Policy, Strategy and Operations

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

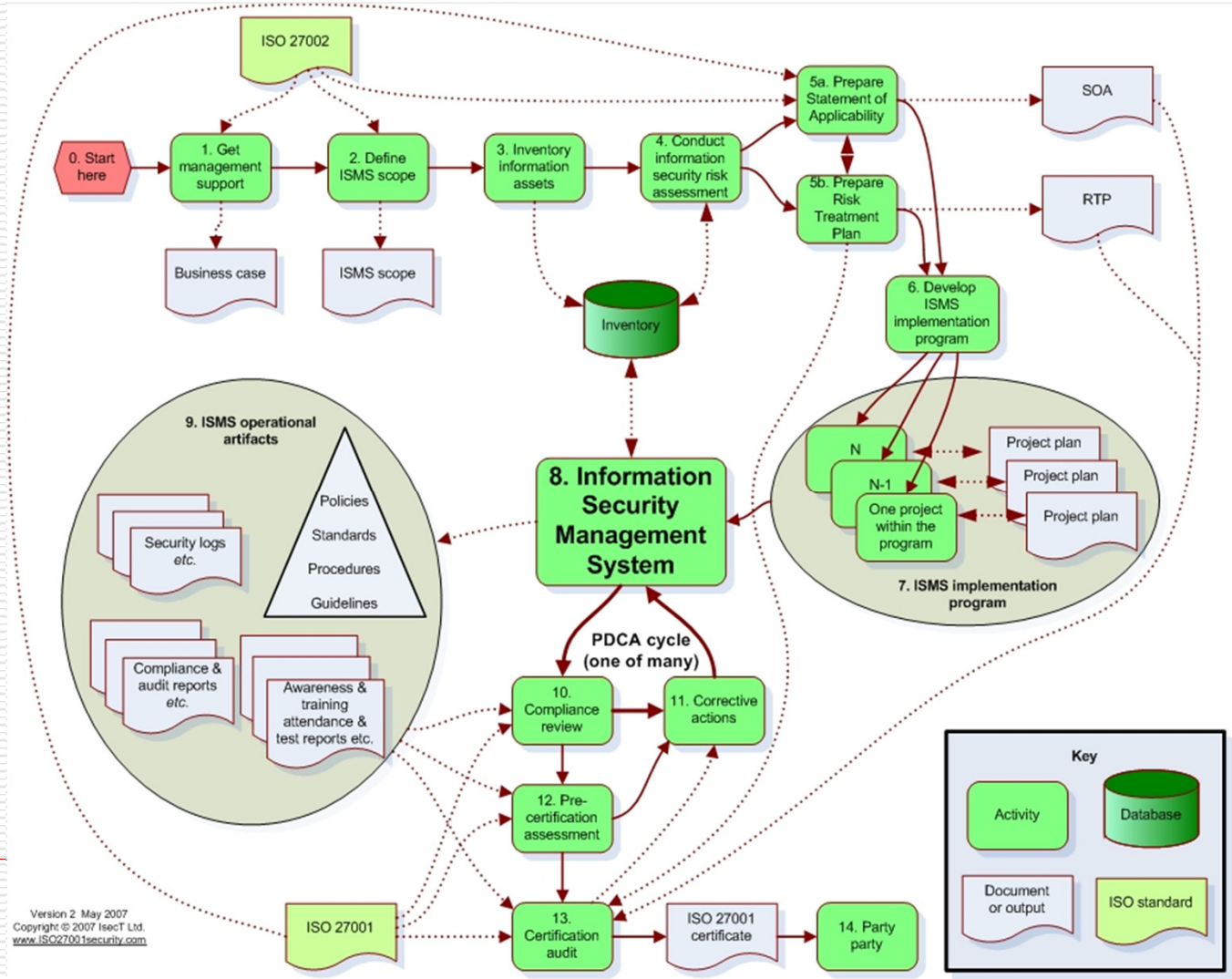
Part II-1: 2012.04.18, 13:30-17:00

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

ISO 27001 ISMS

- ISMS – Information security management system
- ISMS - part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
- ISO 27001 4.1 requirement
  - The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and the risks they face.

Information Security Management Program



ISMS and International Standards

- ISO 27001 requirements

- Requirements to ISMS
- Control objectives

- *Ref: ISO 27001*

ISMS and CobiT

- COBIT (Control Objectives for Information and related Technology) by ISACA (Information Systems Audit and Control Association)

- Managers, Auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies' assets through the development of an IT governance model.

- COBIT covers four domains:
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate

Appropropriate CobiT Requirement

IT PROCESSES Plan and Organize	
PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

IT PROCESSES Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes

IT PROCESSES Deliver and Support	
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

IT PROCESSES Monitor and Evaluate	
ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

PCI DSS

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

ISMS Budgeting

- Employee time
- Contractor and consultant fee
- Equipment costs
- Space requirements
- Testing resources
- Creation of supporting documentation
- Ongoing maintenance
- Contingencies for unexpected costs

Common Information Security Management Challenges

- Inadequate management support
  - Make management your sponsor
- Inadequate funding
  - Show the importance
- Inadequate staffing
  - Delegation, outsourcing, recruitment

Outsourcing ISMS

- Loss of essential skills
- Lack of visibility of information security processes
- Access control risks
- Complexity of incident management
- Cultural differences
- Dependency on supplier
- SLA

ISMS Evaluation

- Compliance vs. Testing
- Internal and External Audit
  - Systems audit
  - Technology audit
  - Process audit
- Annual Audit / Self-Assessment
- Vulnerability Scanning and Penetration Testing

ISACA Audit Framework – /I/

- Audit Charter
  - Purpose, accountability, engagement letter
- Independence
  - Professional and organizational
- Professional ethics and standards
  - Code of Ethics, due diligence
- Planning
  - Coverage, risk-based approach, methods

ISACA Audit Framework – /II/

- Performance of audit work
  - Evidence, documentation
- Reporting
  - Findings, conclusions, recommendations, signed
- Follow-up activities
  - Control of recommendation fulfillment

ISACA Audit Framework – /III/

- Irregularities and illegal acts
- IT Governance
- Use of risk assessment
- Audit materiality
- Using the work of other experts
- Audit evidence
- IT controls
- E-commerce

ISACA Code of Professional Ethics

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting the profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Evidence Gathering Techniques

- Reviewing IS organizational structures
- Reviewing policies and procedures
- Reviewing IS standards
- Reviewing IS documentation
- Interviewing
- Observing processes and employee performance
- Reperformance
- Walkthrough
- System configuration analysis

Evidence requirements

- Independence of the provider of the evidence
- Qualification of the individual providing the information/evidence
- Objectivity of the evidence
- Timing of the evidence

Sampling Requirements

- Statistical sampling
- Non-statistical sampling

Discussion