TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

IX

Lectures

- 05.09.2017 at 12.00-15.15 ICT 312 (introduction)
- 12.09.2017 at 12.00-15.15 self study (roles)
- 19.09.2017 at 12.00-15.15 ICT 312 (business processes)
- 26.09.2017 at 12.00-15.15 ICT 312 (asset list, valuation)
- 03.10.2017 at 12.00-15.15 self study (OCTAVE)
- 10.10.2017 at 12.00-15.15 ICT 312 (risk assessment)
- 17.10.2017 at 12.00-15.15 ICT 312 (risk+control, bow tie)
- 24.10.2017 at 12.00-15.15 ICT 312 (infosecurity controls)
- 31.10.2017 at 12.00-15.15 self study (security metrics)
- 07.11.2017 at 12.00-15.15 ICT 312 (cybersecurity controls)
- 14.11.2017 at 12.00-15.15 self study (COBIT)
- 21.11.2017 at 12.00-15.15 ICT 312 (audit)
- 28.11.2017 at 12.00-15.15 ICT 312 (continuity)
- 05.12.2017 at 12.00-15.15 seminar
- 12.12.2017 at 12.00-15.15 seminar
- 19.12.2017 at 12.00-15.15 seminar
- 26.12.2017 at 12.00-15.15 seminar?

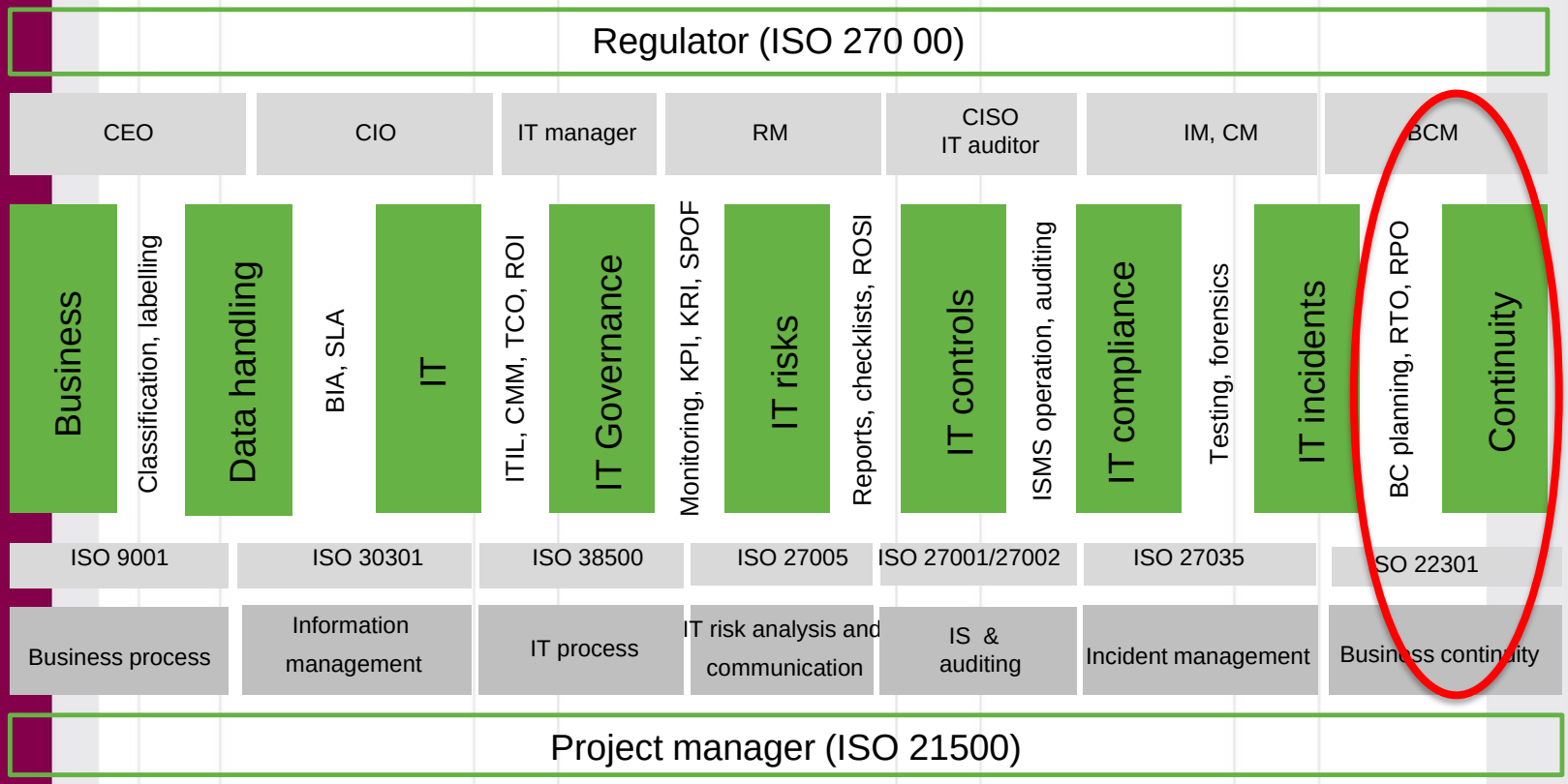
Practical info

Updates in course page

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

IT risk and control concept

Legal obligations for IT security, data protection, business continuity, and internal goals



IT, risk, information security and business continuity management actions

Business continuity

Normal management

- Strategically-driven
- Long analyzed and planned activities
- Company manager
- Organization structure
- Main location and ordinary solutions
- Fomal communication

Crisis management

- Driven by current situation
- Fast and tactical decisions
- Crisis manager
- Crisis teams
- Spare parts and office solutions
- 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/

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.

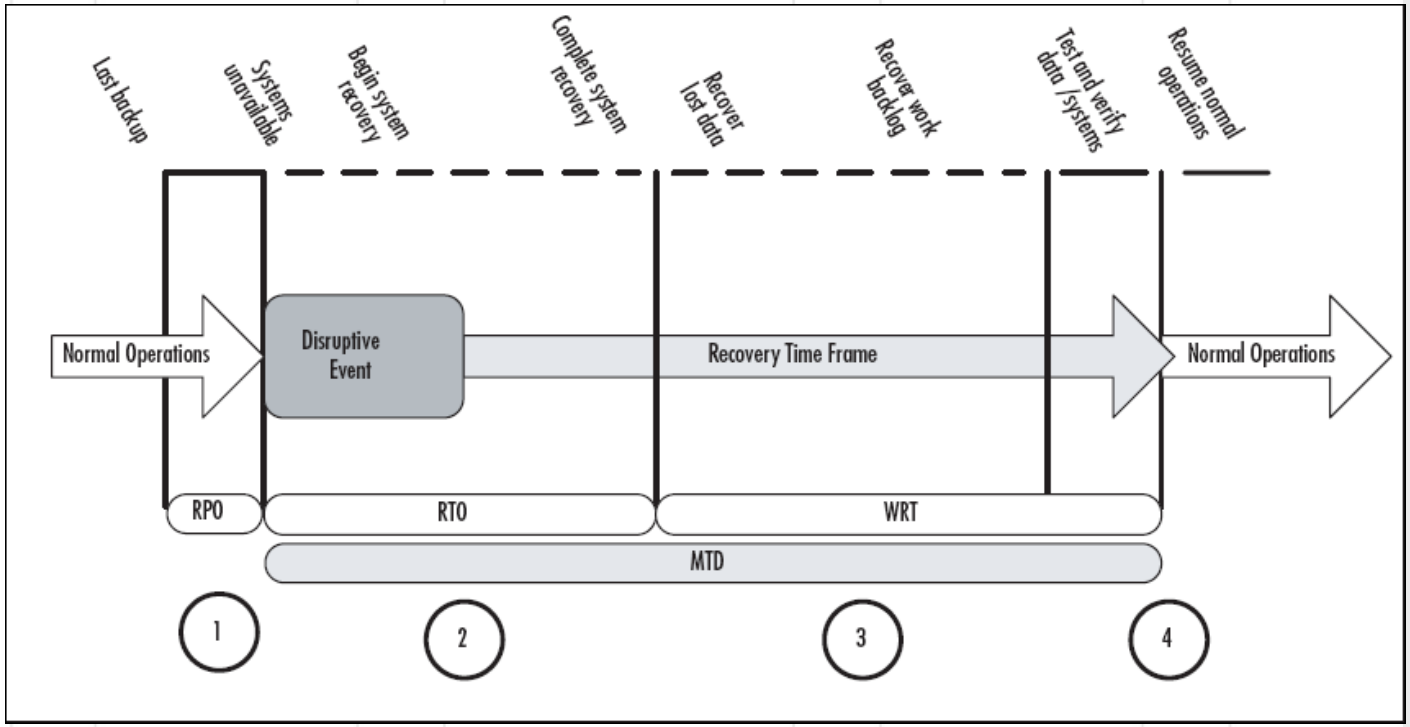
BC terms

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

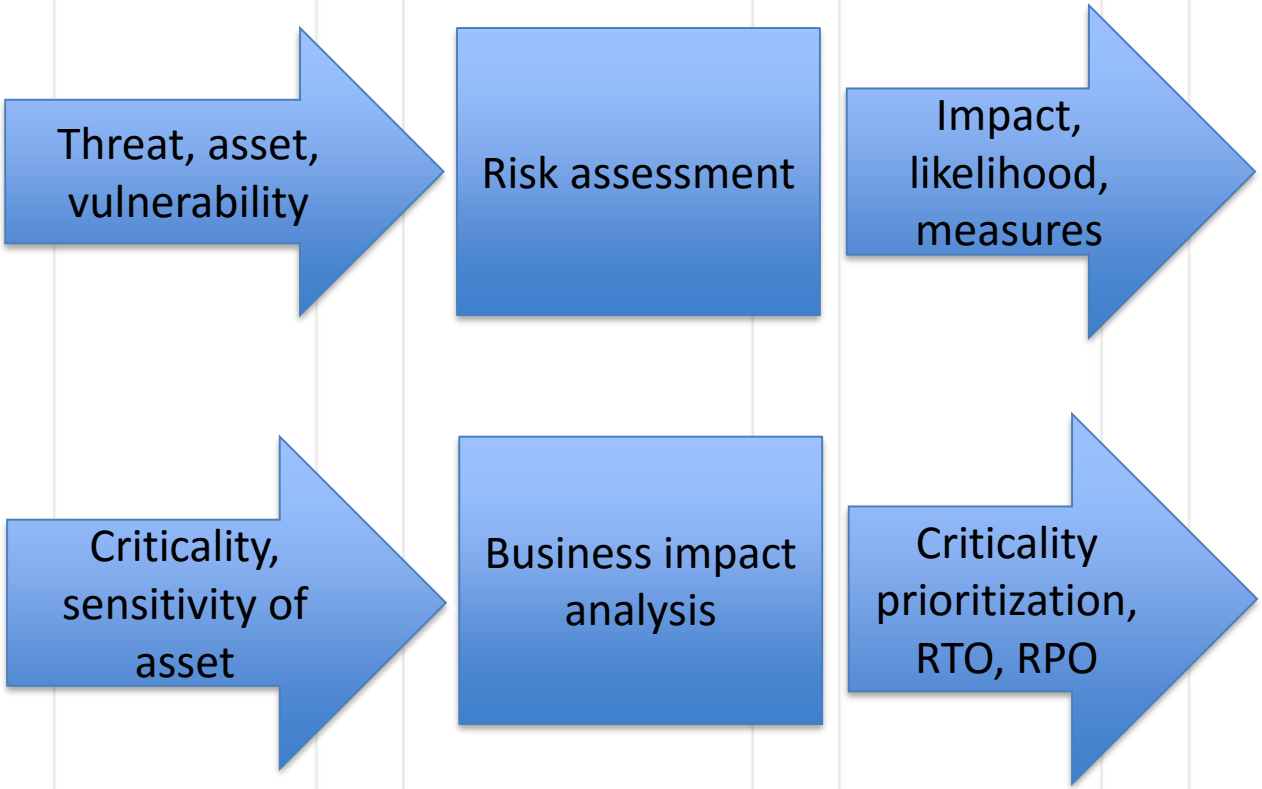
Determine the risks (events or surroundings) that can adversely affect the organization and its resources (people, facilities, technologies) due to business interruption. Determine the potential loss the risks can cause and the controls needed to avoid or mitigate the effects of those risks. Complete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

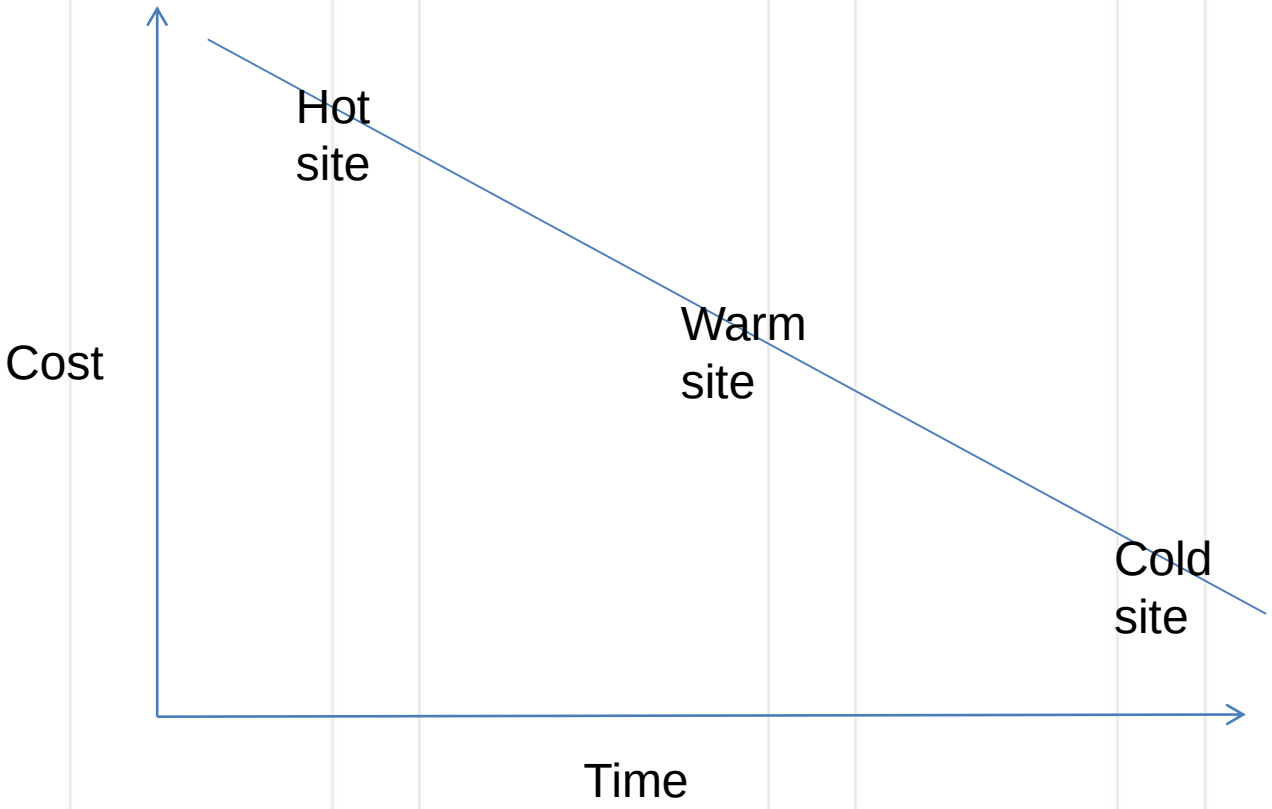

Threat, asset, vulnerability
Risk assessment
Impact, likelihood, measures
Criticality, sensitivity of asset
Business impact analysis
Criticality prioritization, RTO, RPO

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



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

Link

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.

Practice

Exercise XI

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