

# SECURITY RISK MANAGEMENT PROCESS IN THE ORGANIZATION

**Prof. dr. Raimundas Kalesnykas**

*International expert for security risk management & security solutions  
Faculty of Law, Kazimieras Simonavicius University, Vilnius (Lithuania)*

## **NORDPLUS Higher Education Intensive Course**

**“Organization and Individual Security” (14.08.2017.-25.08.2017)**

*11:50 – 13:20, 21 August 2017, Turība University, Riga, Latvia*



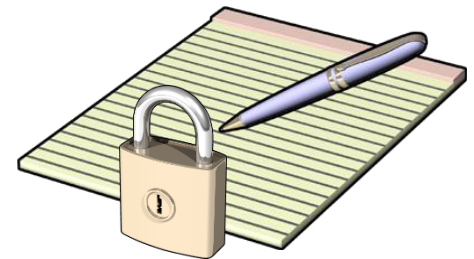
# Why Develop a Security Risk Management Process?

## ➤ **Security risk management**

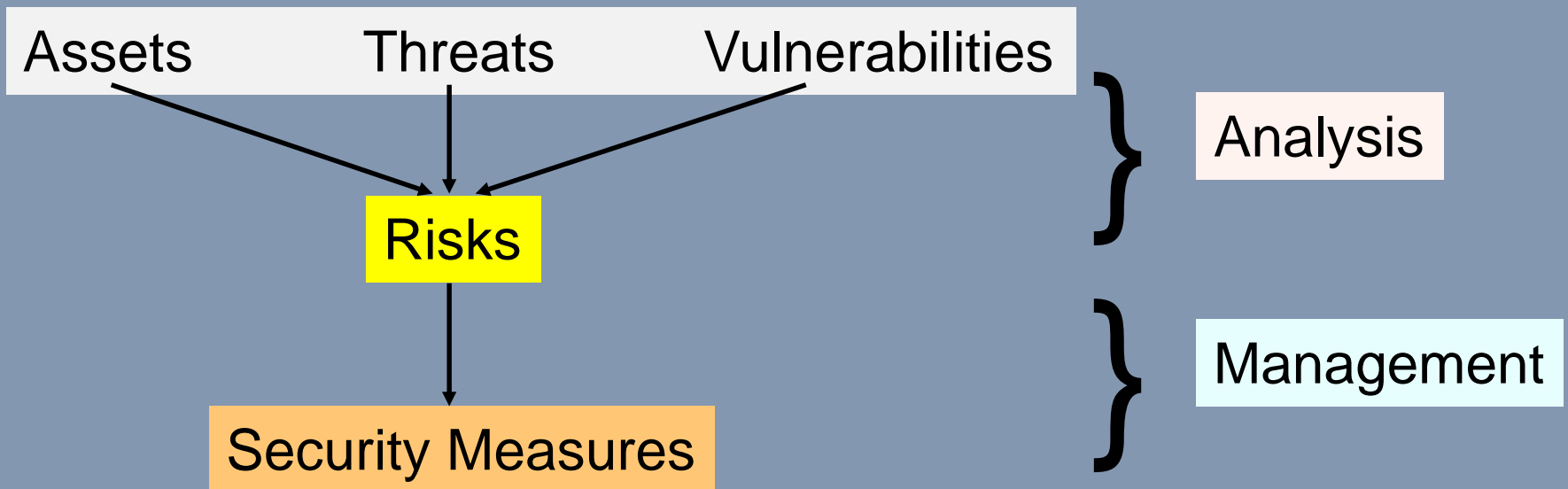
- A process for identifying, prioritizing and managing risk to an acceptable level within the organization

## ➤ **Formal security risk management process can address the following:**

- Threat response time
- Regulatory compliance
- Infrastructure management costs
- Risk prioritization and management



# Security Risk Analysis and Management Framework (1)



# Security Risk Analysis and Management Framework (2)

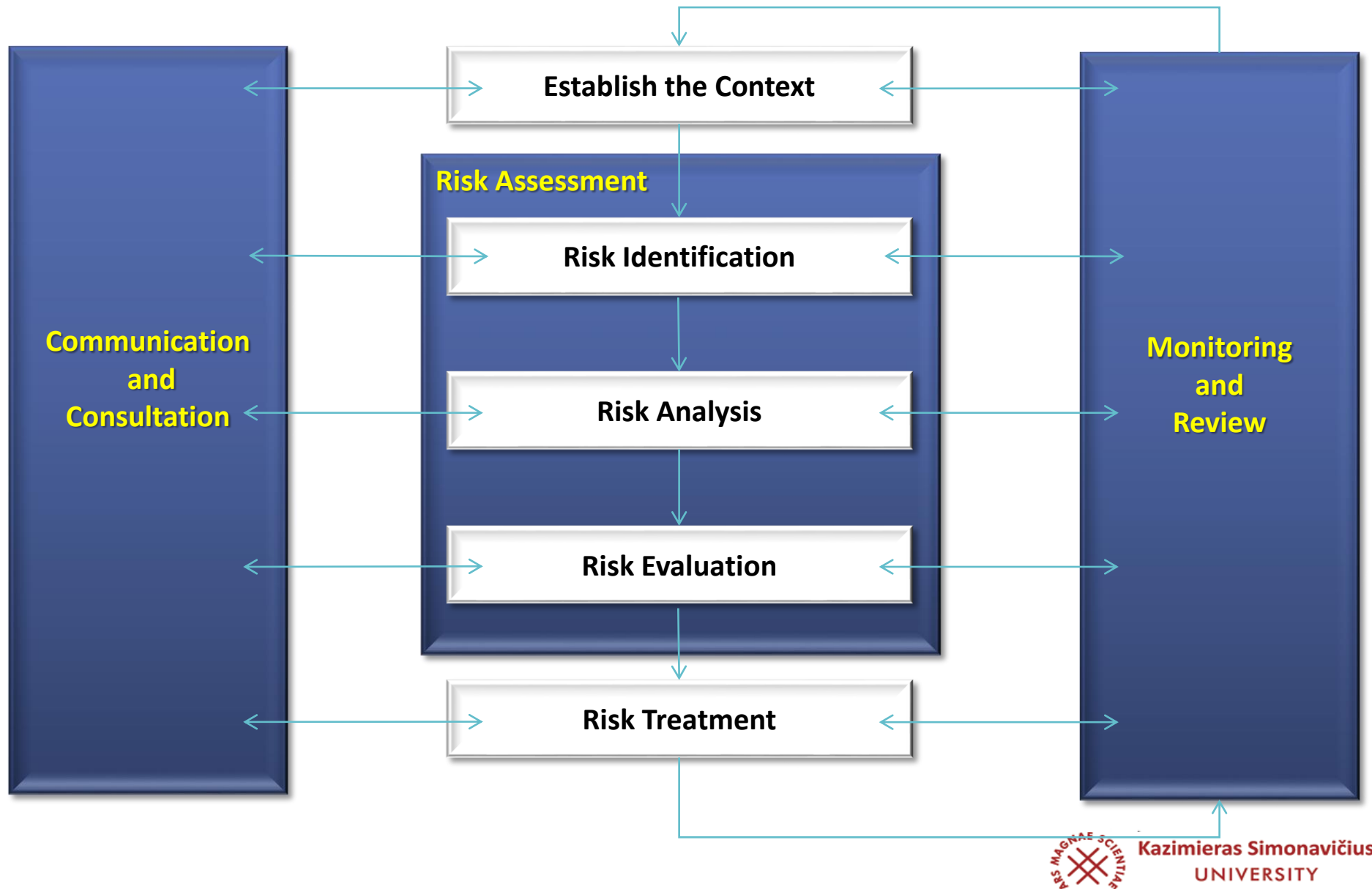
## DEFINITIONS

- **Threat:** Harm that can happen to an asset
- **Impact:** A measure of the seriousness of a threat
- **Attack:** A threatening event
- **Attacker:** The agent causing an attack (not necessarily human)
- **Vulnerability:** a weakness in the system that makes an attack more likely to succeed
- **Likelihood:** potential for an event to harm
- **Risk:** a quantified measure of the likelihood of a threat being realised
- **Prevention:** reduces likelihood
- **Mitigation:** Reduces impact

The meanings of terms in SRM area is not universally agreed!!!


# Organization's Security Risk Management

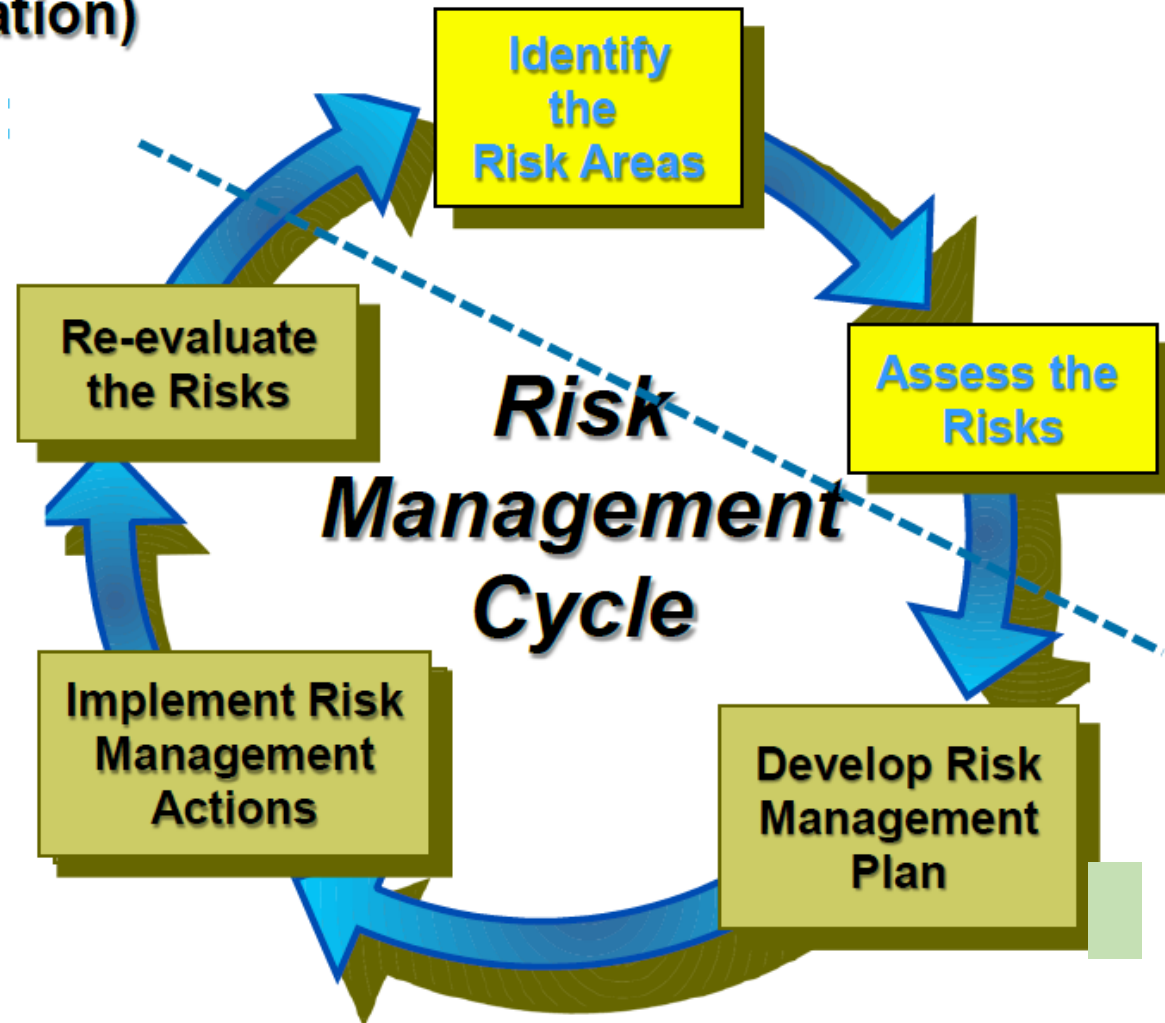
## *ISO 31000 Standard (2009)*



# SRM CYCLE: 2 MAJOR SUB-PROCESSES


 Risk Identification & Assessment

 Risk Control (Mitigation)



# SRM Process

## Risk Management



```
graph TD; RM[Risk Management] --> RI[Risk Identification]; RM --> RC[Risk Control]; RI --> IPA[Identify & Prioritize Assets]; IPA --> IPT[Identify & Prioritize Threats]; IPT --> IVA[Identify Vulnerabilities between Assets and Threats (Vulnerability Analysis)]; IVA --> RA[Risk Assessment]; RA --> CRA[Calculate Relative Risk of Each Vulnerability]; RC --> CBA[Cost-Benefit Analysis]; CBA -.-> A[Avoid]; CBA -.-> C[Control]; CBA -.-> T[Transfer]; CBA -.-> M[Mitigate]; CBA -.-> AC[Accept];
```

The diagram illustrates the SRM (Security Risk Management) process. It begins with a central 'Risk Management' box, which branches into two main paths: 'Risk Identification' and 'Risk Control'. The 'Risk Identification' path is highlighted in yellow and consists of five sequential steps: 'Identify & Prioritize Assets', 'Identify & Prioritize Threats', 'Identify Vulnerabilities between Assets and Threats (Vulnerability Analysis)', 'Risk Assessment', and 'Calculate Relative Risk of Each Vulnerability'. The 'Risk Control' path is highlighted in olive green and starts with 'Cost-Benefit Analysis', which then leads to five risk response options: 'Avoid', 'Control', 'Transfer', 'Mitigate', and 'Accept'. Dashed arrows indicate the flow from 'Cost-Benefit Analysis' to each of these options.

### Risk Identification

Identify & Prioritize Assets

Identify & Prioritize Threats

Identify Vulnerabilities  
between Assets and Threats  
(Vulnerability Analysis)

### Risk Assessment

Calculate Relative Risk  
of Each Vulnerability

### Risk Control

### Cost-Benefit Analysis

Avoid

Control

Transfer

Mitigate

Accept



# SECURITY RISK MANAGEMENT vs SECURITY RISK ASSESSMENT

	<b>Risk Management</b>	<b>Risk Assessment</b>
<b>Goal</b>	<ul style="list-style-type: none"><li>• Manage risks across business to acceptable level</li></ul>	<ul style="list-style-type: none"><li>• Identify and prioritize risks</li></ul>
<b>Cycle</b>	<ul style="list-style-type: none"><li>• Overall program across all four phases</li></ul>	<ul style="list-style-type: none"><li>• Single phase of risk management program</li></ul>
<b>Schedule</b>	<ul style="list-style-type: none"><li>• Scheduled activity</li></ul>	<ul style="list-style-type: none"><li>• Continuous activity</li></ul>
<b>Alignment</b>	<ul style="list-style-type: none"><li>• Aligned with budgeting cycles</li></ul>	<ul style="list-style-type: none"><li>• Not applicable</li></ul>

# SECURITY RISK ASSESSMENT: VULNERABILITIES

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

## **SECURITY RISK ASSESSMENT: CRITERIA**

- Strategic value of the assets
- Criticality of the assets
- Legal, contractual, and regulatory requirements
- Operational and business importance of confidentiality, integrity, and availability (CIA)
- Stakeholders expectations
- Damage to reputation

### **SECURITY RISK: ACCEPTANCE CRITERIA**

- Multiple thresholds and provisions for senior managers to accept risks
- Ratio of estimated benefit to the estimated risk
- Different acceptance criteria for different classes of risk
- May include requirements for future additional treatment

# SECURITY RISK ANALYSIS (SRA)

**SRA involves the identification and assessment of the levels of risk, calculated from the**

- Values of assets
- Threats to the assets
- Their vulnerabilities and likelihood of exploitation

## SECURITY RISK ANALYSIS (SRA): goals

- All assets have been identified
- All threats have been identified: *their impact on assets has been valued*
- All vulnerabilities have been identified and assessed

# SECURITY RISK ANALYSIS (SRA): levels

Better to use levels:

## 1. High, Medium, Low

- **High:** major impact on the organisation
- **Medium:** noticeable impact (“material” in auditing terms)
- **Low:** can be absorbed without difficulty

## 2. 1 - 10

Level	State
0	Non-existent
1	Ad hoc
2	Repeatable
3	Defined process
4	Managed
5	Optimized

## RESPONSES TO RISK

- **AVOID** it completely by withdrawing from an activity
- **ACCEPT** it and do nothing
- **REDUCE** it with security measures

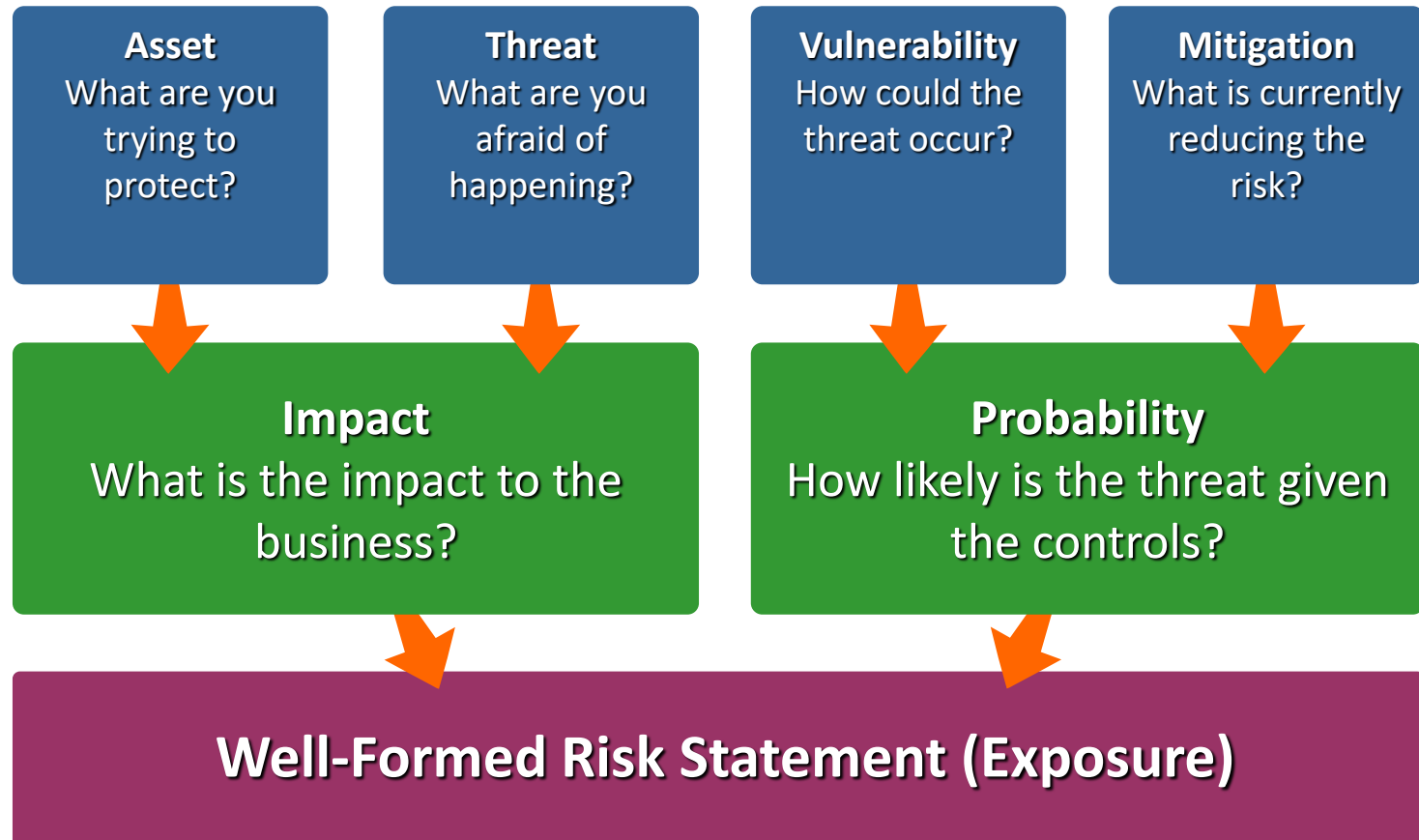
## SELECT AND APPLY SECURITY MEASURES: possible

- **Transfer the risk** (e.g. insurance)
- **Reduce vulnerability** (e.g. publicize security measures in order to deter attackers,
- **Choose effective preventive measures** (e.g. access control, encryption),
- **Reduce impact** (e.g. use fire extinguisher / firewall)
- **Recovery measures** (e.g. restoration from backup)

# SECURITY RISK MATRIX

RISK MATRIX		IMPACT				
LIKELIHOOD		NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
	VERY LIKELY	LOW	MEDIUM	HIGH	VERY HIGH	UNACCEPTABLE
	LIKELY	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
	MODERATELY LIKELY	LOW	LOW	MEDIUM	HIGH	HIGH
	UNLIKELY	LOW	LOW	LOW	MEDIUM	MEDIUM
	VERY UNLIKELY	LOW	LOW	LOW	LOW	LOW

# COMMUNICATING SECURITY RISK



# Security risk management program/strategy in the organization

## REACTIVE

process that responds to security events as they occur

## PROACTIVE

process that reduces the risk of new vulnerabilities in your organization

	Benefits	Drawbacks
Quantitative	<ul style="list-style-type: none"><li>• Risks prioritized by financial impact; assets - by their financial values</li><li>• Results facilitate management of risk by return on security investment</li><li>• Results can be expressed in management-specific terminology</li></ul>	<ul style="list-style-type: none"><li>• Impact values assigned to risks are based upon subjective opinions of the participants</li><li>• Very time - consuming</li><li>• Can be extremely costly</li></ul>
Qualitative	<ul style="list-style-type: none"><li>• Enables visibility and understanding of risk ranking</li><li>• Easier to reach consensus</li><li>• Not necessary to quantify threat frequency</li><li>• Not necessary to determine financial values of assets</li></ul>	<ul style="list-style-type: none"><li>• Insufficient granularity between important risks</li><li>• Difficult to justify investing in control as there is no basis for a cost-benefit analysis</li><li>• Results dependent upon the quality of the risk management team that is created</li></ul>



# Organization's SRM process

## VISION

to manage the protection of an organization's-wide assets,  
enabling the business to advance its mission

## MISSION

is to provide consistent identification, evaluation, and  
treatment of security risks to mitigate potential impacts to  
the business and prioritize protective activities

## GOALS

- to establish organizational policies, procedures, best practices, and capabilities
- to identify and manage security risks to the organization in an effective, consistent, and efficient manner

**EXTERNALLY DRIVEN**

**FINANCIAL RISKS**

ACCOUNTING STANDARDS  
INTEREST RATES  
FOREIGN EXCHANGE  
FUNDS AND CREDIT

**INFRASTRUCTURE RISKS**

COMMUNICATIONS  
TRANSPORT LINKS  
SUPPLY CHAIN  
TERRORISM  
NATURAL DISASTERS  
PANDEMIC

INTERNAL CONTROL  
FRAUD  
HISTORICAL LIABILITIES  
INVESTMENTS  
CAPEX DECISIONS  
LIQUIDITY AND CASHFLOW

RECRUITMENT  
PEOPLE SKILLS  
HEALTH AND SAFETY  
PREMISES  
IT SYSTEMS

**INTERNALLY DRIVEN**

M&A ACTIVITY  
R&D ACTIVITIES  
INTELLECTUAL PROPERTY  
CONTRACTS

BRAND EXTENSIONS  
BOARD COMPOSITION  
CONTROL ENVIRONMENT

ECONOMIC ENVIRONMENT  
TECHNOLOGY DEVELOPMENTS  
COMPETITION  
CUSTOMER DEMAND  
REGULATORY REQUIREMENTS

**MARKETPLACE RISKS**

PRODUCT RECALL  
CSR  
PUBLIC PERCEPTION  
REGULATOR ENFORCEMENT  
COMPETITOR BEHAVIOUR

**REPUTATIONAL RISKS**

**EXTERNALLY DRIVEN**

**Drivers of SRM**

# CONCLUSIONS

## 1. Problems:

- Lack of precision
- Volume of work and volume of output
- Integrating them into a "normal" development process

## 2. Decide on security risk management methodology

## 3. Determine your maturity level

## 4. Conduct security risk assessment & decision-making support

## 5. Implement controls & measure effectiveness



**THANK YOU FOR YOUR ATTENTION!!!**

**Prof. dr. Raimundas Kalesnykas**

*International security expert*

*Faculty of Law, Kazimieras Simonavicius University, Vilnius (Lithuania)*

*e-mail: [raimundas.kalesnykas@ksu.lt](mailto:raimundas.kalesnykas@ksu.lt) [www.ksu.lt](http://www.ksu.lt)*

**NORDPLUS Higher Education Intensive Course**

**“Organization and Individual Security” (14.08.2017.–25.08.2017)**

*14:20 – 15:50, 23 August 2017, Turība University, Riga, Latvia*