# Policy, Strategy and Operations

IWOSI: The Information Warfare, Cyber Warfare and Open Sources Intelligence – Yasar University Izmir, Turkey 2012

**Part I-2: 2012.04.18, 10:00-12:00**

Dr. Nikolaj Goranin, CISM, CISA
Vilnius Gediminas Technical University

# Risk Management

- Risk management is a process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss.
- There is a risk in doing something and not doing something.
- Organization must understand the relevant risk.
- Risk management is a basis for decision making in sphere of information security.

# Related Definitions

- Risk assessment
- Controls – protect against threats
- Countermeasures – reduce threats
- Quantitave R.A. methods
- Qualitative R.A. methods
- Semiquantative R.A. methods

# Outcomes of Risk Management

- Understanding of threats, vulnerabilities, risk profile
- Understanding of risk exposure and consequences of compromise
- Awareness of risk management priorities based on potential consequences
- Risk mitigation strategy sufficient to achieve acceptable consequences from **residual risk**
- Organizational acceptance/deference based on an understanding of the potential consequences of the residual risk

# Developing a Risk Management Program

- Establish context and purpose
- Define scope and charter
- Determine objectives
- Determine methodologies
- Designate program development team

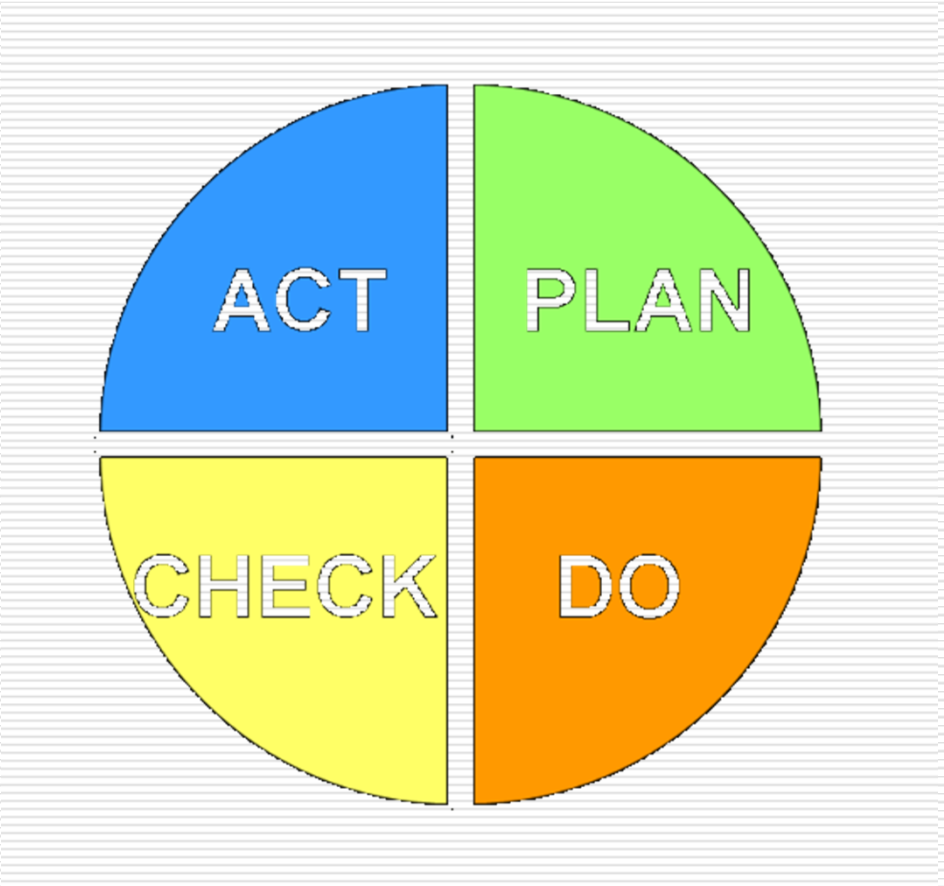
# Concepts

- Threat
- Vulnerability
- Risk
- Control
- Countermeasure
- Criticality
- Sensitivity
- Recovery Time Objectives (RTO)
- Recovery Point Objectives (RPO)
- Service Delivery Objectives (SDO)
- …

# Risk Management Process

- Establish scope and boundaries
- Risk assessment
- Risk treatment
- Acceptance of residual risk
- Risk communication and monitoring

# Risk Management and PDCA



# Risk Assessment

1. Identification
2. Analysis
3. Evalution

# Risk Treatment

- Avoid
- Reduce
- Transfer
- Retain

# Defining the Context

- External Environment:
  - Market, financial and political environment;
  - Law and regulatory environment;
  - Social and cultural conditions;
  - External stakeholders.

- Internal Environment:
  - Key business drivers;
  - Organizations SWOT;
  - Internal stakeholders;
  - Structure and control;
  - Assets and resources;
  - …

# NIST Risk Assessment Methodology

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

# Threats

- Natural
- Unintentional
- Intentional physical
- Intentional non-physical

# Vulnerabilities

- Defective software
- Improper configuration
- Inadequate compliance enforcement
- Poor network design
- Uncontrolled processes
- Inadequate management
- Insufficient staff
- Lack of knowledge
- Lack of proper maintenance
- Poor passwords
- Untested technology
- Unprotected communication
- Lack of redundancy
- Poor management communication

# Risks

- Facility risk
- Health and safety risk
- Information security risk
- Reputation risk
- Strategic risk
- Processing risk
- Technology risk
- Management risk
- Criminal risk
- Human resources risk
- Supplier risk
- Ethics risk
- Geopolitical risk
- Cultural risk
- …

# Calculating Risk Value

- Quantative
- Qualitative
- Semiquantitave

- Usually: Product of likelihood and impact.

# Control categories

- Preventive
- Detective
- Corrective
- Compensatory
- Deterrent

# Discussion