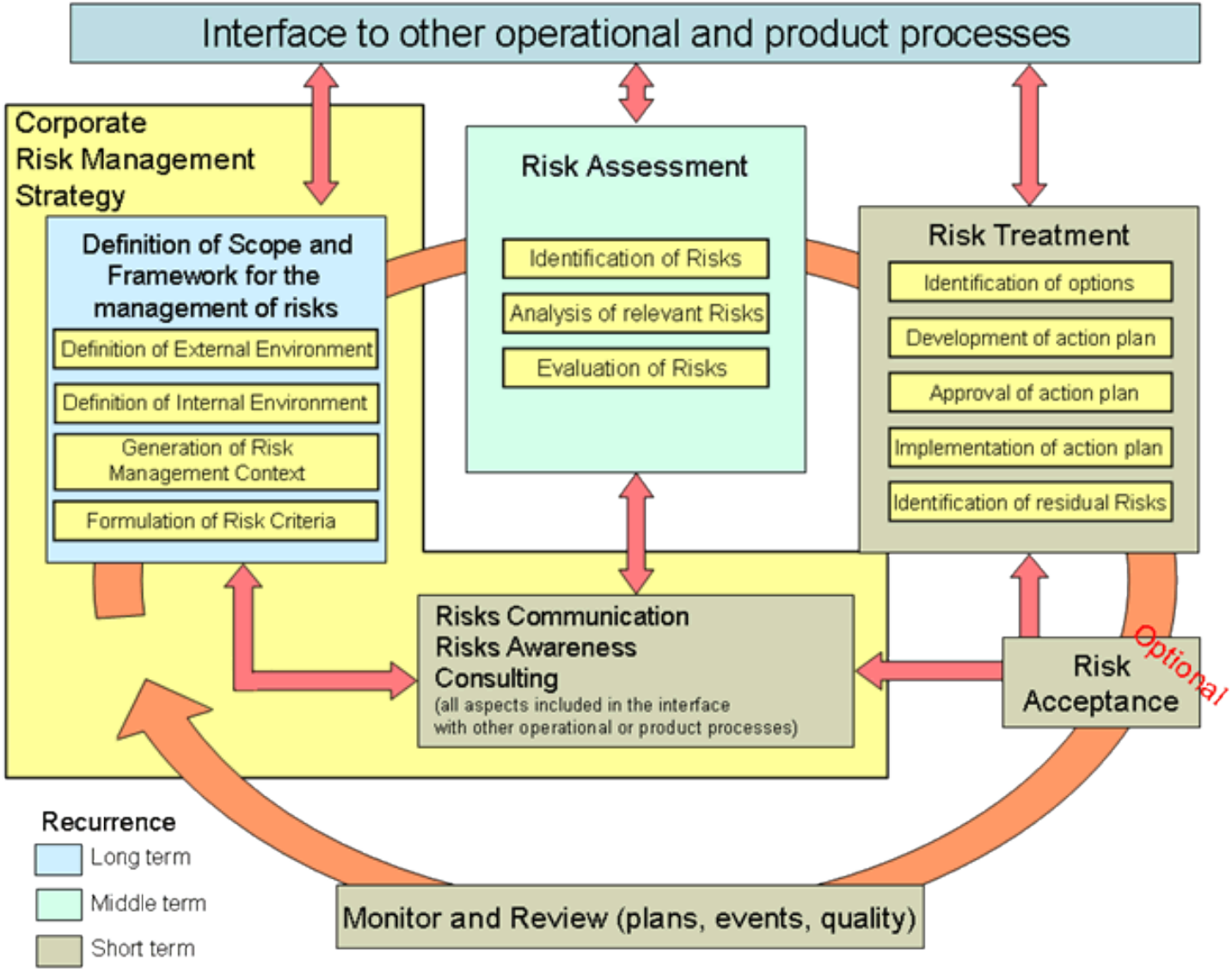
ITI8610 Software Assurance

Risk Management Basics

Aleksandr Lenin

Risk Management



Risk Management Standards

1. ISO Guide 73:2009 Risk management - Vocabulary
2. ISO/IEC 27002:2013 Code of Practice for Information Security Controls
3. ISO/IEC 27005:2011 Information Security Risk Management
4. ISO/IEC 31000:2009 Risk Management – Principles and Guides
5. ISO/IEC 31010:2009 Risk Management – Risk Assessment Techniques

Risk Treatment

Risk Management Activities

Risk Management is comprised of several activities:

- Risk assessment
  1. Risk identification
  2. Risk analysis (impact/likelihood estimation)
  3. Risk evaluation (prioritization, comparison with risk criteria – if risk is tolerable or not)
- Risk treatment
- Risk communication
- Monitoring and review
- Risk acceptance (optional)

Risk Assessment

Risk analysis has four main goals:

1. Identify assets and their values
2. Identify vulnerabilities and threats
3. Quantify the likelihood and business impact on threats
4. Provide a cost-benefit analysis, reach a meaningful trade–off between the impact of the threat and the costs of security controls

The results of risk analysis provide the higher-level management with sufficient details to decide:

- Which risks should be mitigated
- Which risks should be transferred
- Which risks should be accepted

Risk Communication

A process to exchange to share information about risk between the decision-maker and other stakeholders inside and outside an organization (e.g. departments and outsourcers).

An information can relate to the:

- existence
- nature
- form
- probability
- severity
- acceptability
- treatment
- ...(any other aspects of risk)

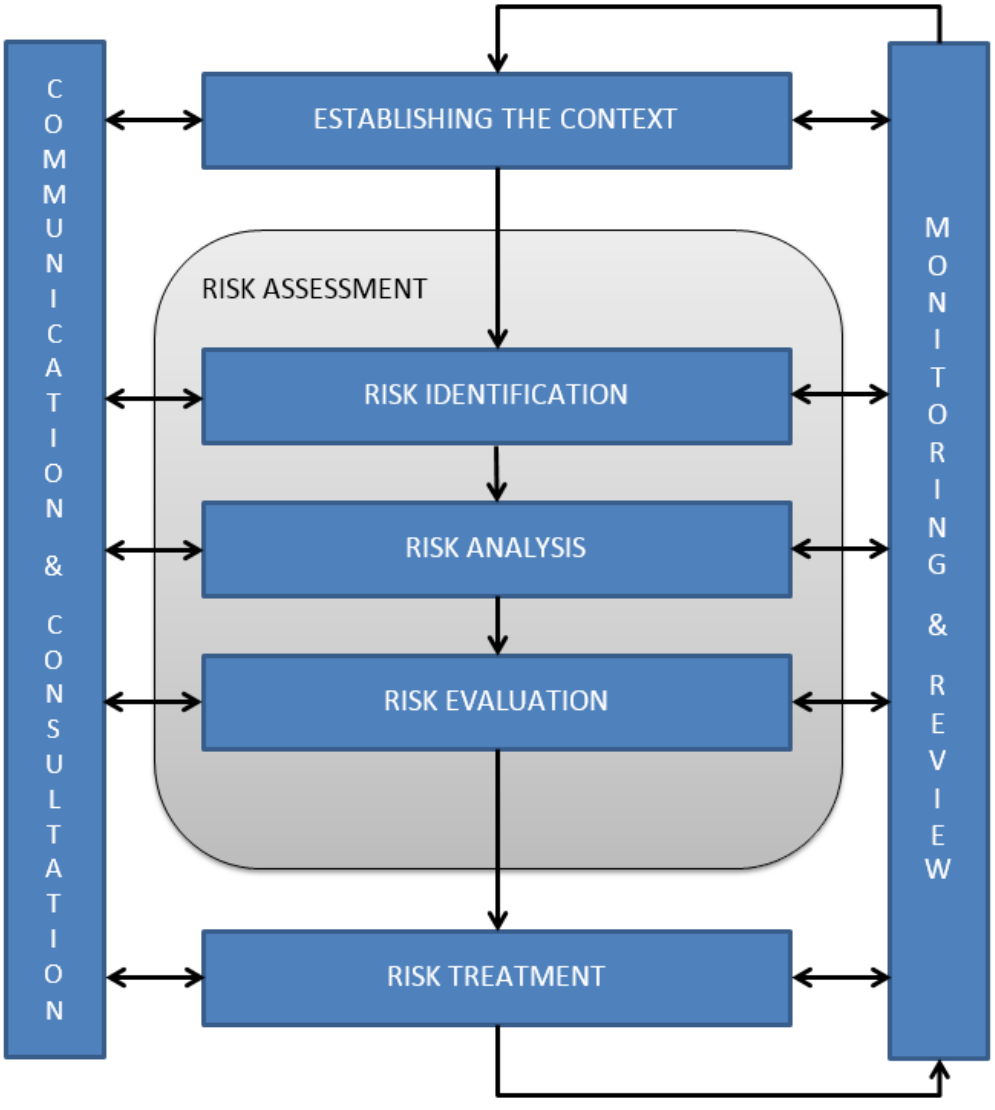
Monitoring and Review

- A process for measuring the efficiency of organization's risk management processes is the establishment of ongoing monitoring and review process
- This process makes sure that the specified management action plans remain relevant and updated
- This process also implements control activities including re-evaluation of the scope and compliance with decisions

Risk Acceptance (optional)

- A decision to accept the risk by the responsible management of the organization
- Risk acceptance depends on the defined risk criteria

Risk Management



Risk Levels

Strategic	high-level goals, aligned with and supporting the mission
Tactical	tactical goals, programs, projects, resources
Operational	effective and efficient use of resources
Reporting	reliability of reporting
Compliance	compliance with applicable laws and regulations

Risk Levels

Risk Management (in general):

- Looks at various possibilities of loss
- Determines what could cause greatest loss
- Applies controls appropriately

Risk Levels

Strategic Planning:

- Produces fundamental long-term security decisions and actions
- Shapes and guides what is needed and how it can be achieved
- Includes
  - broad scale information gathering
  - exploration of alternatives
  - puts an emphasis on future applications

Risk Levels

Tactical Security Management:

- Addresses daily operations that keep enterprise viable
- Managers set very general goals that require more than one year to achieve
- Tactical plans provide specifics for implementing the strategic plan

Risk Levels

Operational Security Management:

- Short-term plans concerning day-to-day work
- Aligned with long-term goals
- Supports tactical plans
- Examples:
  - Policies
  - Procedures
  - Methods
  - Rules
  - ...

Risk Assessment

- Qualitative Risk Assessment
- Quantitative Risk Assessment

thank you for your attention