TALLINN UNIVERSITY OF TECHNOLOGY

Information and Cyber Security Assurance in Organisations

ITX8090

IV

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 (IS management metrics, IS economics)
~~22.11.2016 – Lecture 12 (self reading - IT auditing (ISACA))~~
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

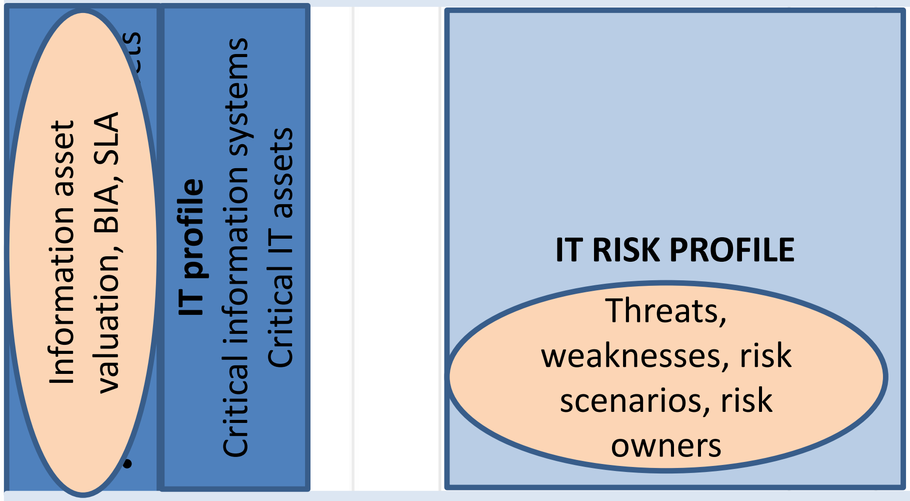
https://courses.cs.ttu.ee/pages/ITX8090

Practical info

HW example

Concept progress

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



ets

Information asset valuation, BIA, SLA

IT profile

Critical information systems

Critical IT assets

IT RISK PROFILE

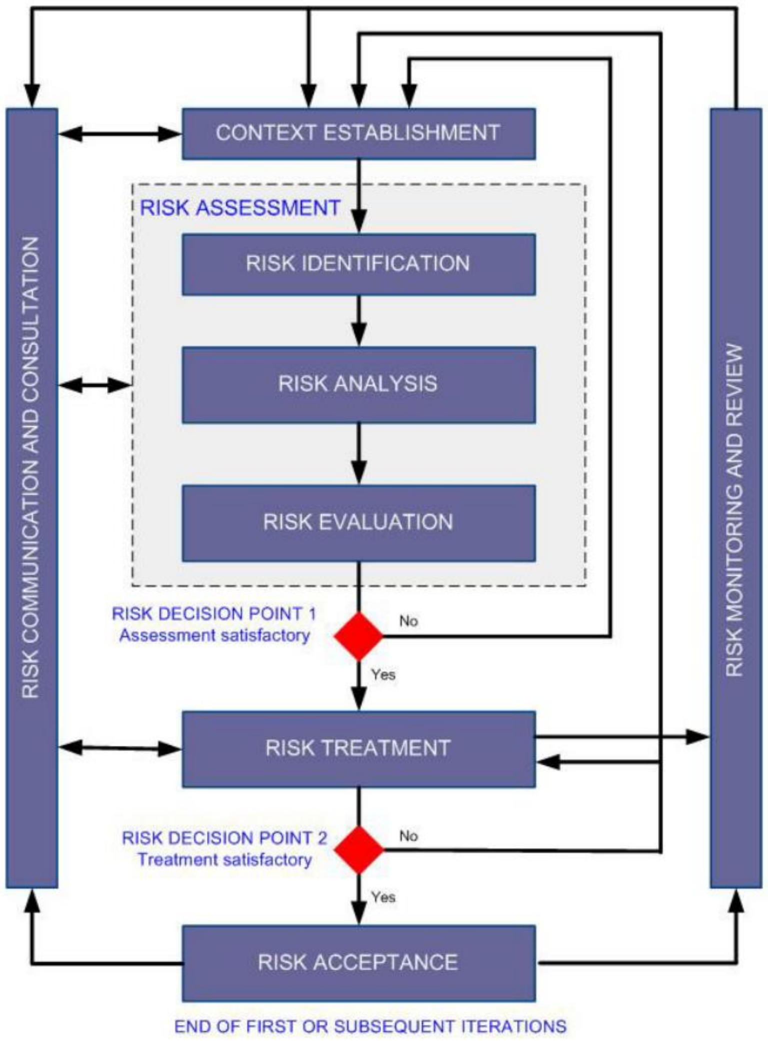
Threats, weaknesses, risk scenarios, risk owners

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 …)

Standard 27005

- ISO/IEC 27005:2011 is applicable to all types of organizations which intend to manage risks that could compromise the organization's information security.
- ISO/IEC 27005:2011 provides guidelines for information security risk management.

Process 27005



Context establishment

Criteria include the risk evaluation, risk acceptance and impact evaluation criteria:

- legal and regulatory requirements
- the strategic value for the business of information processes
- stakeholder expectations
- negative consequences for the reputation of the organization

Risk identification

Risk identification states what could cause a potential loss; the following are to be identified:

- assets, primary (i.e. Business processes and related information) and supporting (i.e. hardware, software, personnel, site, organization structure)
- threats
- existing and planned security measures
- vulnerabilities
- consequences
- related business processes

Risk analysis

Risk analysis (estimation) has as input the output of risk analysis and can be split in the following steps:

- assessment of the consequences through the valuation of assets
- assessment of the likelihood of the incident (through threat and vulnerability valuation)
- assign values to the likelihood and consequence of the risks

Risk evaluation

The risk evaluation process receives as input the output of risk analysis process. It compares each risk level against the risk acceptance criteria and prioritize the risk list with risk treatment indications.

Risk treatment and acceptance

The risk treatment process aim at selecting security measures to:

- reduce
- retain
- avoid
- transfer

risk and produce a risk treatment plan, that is the output of the process with the residual risks subject to the acceptance of management.

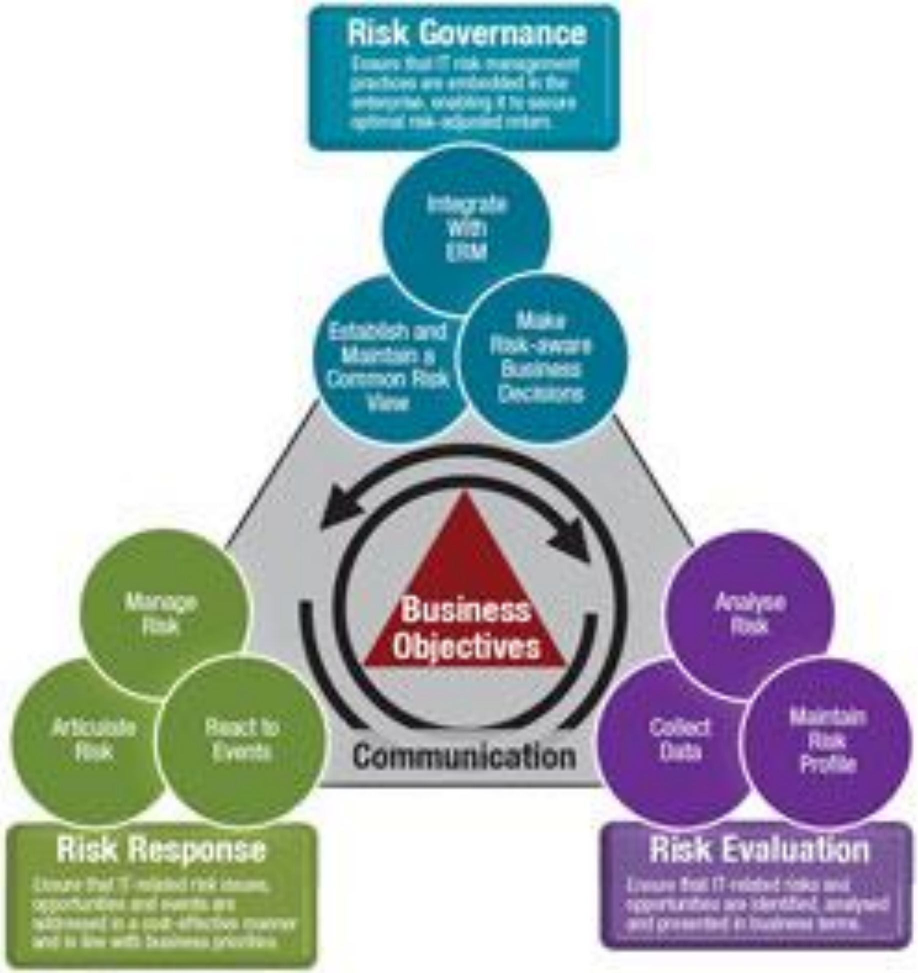
Risk communication

Risk communication is a horizontal process that interacts bidirectionally with all other processes of risk management. Its purpose is to establish a common understanding of all aspect of risk among all the organization's stakeholder.

Risk monitoring and review

Risk management is an ongoing, never ending process. Within this process implemented security measures are regularly monitored and reviewed to ensure that they work as planned and that changes in the environment rendered them ineffective. Business requirements, vulnerabilities and threats can change over the time.

Best practice (RiskIT)


Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

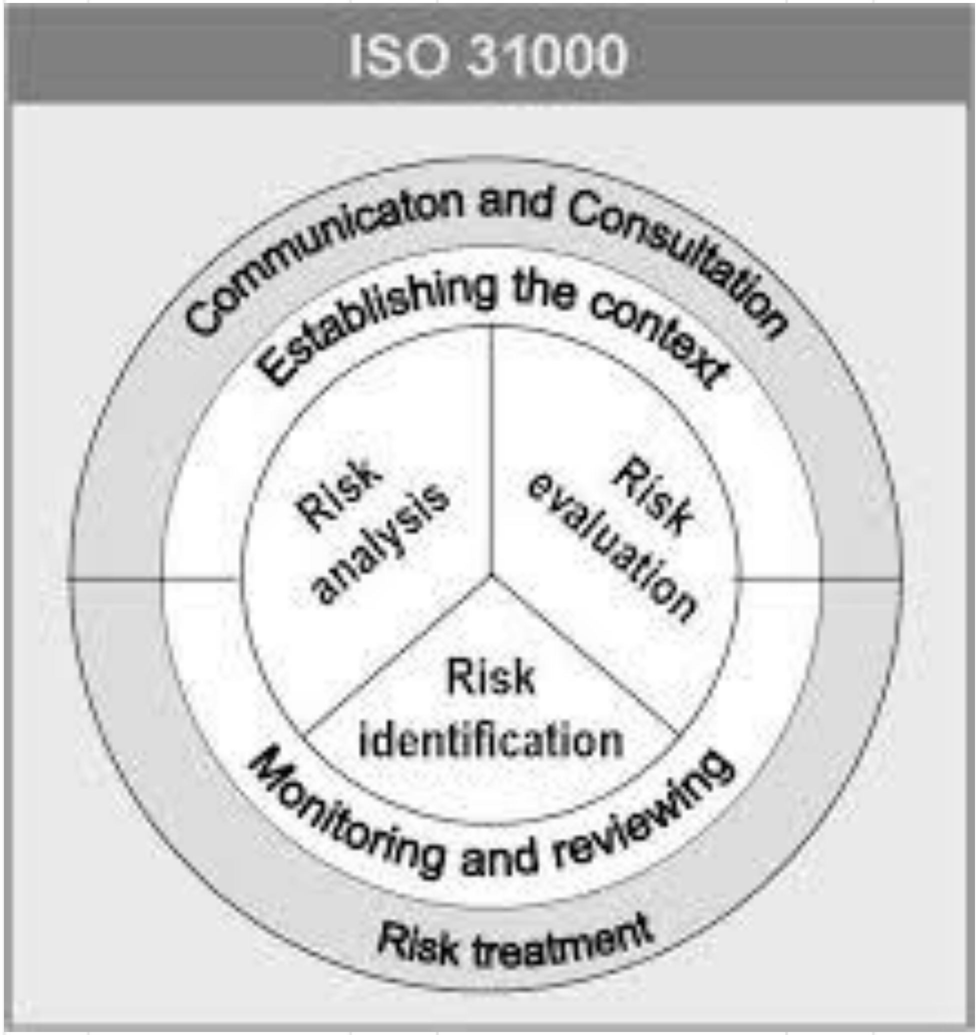
Best practice (RiskIT)

Risk IT provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues.

Best practice (RiskIT)

Risk IT was published in 2009 by ISACA. It is the result of a work group composed by industry experts and some academics of different nations, coming from organizations such as IBM, PricewaterhouseCoopers, Risk Management Insight, Swiss Life, and KPMG.

Standard (ISO 31000)



Standard (ISO 31000)

ISO 31000 is intended to be a family of standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000:2009 is to provide principles and generic guidelines on risk management.

Standard (ISO 31000)

ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

Definitions (threat)

ISO 27005

A potential cause of an incident, that may result in harm of systems and organization

NIST

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Definitions (threat)

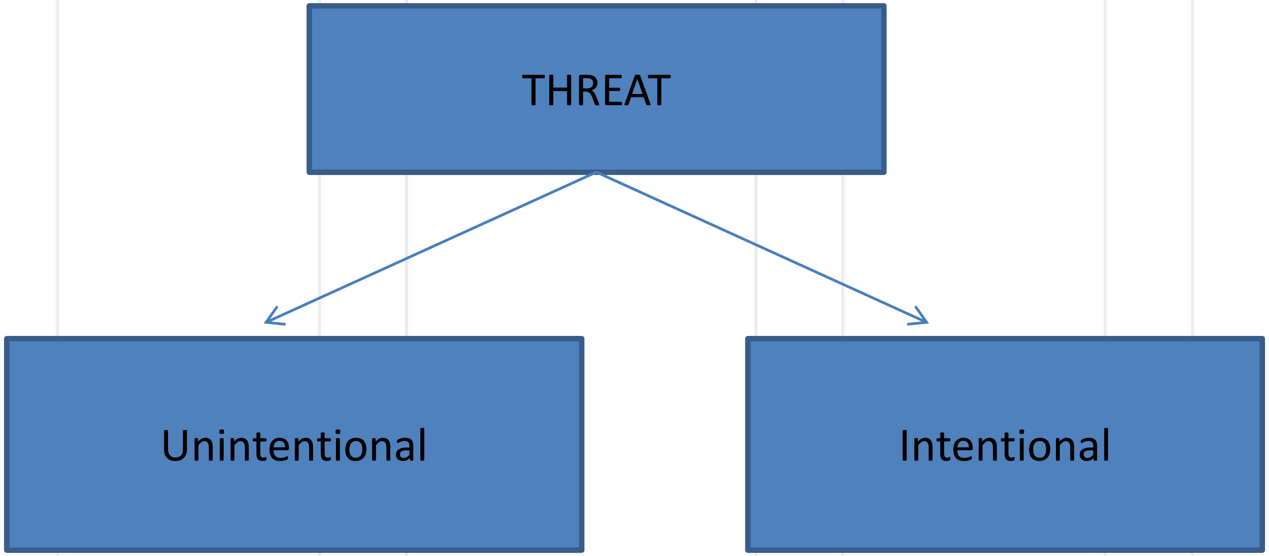
National Information Assurance Glossary

Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

ENISA gives a similar definition

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threats



Threats

Unintentional (elemental)

- Environmental - lightning, flood, too low or high temperatures, fire and the like;
- Technical faults - a power failure, computer failure and the like;
- Human threats - errors, mistakes, illness, exits and the like;

One threat can lead to another, such as lightning - > computer failure, flood - > power failure.

Threats

Intentional (attacks)

- Physical attacks;
- Misuse of resources;
- Resource blocking;
- Information fishing;
- Data forgery;
- Manipulation with systems;
- …

Definitions (vulnerability)

ISO 27005

A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission

National Information Assurance Glossary

Vulnerability — Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited

Definitions (vulnerability)

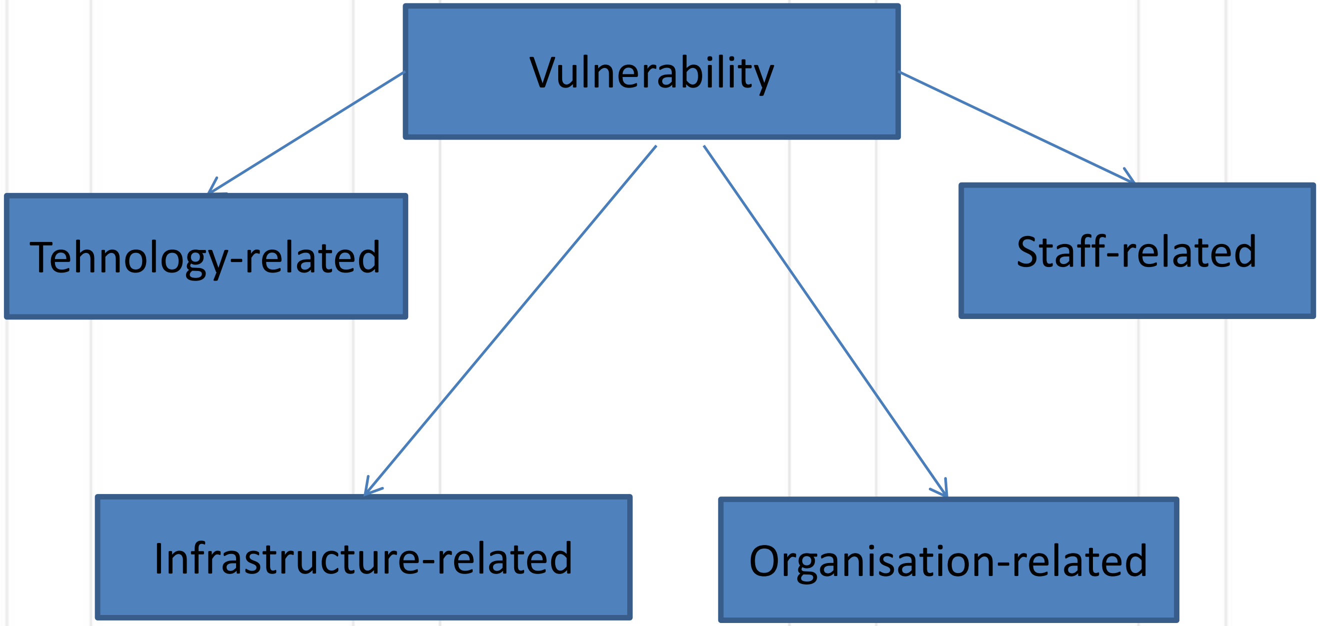
NIST

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

ENISA

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Vulnerability



Vulnerability

Tehnology-related

Staff-related

Infrastructure-related

Organisation-related

Vulnerability

Technology-related

- Obsolete technology, „legacy“;
- Improper placement;
- Errors in programs, operating systems;
- Weaknesses in technology management;
- …

Vulnerability

Infrastructure-related

- Unfavorable location;
- Natural conditions;
- Decaying infrastructure;
- Communication system installation deficiencies;
- Malicious neighbor;
- …

Vulnerability

Staff-related

Lack of experience;

Excessive trust;

Incorrect procedures;

Ignorance and low motivation level;

Failure to comply with security requirements;

Self-interest;

…

Vulnerability

Organisation-related

- Lack of security organisation;
- Shortcomings in the organisation of work;
- Resource management deficiencies;
- Documenting drawbacks;
- Deficiencies in selection of security measures;
- Deficiencies in control of security measures;
- …

Listing sources

Internal possibilities

- Predefined forms;
- Interviews;
- Questionnaires;
- Debates;
- Analysis of the documents;
- Observations;
- Incidents occurred;
- Audit reports.

External possibilities

- Standards;
- Statistics;
- How is the in other similar businesses?
- How is the country as a whole?
- How is Europe?
- What are the trends in the world?
- Agencies.

Pairing (NIST)

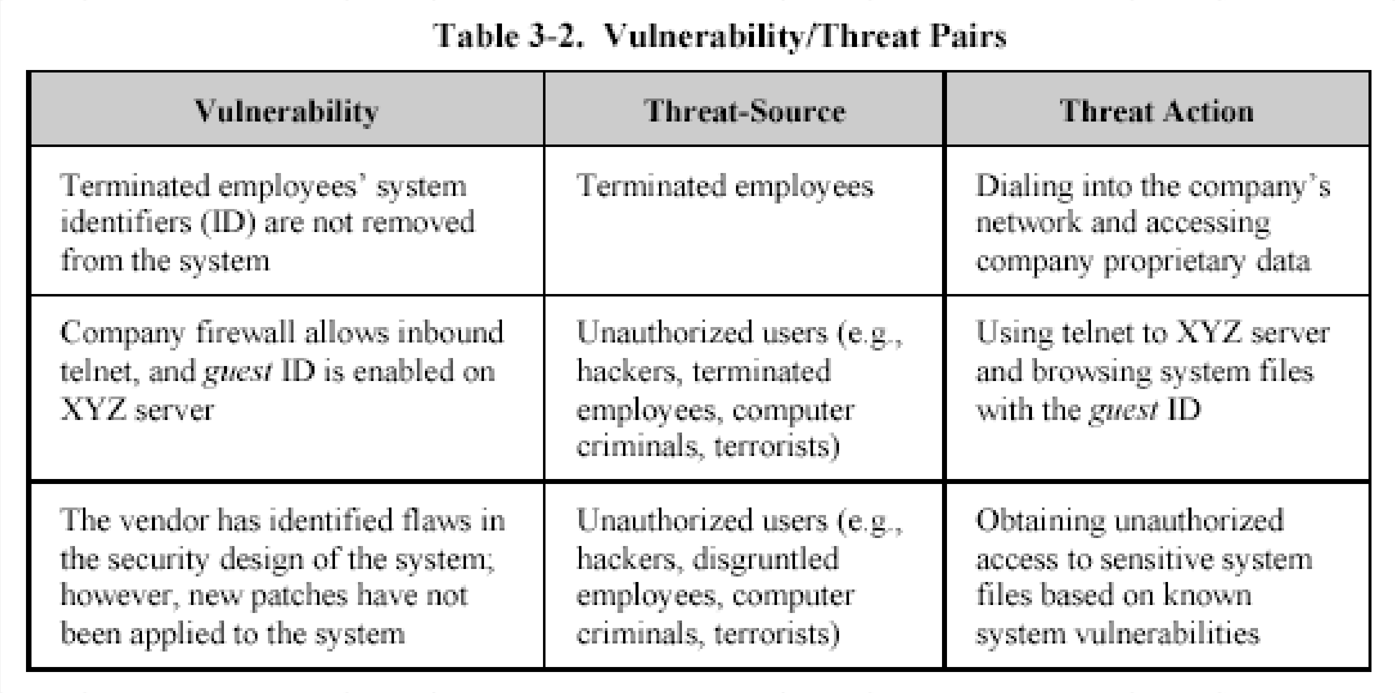


Table 3-2. Vulnerability/Threat Pairs

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Risk scenario

Component	Description
Participant	Internal (employee, temporary employee) External (competitor, external business partner, regulator, market operator)
Threat	Malicious Accidental Malfunction Natural error External requirement
Event	Disclosure Disruption Modification Theft

Risk scenario

Component	Description
Event	Destruction Structure change Ineffective Use Regulations violation Misuse
Information asset/IT asset	Organisation Processes Infrastructure IT infrastructure Information Applications
Time	Time period The critical/non- critical time Detection speed

Advising questions

1. Asset - **what** should be protected?
2. Threat - **who** or **what** uses the advantage of the weakness?
3. Weakness - **why** is asset vulnerable?
4. Risk - **what** may happen if weakness exploited and **how** likely is it?

Practice

Creating risk scenarios (based on standardized list of threats)

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