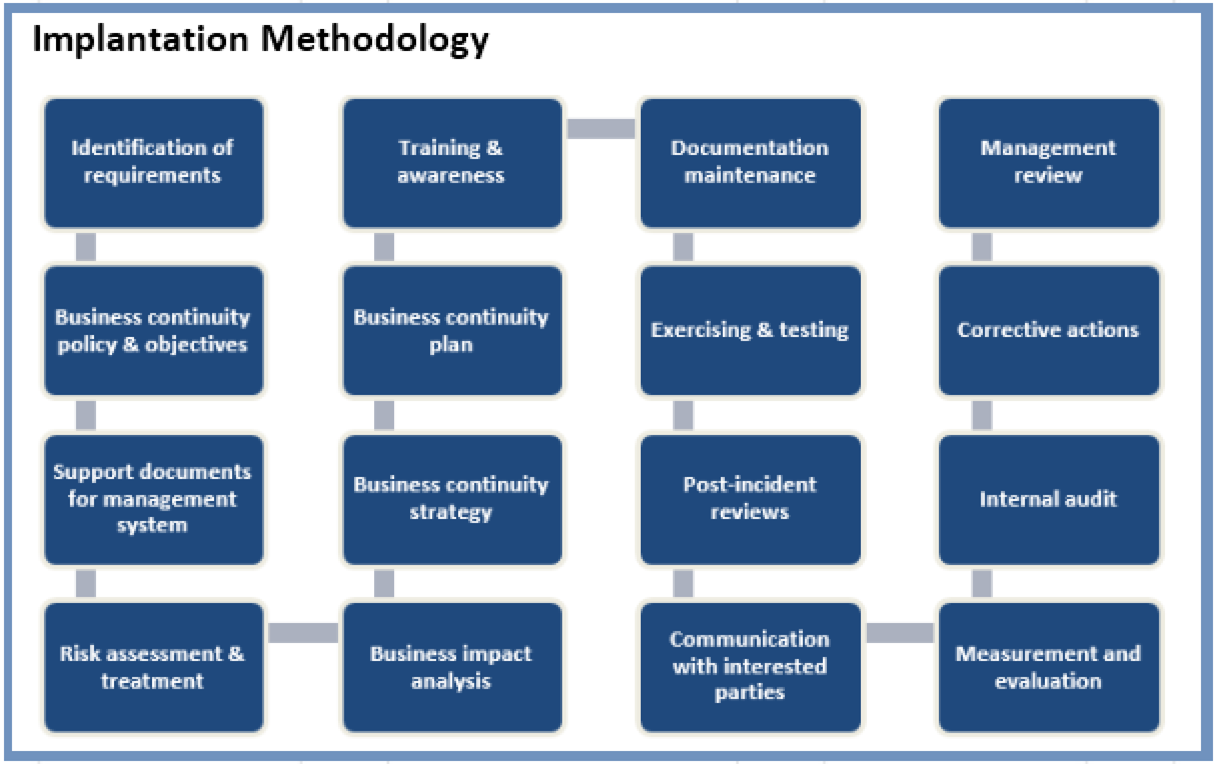
Establish applicable procedures and policies for coordinating the continuity and restoration activities with external agencies (local, regional, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes and regulations.

ISO 22301

ISO 22301

"Societal security – Business continuity management systems – Requirements", specifies a management system to manage an organization's business continuity arrangements. It is formal in style in order to facilitate compliance auditing and certification.

ISO 22301



Implantation Methodology

Identification of requirements

Business continuity policy & objectives

Support documents for management system

Risk assessment & treatment

Business impact analysis

Business continuity strategy

Business continuity plan

Training & awareness

Documentation maintenance

Exercising & testing

Post-incident reviews

Communication with interested parties

Measurement and evaluation

Internal audit

Corrective actions

Management review

Practice

Exercise

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