2019-03-18

IT Security #6

Organizational IT Security Policy & Analysis & Implementation
Theme C (ii) on Management issues

Niels Christian Juul

Informatik
Datalogi
Roskilde Universitet

Roskilde Universitet
Niels Christian Juul
Hus 08.2-071
Universitetsvej 1
4000 Roskilde
ncjuul@ruc.dk

IT-security

Course book

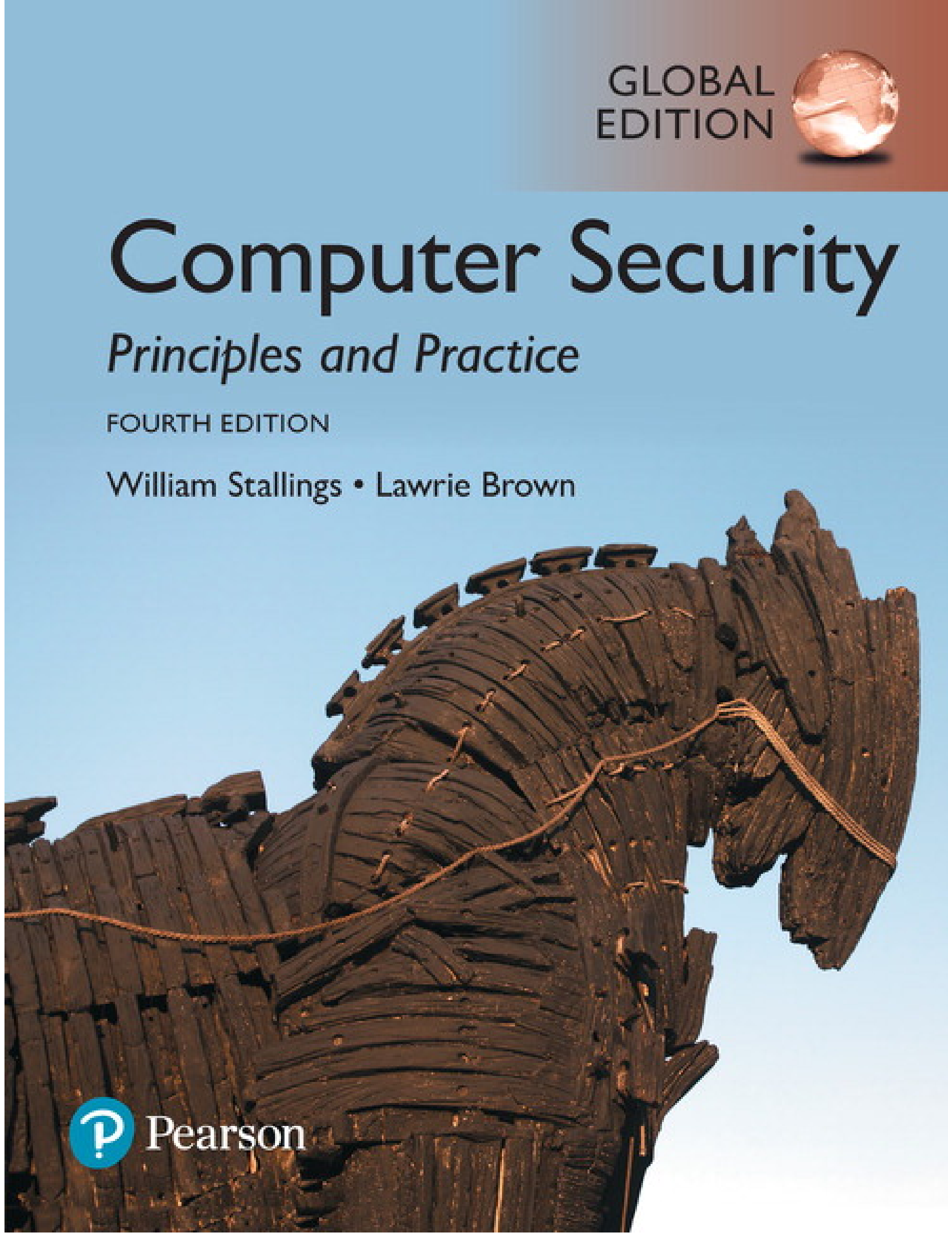
- Chapter 14 + 15 today

Next time:

- Selected parts of Chapter 16, 17, 18

Student presentations, eg.

- 17.3 on e-mail policy (compare to RUC)
- ??



Learning outcome

Be able to

- manage information security in an organization
- conduct a thorough risk analysis wrt organizational information security
- select relevant security controls
- create an security implementation plan

Exam themes/questions:

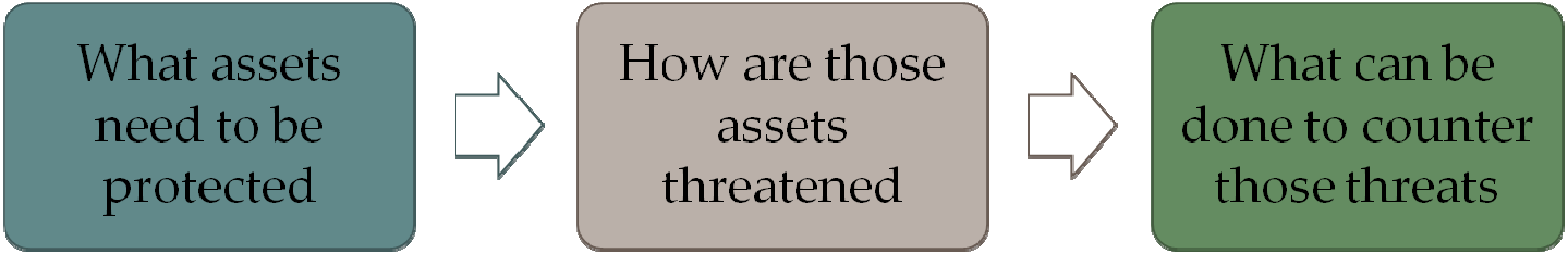
- What is Security Policy and how should it be managed?
- How to conduct a Detailed Security Risk Assessment?
- How to make a Security Implementation Plan?

Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. Risk Assessment, Overview, Ch. 14.3
4. Detailed Risk Analysis, Ch. 14.4
5. Case: Silver Mine, Ch. 14.5
6. Security Controls, Ch. 15.2 (Monica)
7. Security Planning, Ch. 15.3
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

IT Security Management Overview

Is the formal process of answering the questions:



What assets need to be protected
How are those assets threatened
What can be done to counter those threats

- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

Table 14.1
27000 Series of Standards on IT Security Techniques

27000:2016	“Information security management systems - Overview and vocabulary” provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	“Information security management systems – Requirements” specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2013	“Code of practice for information security management” provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	“Information security management system implementation guidance” details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	“Information security management – Measurement” provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	“Information security risk management” provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2015	“Requirements for bodies providing audit and certification of information security management systems” specifies requirements and provides guidance for these bodies.

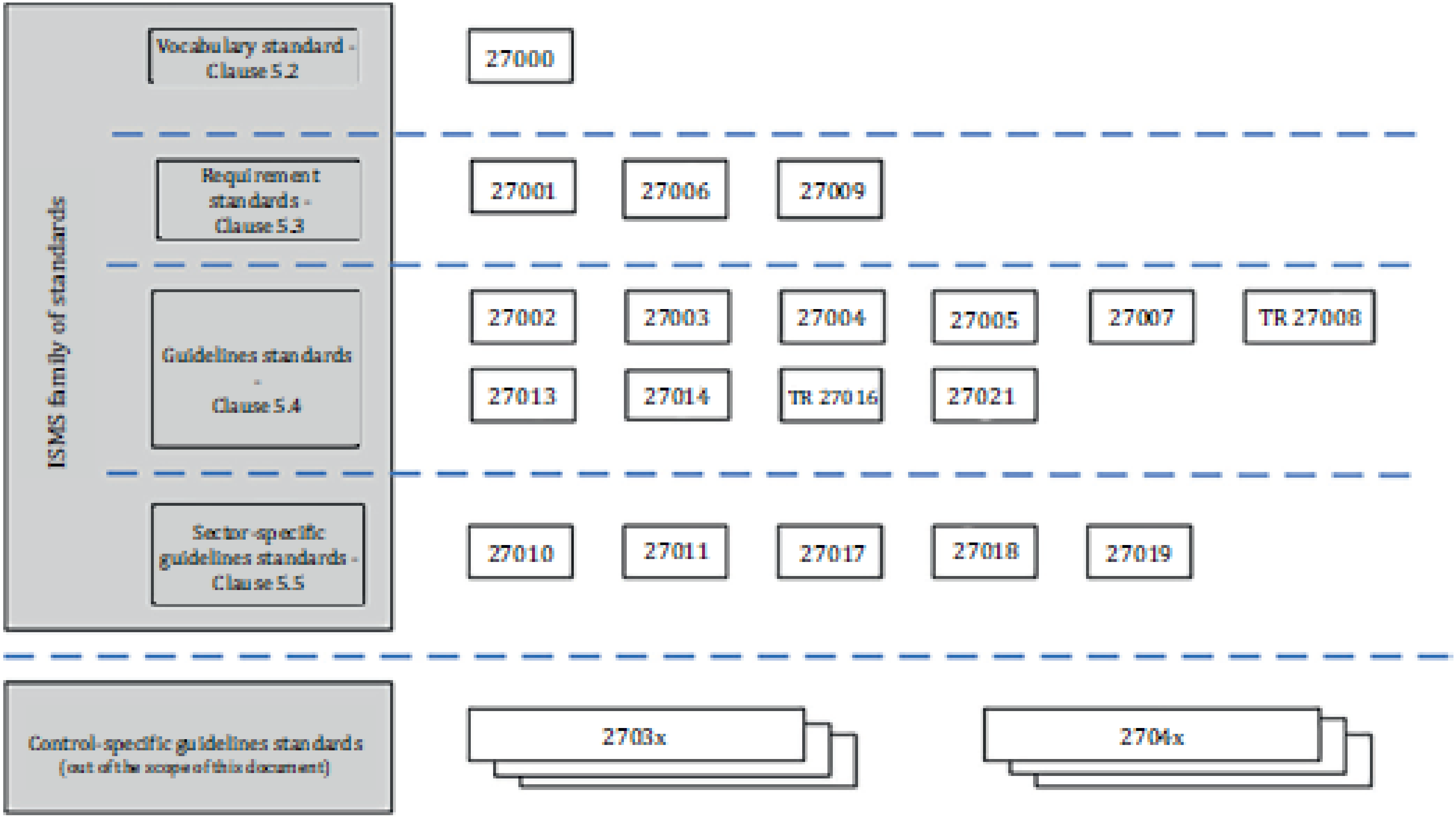
ISO 27000 Series Information technology – security techniques

ISMS

27000:2018	Information security management systems -- Overview and vocabulary
27001:2013	Information security management systems -- Requirements
27002:2013	Code of practice for information security controls
27003:2017	Information security management systems -- Guidance
27004:2016	Information security management -- Monitoring, measurement, analysis and evaluation
27005:2018	Information security risk management
27006:2015	Requirements for bodies providing audit and certification of information security management systems
27007:2017	Guidelines for information security management systems auditing
27008:2019	Guidelines for the assessment of information security controls
27009:2016	Sector-specific application of 27001 -- Requirements
27010:2015	Information security management for inter-sector and inter-organizational communications

Informatik
Datalogi
Roskilde Universitet

ISO 27000 ISMS family of standards relationship



ISMS family of standards

Vocabulary standard - Clause 5.2

27000

Requirement standards - Clause 5.3

27001

27006

27009

Guidelines standards - Clause 5.4

27002

27003

27004

27005

27007

TR 27008

27013

27014

TR 27016

27021

Sector-specific guidelines standards - Clause 5.5

27010

27011

27017

27018

27019

Control-specific guidelines standards (out of the scope of this document)

2703x

2704x

ISO 27000 Series Information technology – security techniques

27011:2016	Code of practice for Information security controls based on 27002 for telecommunications organizations
27013:2015	Guidance on the integrated implementation of 27001 and 20000-1
27014:2013	Governance of information security
27016:2014	Information security management -- Organizational economics
27017:2015	Code of practice for information security controls based on 27002 for cloud services
27018:2019	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
27019:2017	Information security controls for the energy utility industry
27021:2017	Competence requirements for information security management systems professionals
27023:2015	Mapping the revised editions of 27001 and 27002
27030 [U]	Guidelines for security and privacy in Internet of Things (IoT)
27031:2011	Guidelines for information and communication technology readiness for business continuity

ISO 27000 Series Information technology – security techniques

27032 [U]	IT Security Techniques -- Cybersecurity -- Guidelines for Internet Security
27033-1:2015	Network security Part 1: Overview and concepts
27033-2:2012	Part 2: Guidelines for the design and implementation of network security
27033-3:2010	Part 3: Reference networking scenarios -- Threats, design techniques and control issues
27033-4:2014	Part 4: Securing communications between networks using security gateways
27033-5:2013	Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
27033-6:2016	Part 6: Securing wireless IP network access

ISO 27000 Series Information technology – security techniques

27034-1:2011	Application security Part 1: Overview and concepts
27034-2:2015	Part 2: Organization normative framework
27034-3:2018	Part 3: Application security management process
27034-4 [U]	Part 4: Validation and verification
27034-5:2017	Part 5: Protocols and application security controls data structure
27034-6:2016	Part 6: Case studies
27034-7:2018	Part 7: Assurance prediction framework
27035-1:2016	Information security incident management Part 1: Principles of incident management
27035-2:2016	Part 2: Guidelines to plan and prepare for incident response
27035-3 [U]	Part 3: Guidelines for incident response operations

ISO 27000 Series Information technology – security techniques

27036-1:2014	Information security for supplier relationships Part 1: Overview and concepts
27036-2:2014	Part 2: Requirements
27036-3:2013	Part 3: Guidelines for information and communication technology supply chain security
27036-4:2016	Part 4: Guidelines for security of cloud services
27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
27038:2014	Specification for digital
27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
27040:2015	Storage security
27041:2015	Guidance on assuring suitability and adequacy of incident investigative method
27042:2015	Guidelines for the analysis and interpretation of digital evidence
27043:2015	Incident investigation principles and processes

ISO 27000 Series Information technology – security techniques

27045 [U]	Big data security and privacy -- Processes
27050-1:2016	Electronic discovery Part 1: Overview and concepts
27050-2:2018	Part 2: Guidance for governance and management of electronic discovery
27050-3:2017	Part 3: Code of practice for electronic discovery
27050-4 [U]	Part 4: Technical readiness
27070 [U]	Security requirements for establishing virtualized roots of trust
27099 [U]	Public key infrastructure -- Practices and policy framework
27100 [U]	Cybersecurity -- Overview and concepts
27101 [U]	Cybersecurity -- Framework development guidelines
27102 [U]	Information security management guidelines for cyber insurance
27103:2018	Cybersecurity and ISO and IEC Standards

ISO 27000 Series Information technology – security techniques

27550 [U]	Privacy engineering
27551 [U]	Requirements for attribute-based unlinkable entity authentication
27552 [U]	Extension to 27001 and 27002 for privacy information management -- Requirements and guidelines
27553 [U]	Security requirements for authentication using biometrics on mobile devices
27554 [U]	Application of ISO 31000 for assessment of identity management-related risk
27555 [U]	Establishing a PII deletion concept in organizations
27570 [U]	Privacy guidelines for Smart Cities

And you should also look for security techniques at other series in ISO, eg. 9700, 10100, 11000, 13000, 15000, 18000, 19000, 20000, 24000, and 29000

ISO / IEC JTC 1 / SC 27 IT Security techniques

BUT

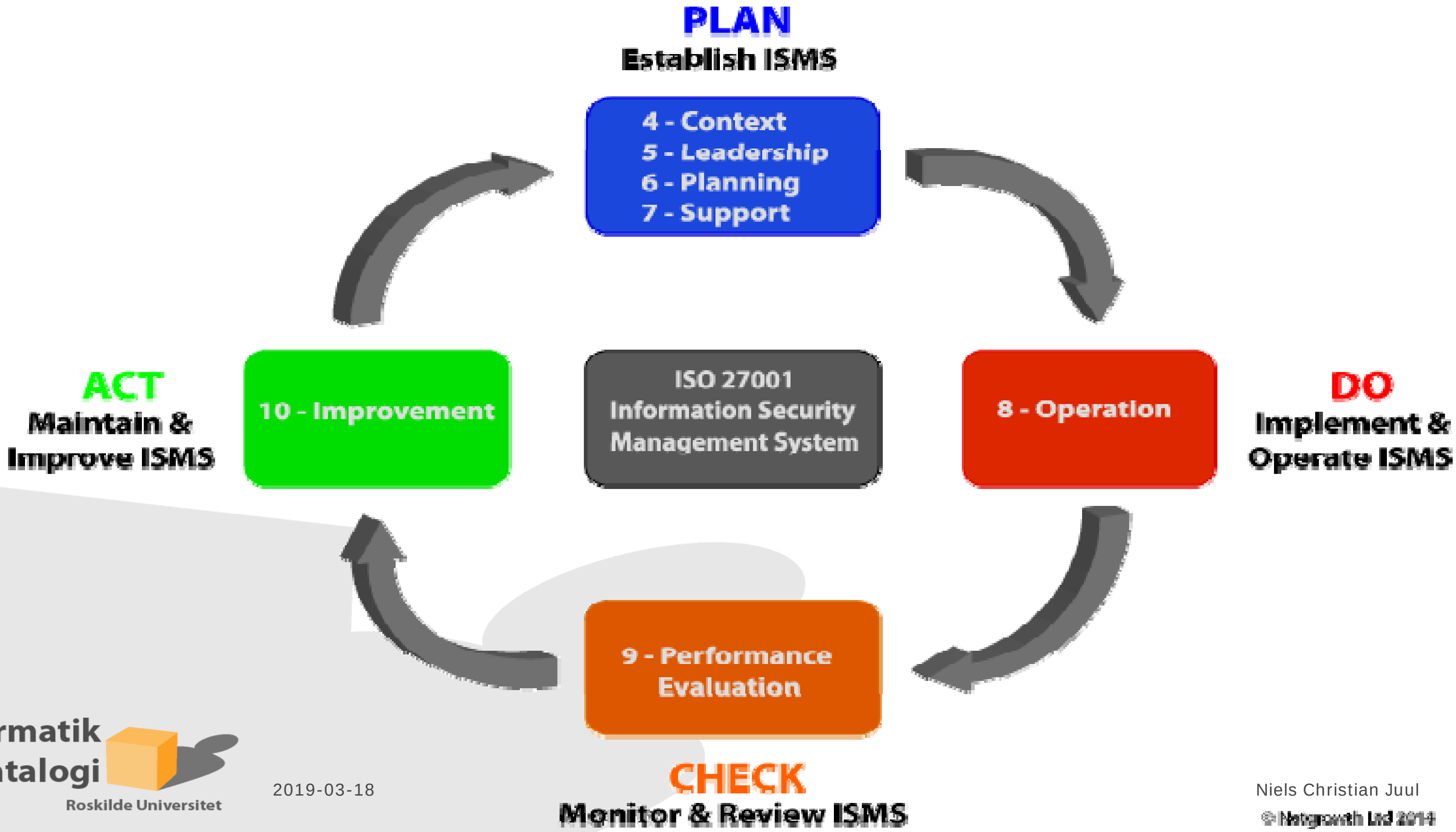
- What are the "drawbacks" of ISO standards?

- Cost of each standard downloaded
- Time to learn the standard

- Time and cost to plan, implement, audit, and revise (27001)

- Focus on procedures more than actual effects and efficiency

Information Security Management System



PLAN
Establish ISMS

4 - Context
5 - Leadership
6 - Planning
7 - Support

DO
Implement & Operate ISMS

8 - Operation

ISO 27001
Information Security Management System

CHECK
Monitor & Review ISMS

9 - Performance Evaluation

ACT
Maintain & Improve ISMS

10 - Improvement

© Netgrowth Ltd 2014

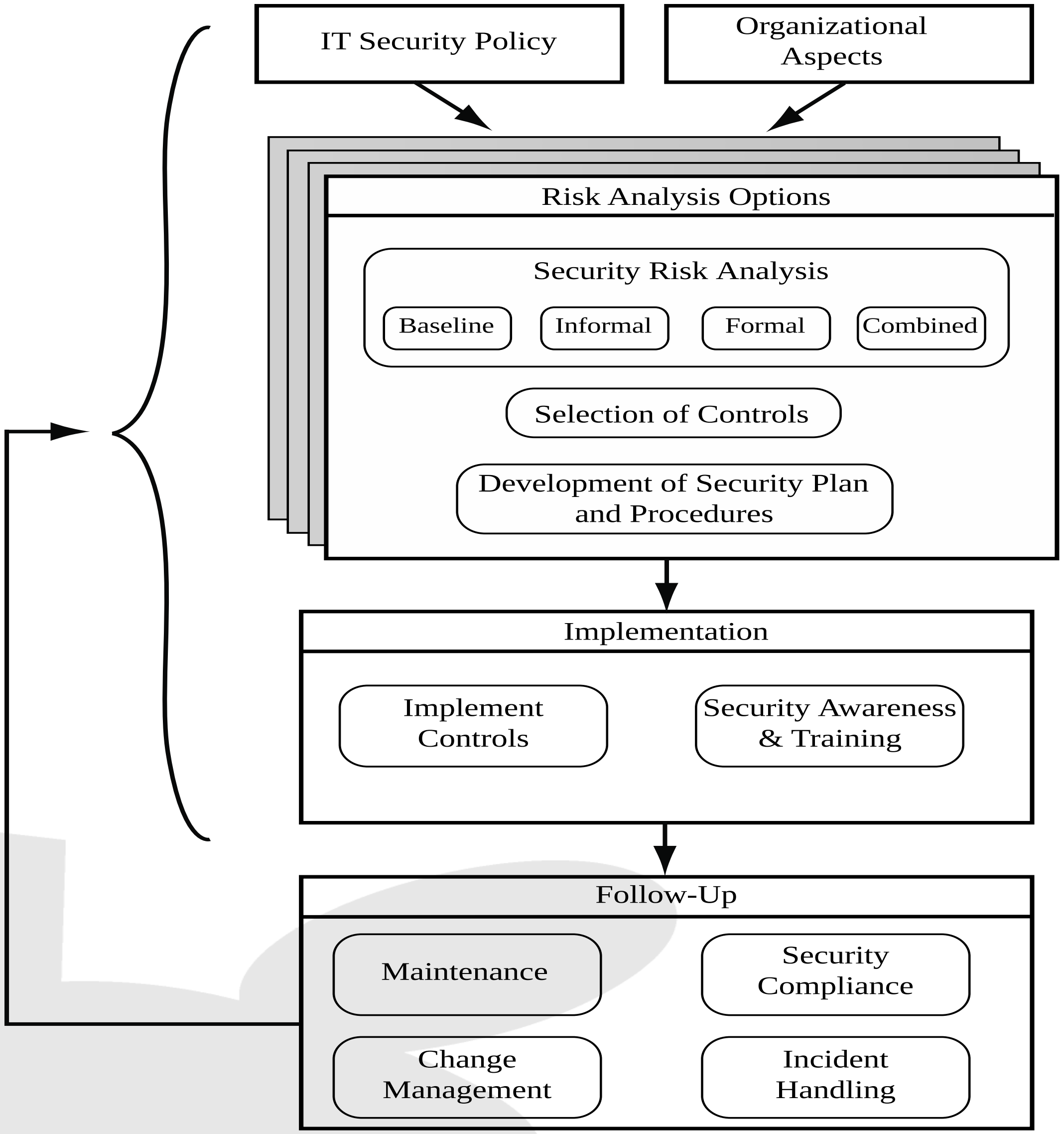
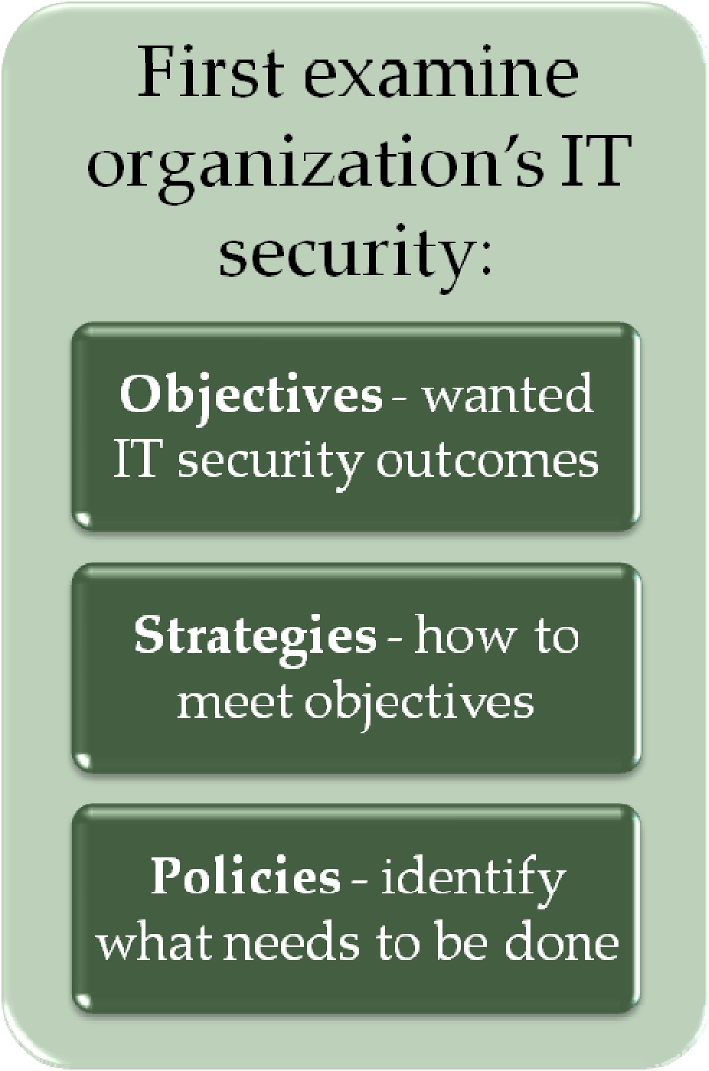


Figure 14.1 Overview of IT Security Management

Organizational Context and Security Policy

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments
- Examine role and importance of IT systems in organization



First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of responsibilities
- Risk management approach
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer (CISO)
  - To provide consistent overall supervision
  - Liaison with senior management
  - Maintenance of IT security objectives, strategies, policies
  - Handle incidents
  - Management of IT security awareness and training programs
  - Interaction with IT project security officers
- Large organizations need separate IT project security officers associated with major projects and systems
  - Manage security policies within their area

Roskilde University Information Security Policy

Find the university's documented official policy:

General information security policy for Roskilde University

- How long does it take to find and download it?
- Is it adequately published (in English and/or Danish) ?

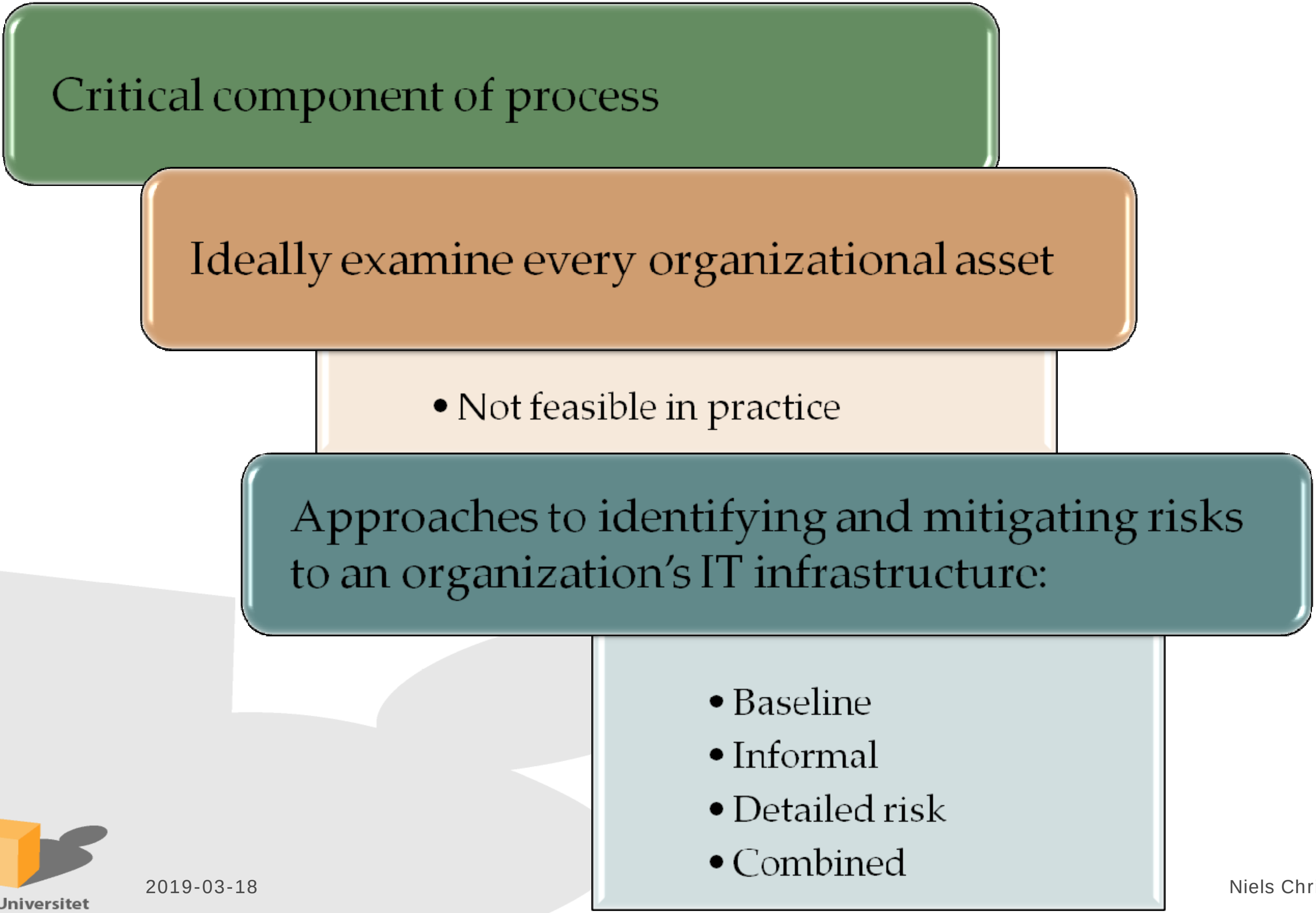
And review it:

- Which of the topics listed on page 485-486 in the book is addressed and which not?
- Is the document adequate for its purpose?

Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. **Risk Assessment, Overview, Ch. 14.3**
4. Detailed Risk Analysis, Ch. 14.4
5. Case: Silver Mine, Ch. 14.5
6. Security Controls, Ch. 15.2 (Monica)
7. Security Planning, Ch. 15.3
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

Security Risk Assessment



Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use “industry best practice”
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

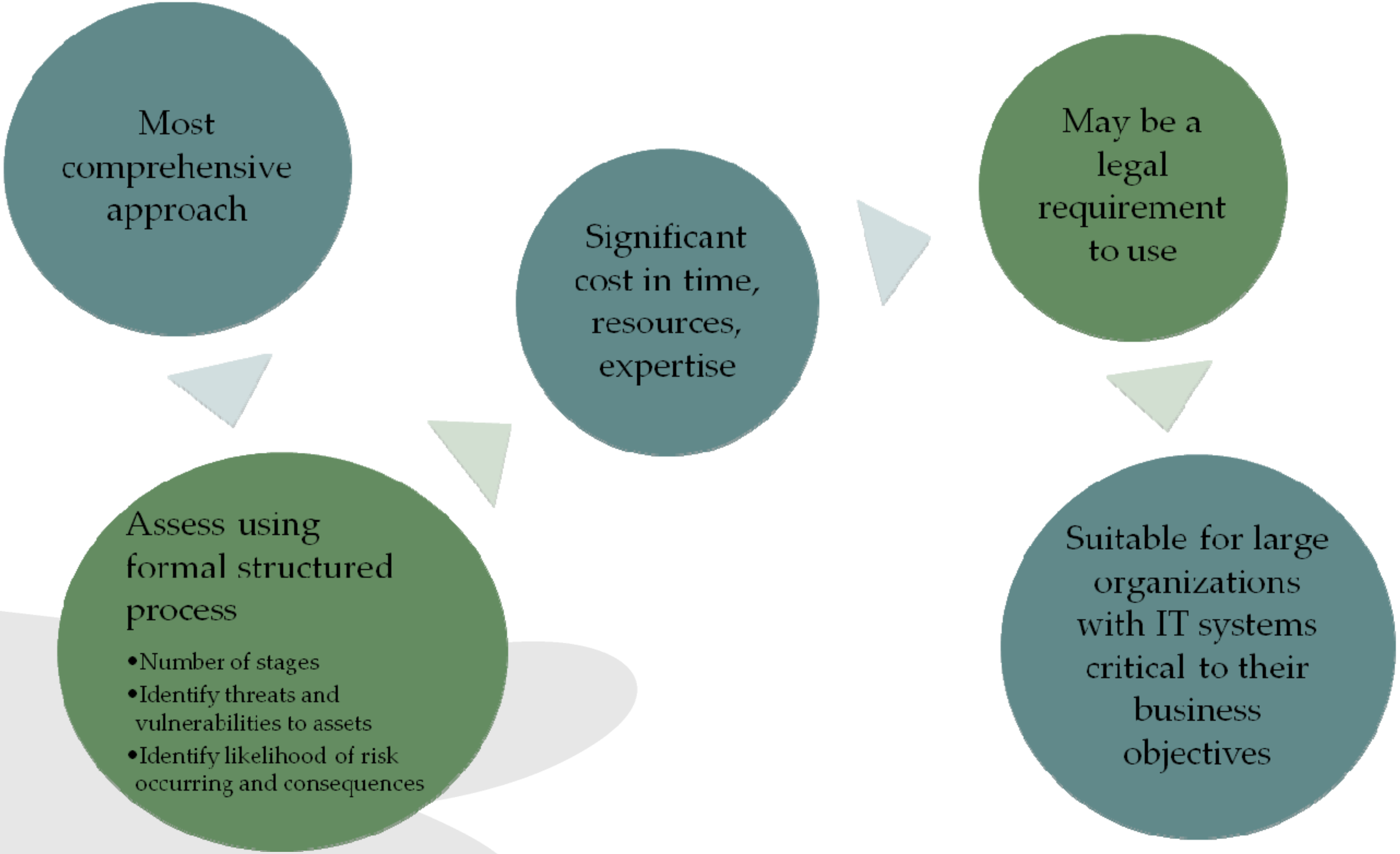
Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis



Most comprehensive approach

Assess using formal structured process

- Number of stages
- Identify threats and vulnerabilities to assets
- Identify likelihood of risk occurring and consequences

Significant cost in time, resources, expertise

May be a legal requirement to use

Suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- Combines elements of the baseline, informal, and detailed risk analysis approaches
- Aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time
- Approach starts with the implementation of suitable baseline security recommendations on all systems
- Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment
- A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements
- Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted
- Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

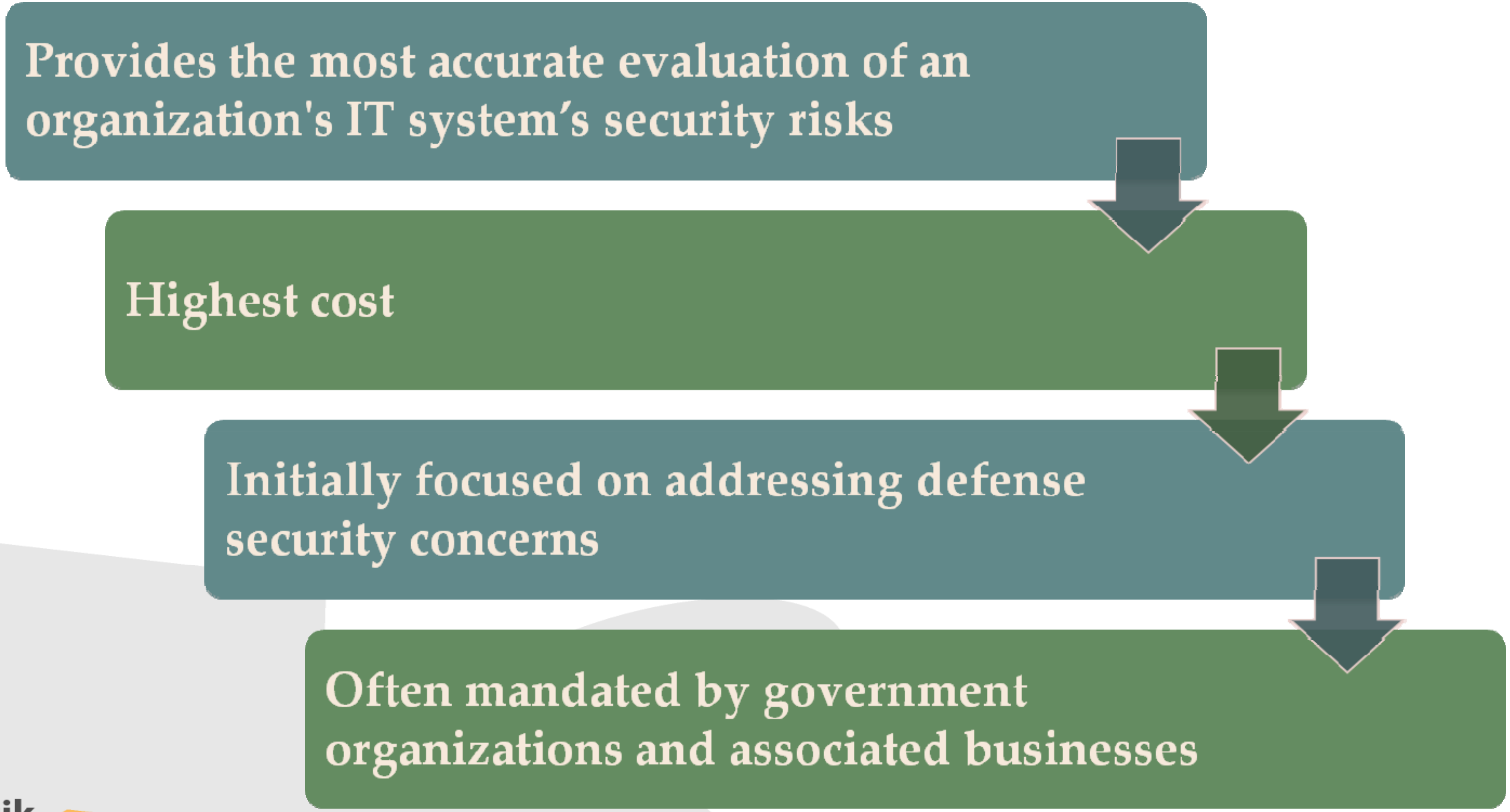
Exercise

- Which approach is reflected in the security policy document from Roskilde University, 2012?
- Why?

Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. Risk Assessment, Overview, Ch. 14.3
4. **Detailed Risk Analysis, Ch. 14.4**
5. Case: Silver Mine, Ch. 14.5
6. Security Controls, Ch. 15.2 (Monica)
7. Security Planning, Ch. 15.3
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

Detailed Security Risk Analysis



Provides the most accurate evaluation of an organization's IT system’s security risks

Highest cost

Initially focused on addressing defense security concerns

Often mandated by government organizations and associated businesses

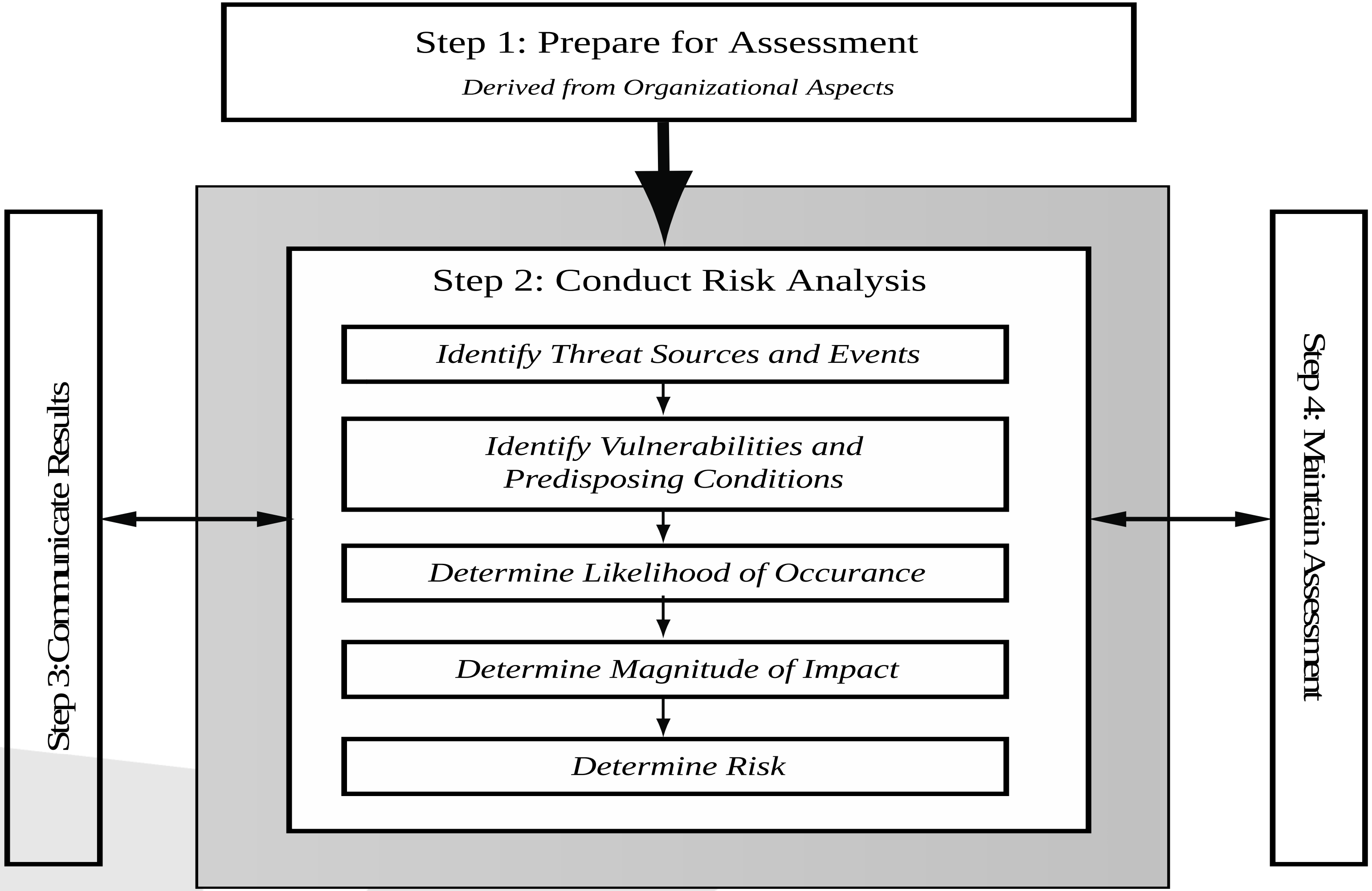

Step 1: Prepare for Assessment
Derived from Organizational Aspects
Step 2: Conduct Risk Analysis
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurance
Determine Magnitude of Impact
Determine Risk
Step 3:Communicate Results
Step 4: Maintain Assessment

Figure 14.3 Risk Assessment Process

Step 1: Establishing the Context

- Initial step
  - Determine the basic parameters of the risk assessment
  - Identify the assets to be examined
- Explores political and social environment in which the organization operates
  - Legal and regulatory constraints
  - Provide baseline for organization’s risk exposure
- Risk appetite
  - The level of risk the organization views as acceptable

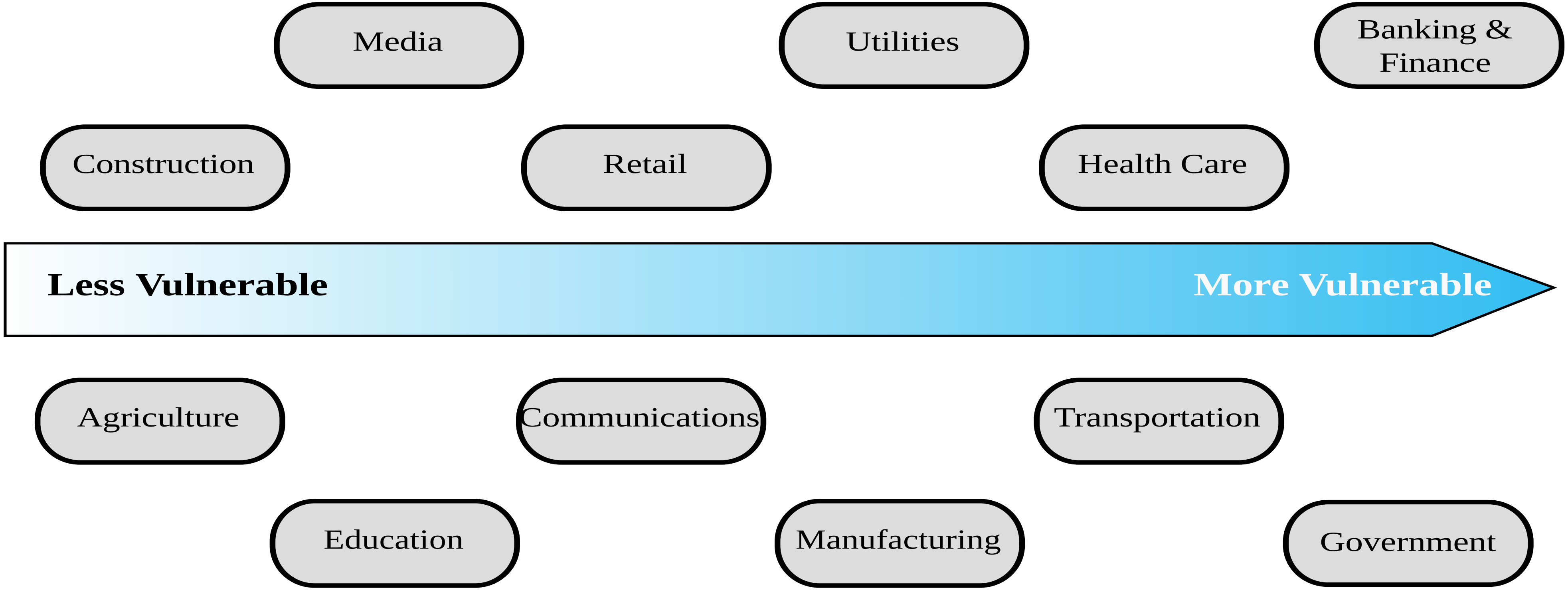
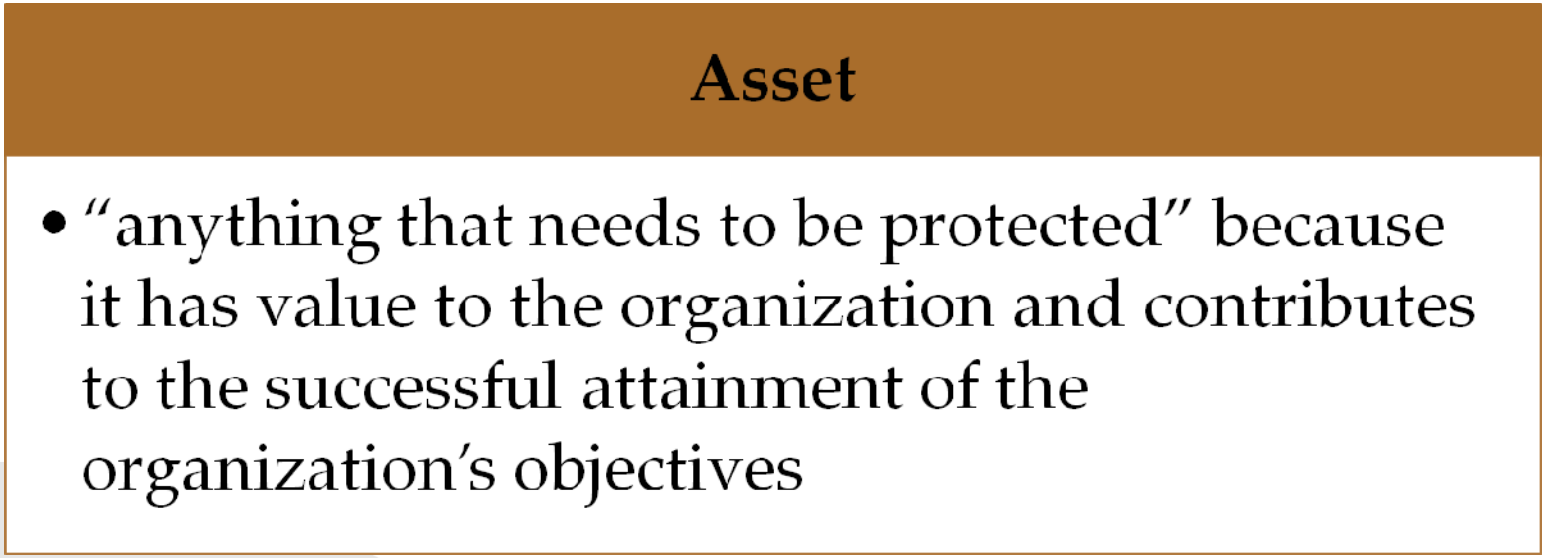


Figure 14.4 Generic Organizational Risk Context

Asset Identification

- Last component is to identify assets to examine
- Draw on expertise of people in relevant areas of organization to identify key assets
  - Identify and interview such personnel



Asset

- "anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives

Exercise: Roskilde case

1. Identify an important asset, that RUC needs to care about

Step 2: Conduct Risk Analysis

- Identify the threats or risks the assets are exposed to
- Vulnerability Identification
- Likelihood of occurrence
- Cost to organization in case of incident
- Determine risk

Terminology

Asset:

- A system resource or capability of value to its owner that requires protection

Threat:

- A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner

Vulnerability:

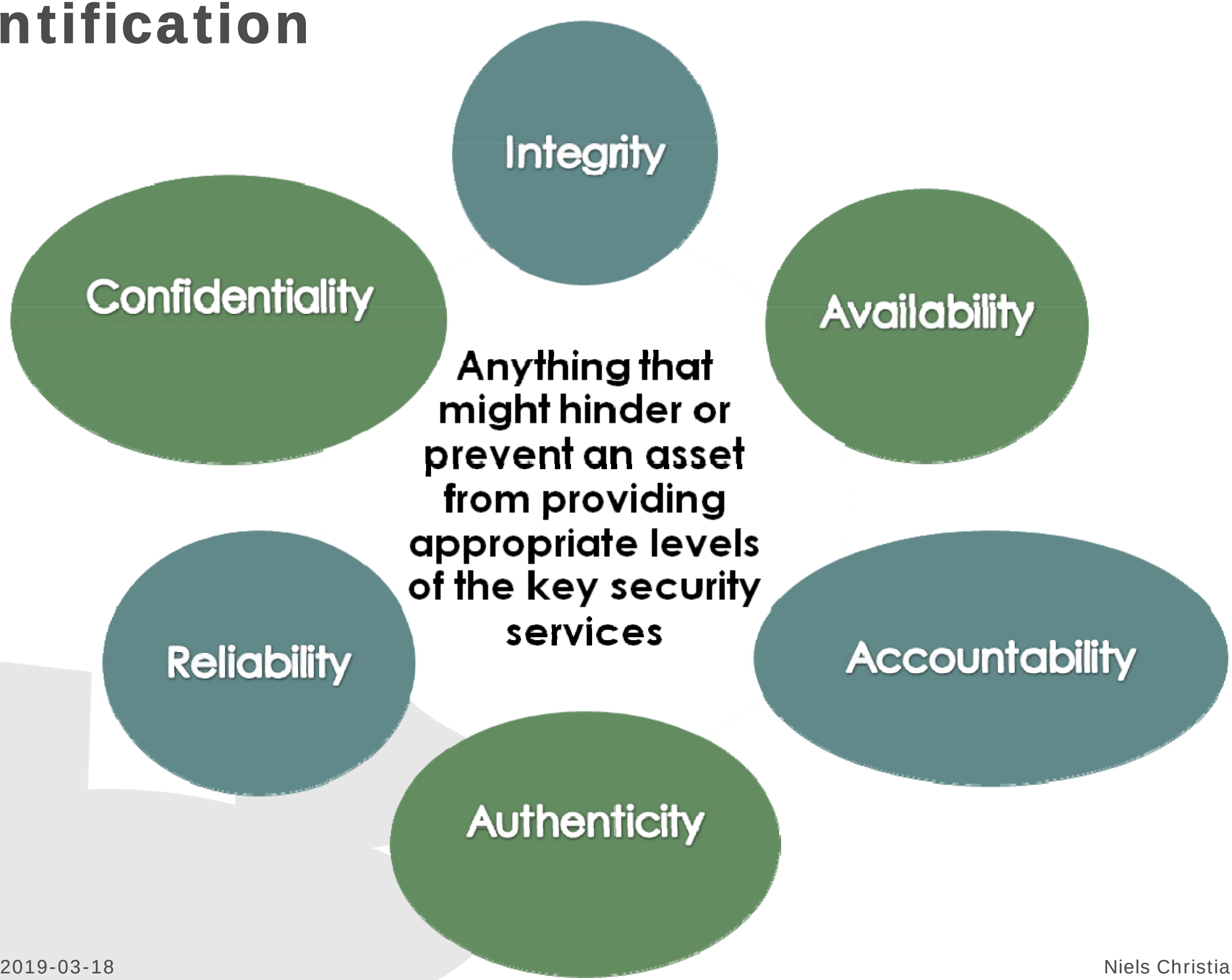
- A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat

Risk:

- The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner

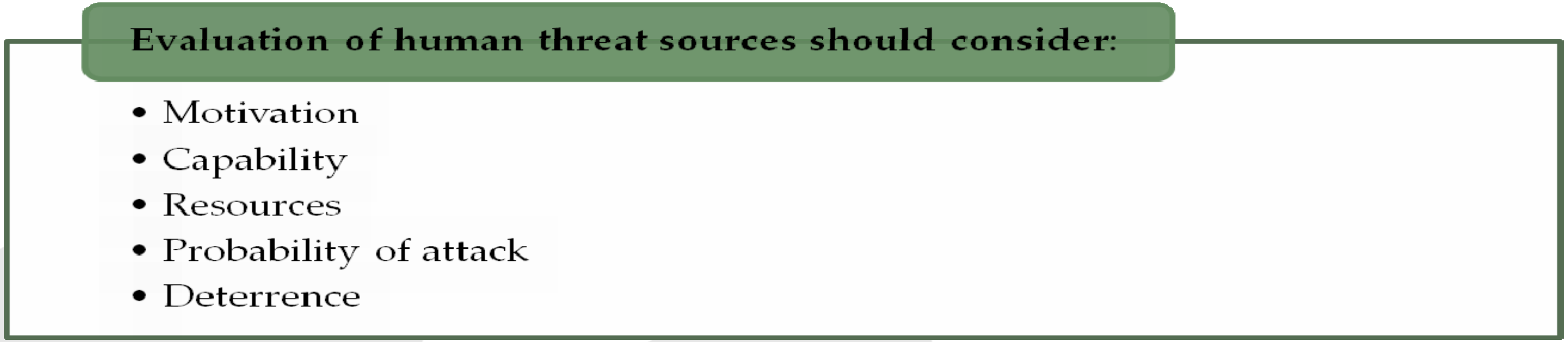
Threat Identification

- A threat is:


Integrity
Confidentiality
Availability
Anything that might hinder or prevent an asset from providing appropriate levels of the key security services
Reliability
Accountability
Authenticity

Threat Sources

- Threats may be
  - Natural “acts of God”
  - Man-made
  - Accidental or deliberate



Evaluation of human threat sources should consider:

- Motivation
- Capability
- Resources
- Probability of attack
- Deterrence

- Any previous experience of attacks seen by the organization also needs to be considered

Vulnerability Identification

- Identify exploitable flaws or weaknesses in organization’s IT systems or processes
    - Determines applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- Outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

Exercise: Roskilde case

1. Identify an important asset, that RUC needs to care about
2. **What are the treats to that asset?**
3. **Which vulnerabilities?**

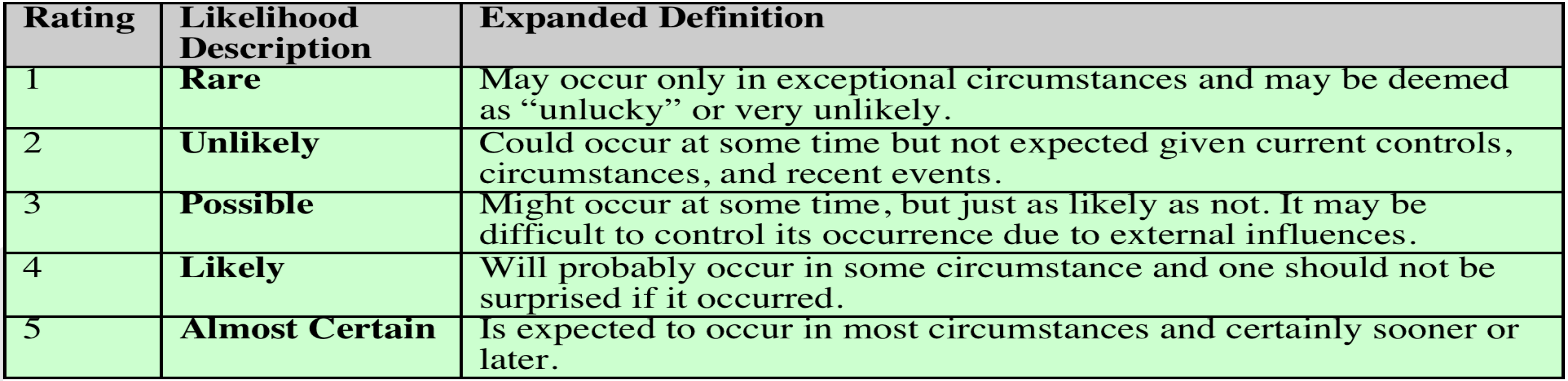
Analyze Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
- Specify consequence should threat occur
- Derive overall risk rating for each threat
  - Risk = probability threat occurs x cost to organization
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative, ratings

Analyze Existing Controls

- Existing controls used to attempt to minimize threats need to be identified
- Security controls include:
  - Management
  - Operational
  - Technical processes and procedures
  - Use checklists of existing controls and interview key organizational staff to solicit information

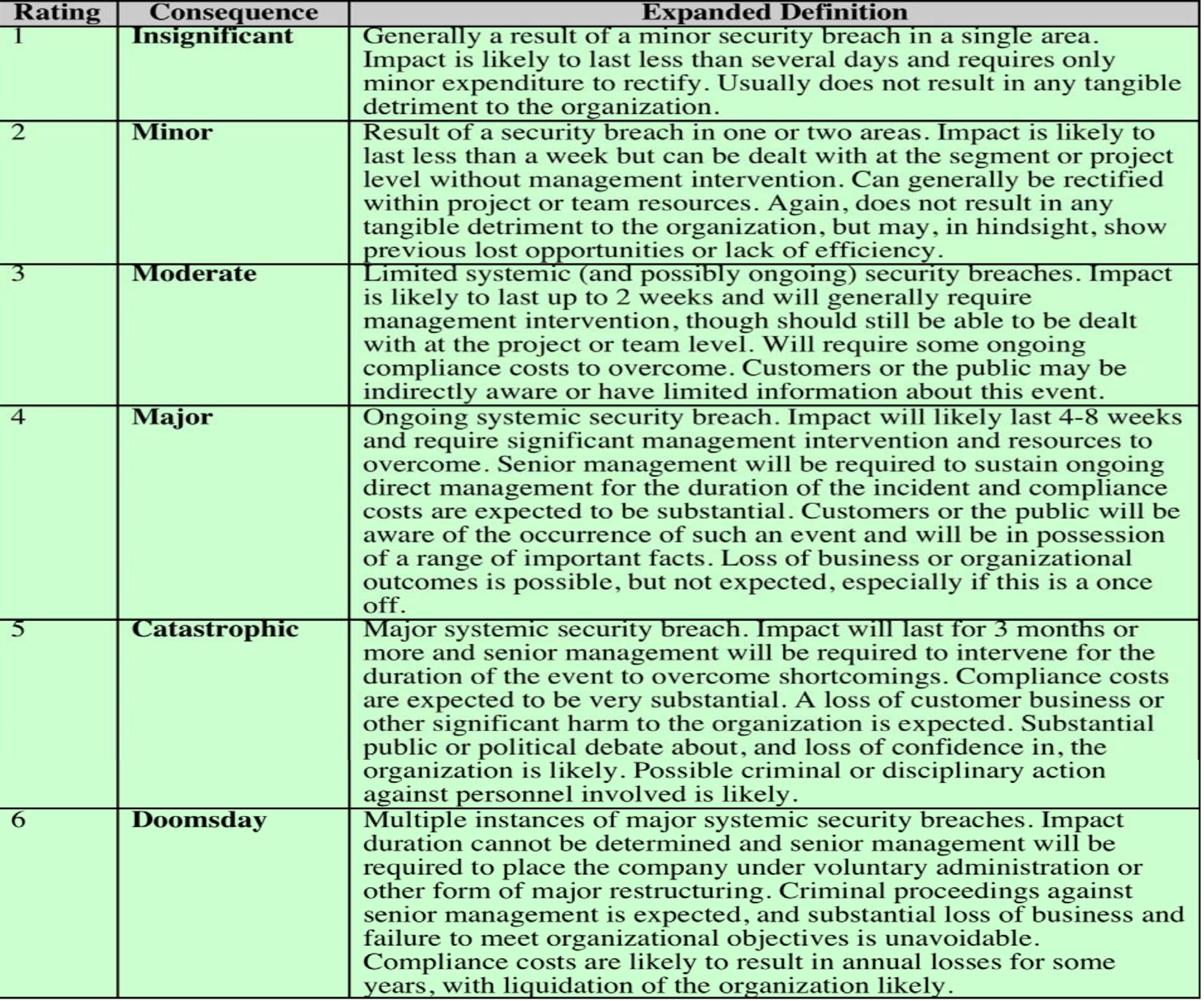
Table 14.2
Risk Likelihood



Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Table 14.3

Risk Consequences

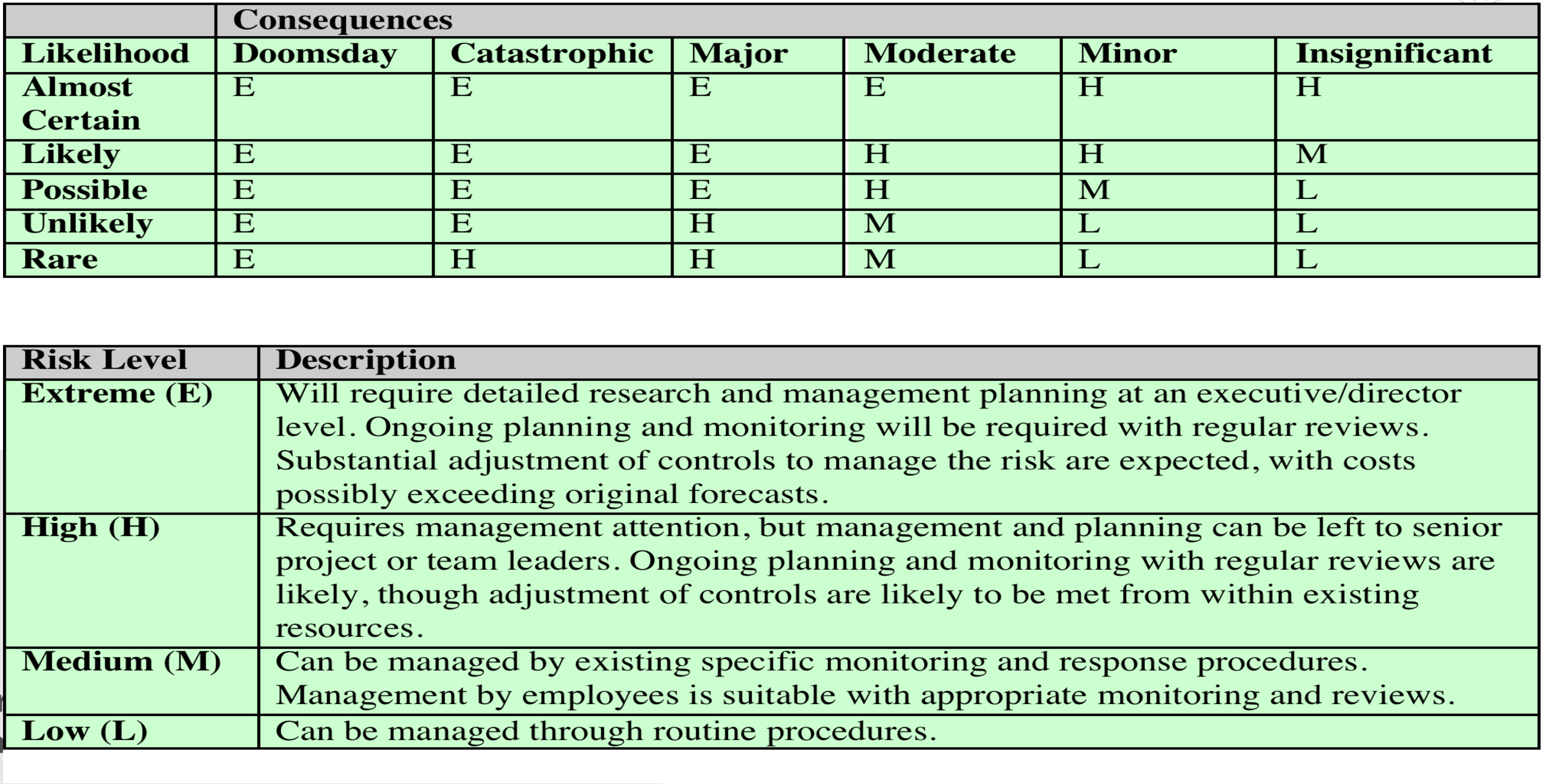


Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

(Table can be found on pages 476-477 in textbook)

Table 14.4

Risk Level Determination and Meaning



	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Table 14.5

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

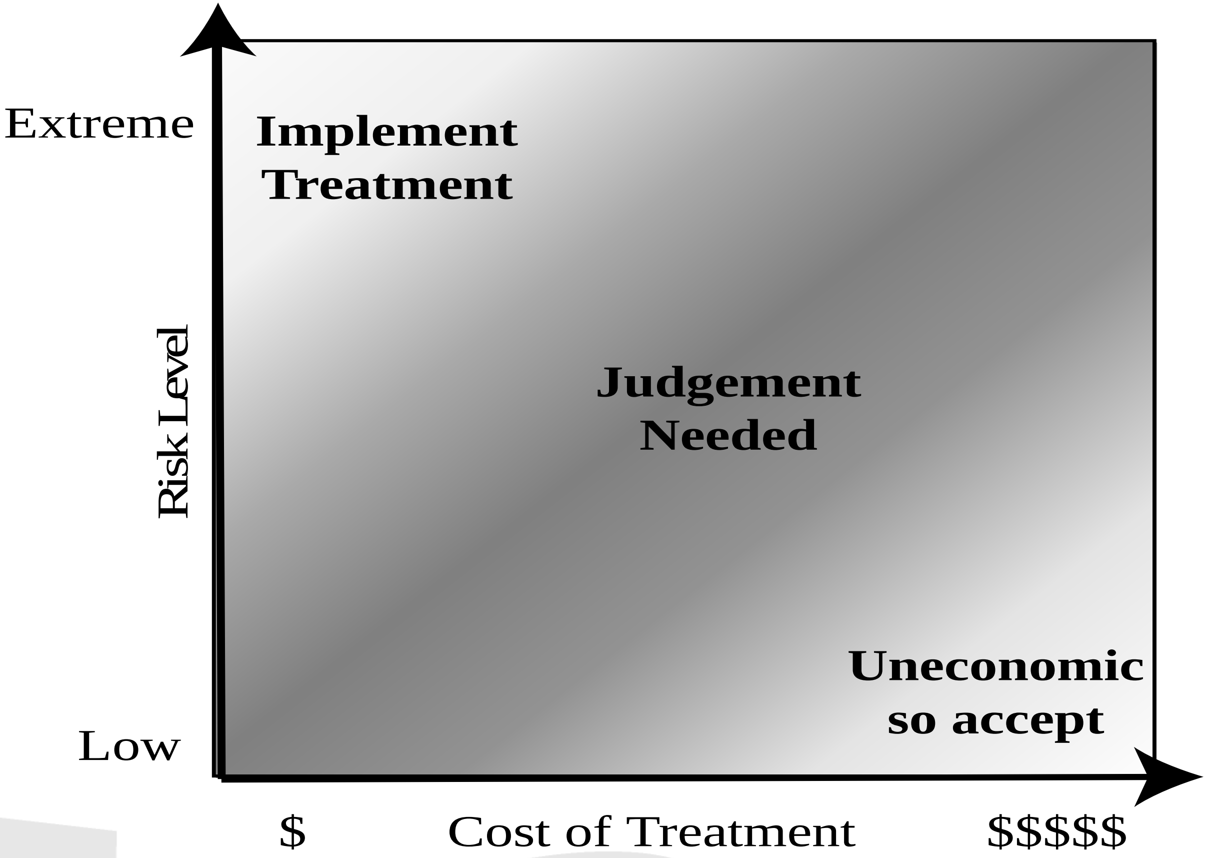
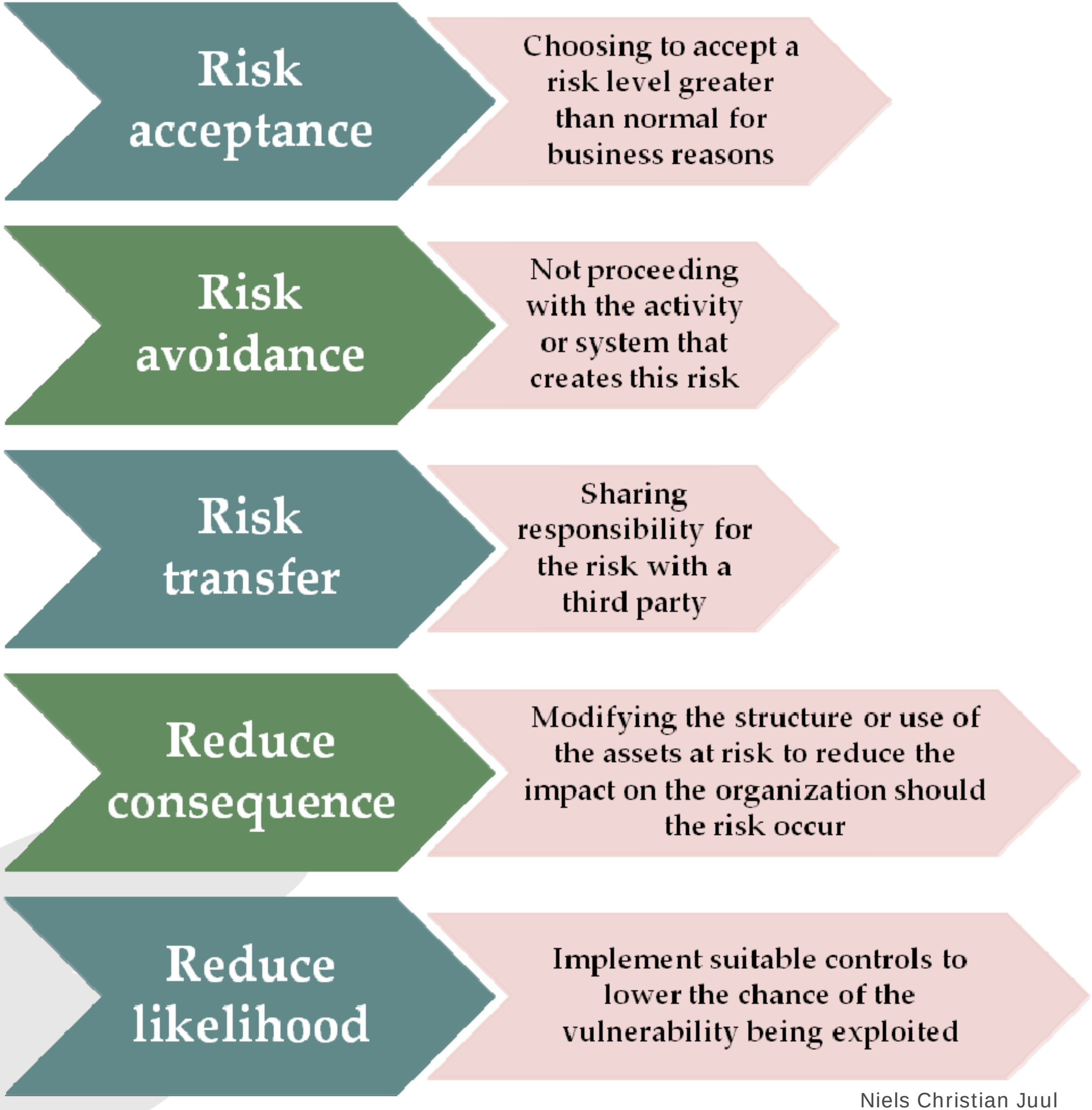


Figure 14.5 Judgment About Risk Treatment

Exercise: Roskilde case

1. Identify an important asset, that RUC needs to care about
2. What are the treats to that asset?
3. Which vulnerabilities?
4. **What are the likelihood of the risk?**
5. **What are the risk consequences and the cost of addressing the risk?**

Risk Treatment Alternatives



Risk acceptance: Choosing to accept a risk level greater than normal for business reasons

Risk avoidance: Not proceeding with the activity or system that creates this risk

Risk transfer: Sharing responsibility for the risk with a third party

Reduce consequence: Modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur

Reduce likelihood: Implement suitable controls to lower the chance of the vulnerability being exploited

Summary, chapter 14

- IT security management
- Organizational context and security policy
- Security risk assessment
  - Baseline approach
  - Informal approach
  - Detailed risk analysis
  - Combined approach
- Detailed security risk analysis
  - Context and system characterization
  - Identification of threats/risks/vulnerabilities
  - Analyze risks
  - Evaluate risks
  - Risk treatment

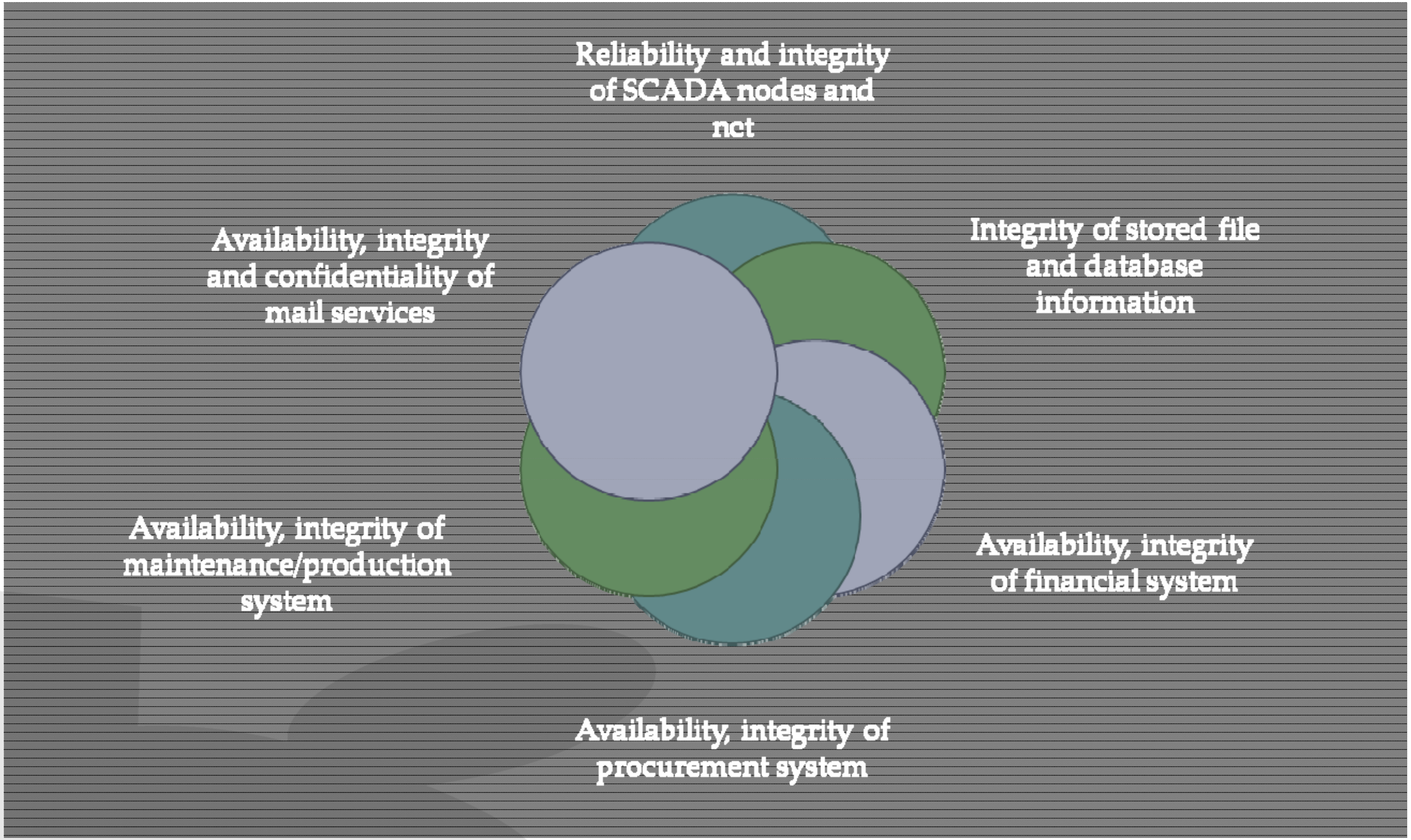
Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. Risk Assessment, Overview, Ch. 14.3
4. Detailed Risk Analysis, Ch. 14.4
5. **Case: Silver Mine, Ch. 14.5**
6. Security Controls, Ch. 15.2 (Monica)
7. Security Planning, Ch. 15.3
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

Case Study: Silver Star Mines

- Fictional operation of global mining company
- Large IT infrastructure
  - Both common and specific software
  - Some directly relates to health and safety
  - Formerly isolated systems now networked
- Decided on combined approach
- Mining industry less risky end of spectrum
- Subject to legal/regulatory requirements
- Management accepts moderate or low risk

Assets



Reliability and integrity of SCADA nodes and nct

Integrity of stored file and database information

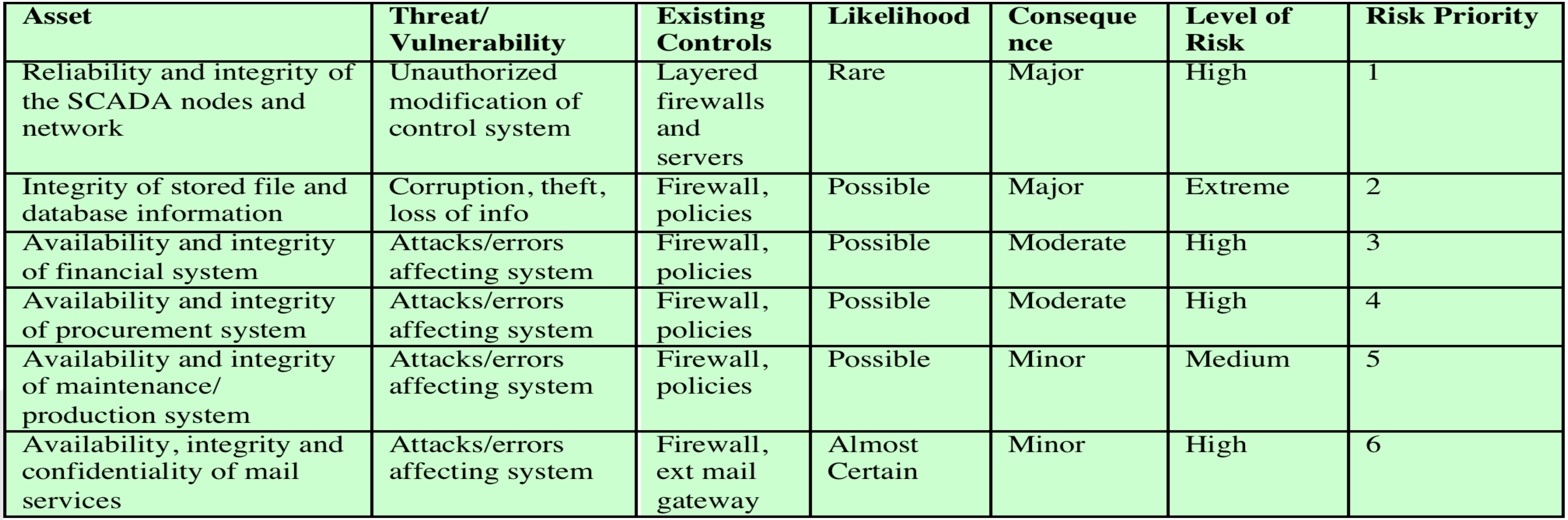
Availability, integrity of financial system

Availability, integrity of procurement system

Availability, integrity of maintenance/production system

Availability, integrity and confidentiality of mail services

Table 14.6
Silver Star Mines Risk Register



Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls and servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost Certain	Minor	High	6

(Table is on page 482 in textbook)

Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. Risk Assessment, Overview, Ch. 14.3
4. Detailed Risk Analysis, Ch. 14.4
5. Case: Silver Mine, Ch. 14.5
6. **Security Controls, Ch. 15.2 (Monica)**
7. Security Planning, Ch. 15.3
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

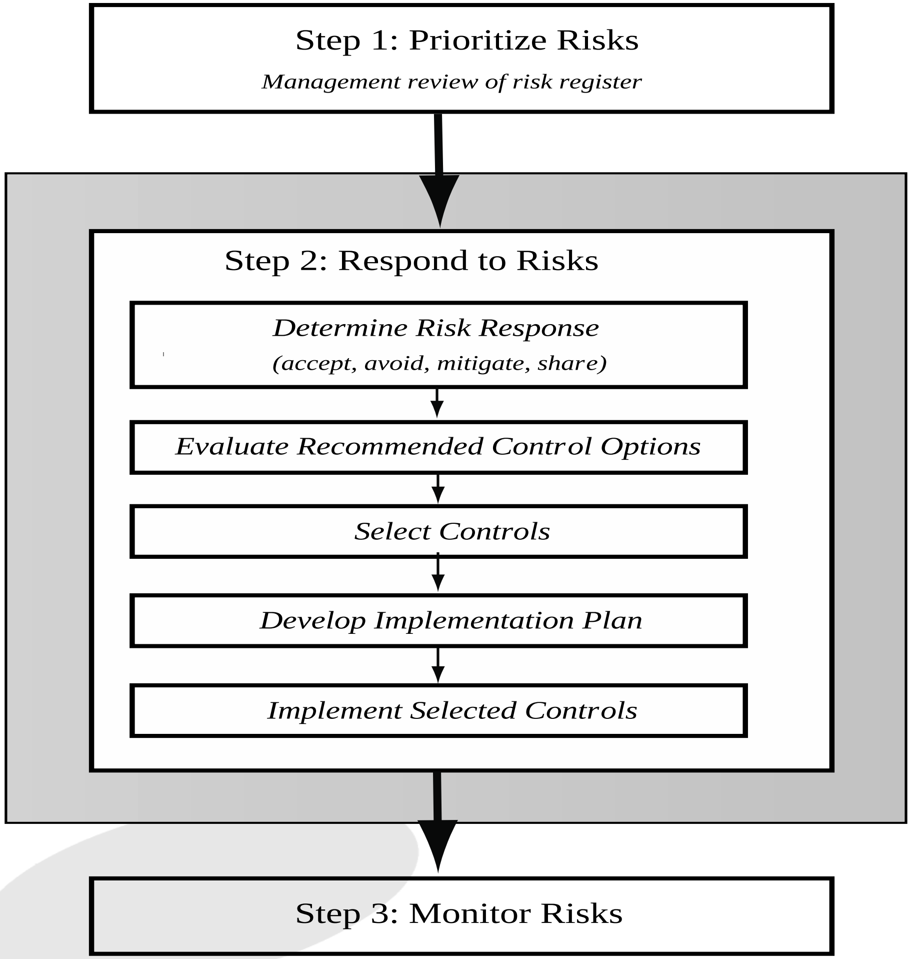

Step 1: Prioritize Risks
Management review of risk register
Step 2: Respond to Risks
Determine Risk Response
(accept, avoid, mitigate, share)
Evaluate Recommended Control Options
Select Controls
Develop Implementation Plan
Implement Selected Controls
Step 3: Monitor Risks

Figure 15.1 IT Security Management Controls and Implementation

Security Control

Control is defined as:

- “An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action.”

Control Classifications

- Management controls
  - Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
  - These controls refer to issues that management needs to address
- Operational controls
  - Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
  - These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
  - They are used to improve the security of a system or group of systems
- Technical controls
  - Involve the correct use of hardware and software security capabilities in systems
  - These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

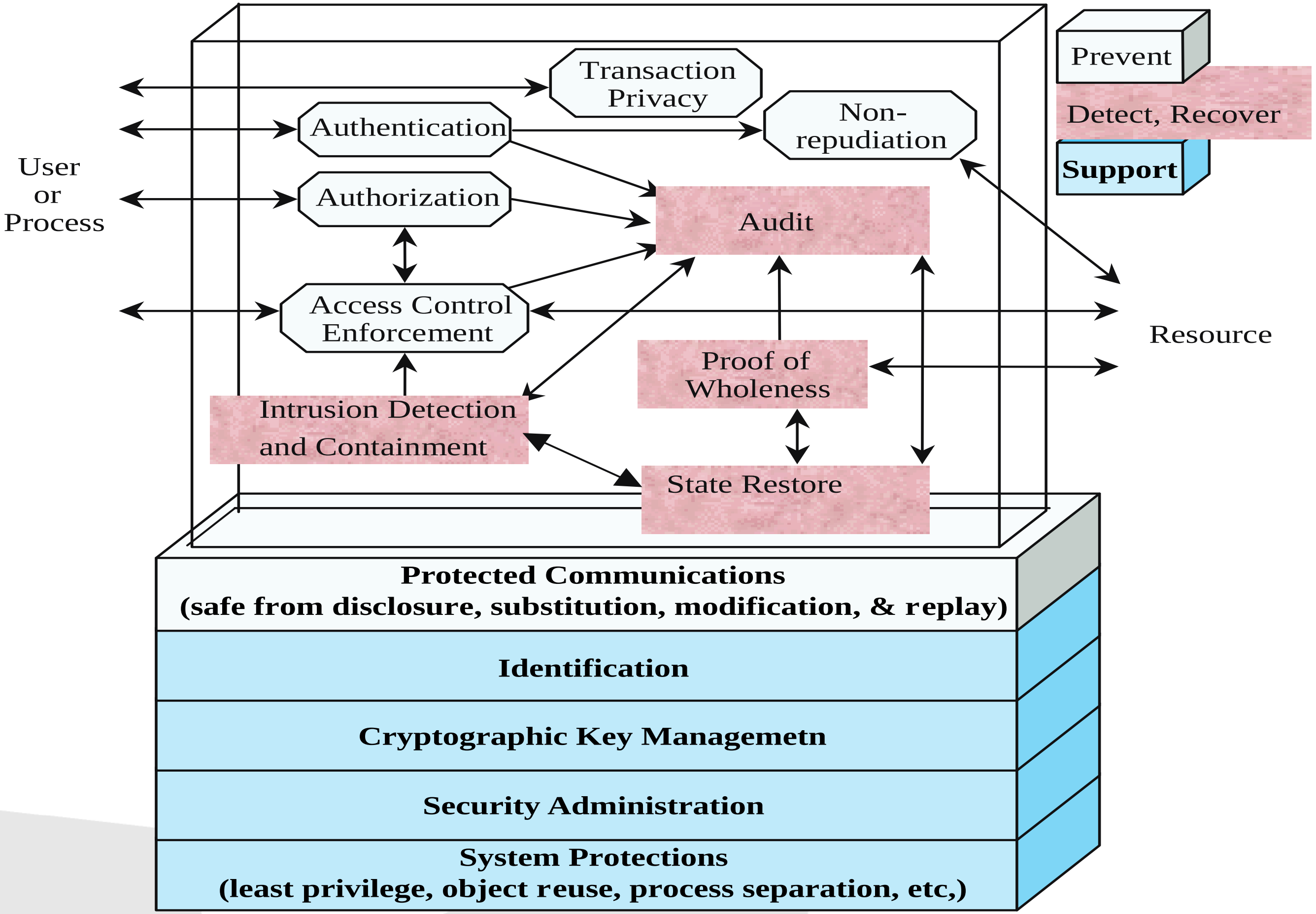

Transaction Privacy
Authentication
Non-repudiation
User or Process
Authorization
Audit
Access Control Enforcement
Resource
Proof of Wholeness
Intrusion Detection and Containment
State Restore
Prevent
Detect, Recover
Support
Protected Communications (safe from disclosure, substitution, modification, & replay)
Identification
Cryptographic Key Managemetn
Security Administration
System Protections (least privilege, object reuse, process separation, etc,)

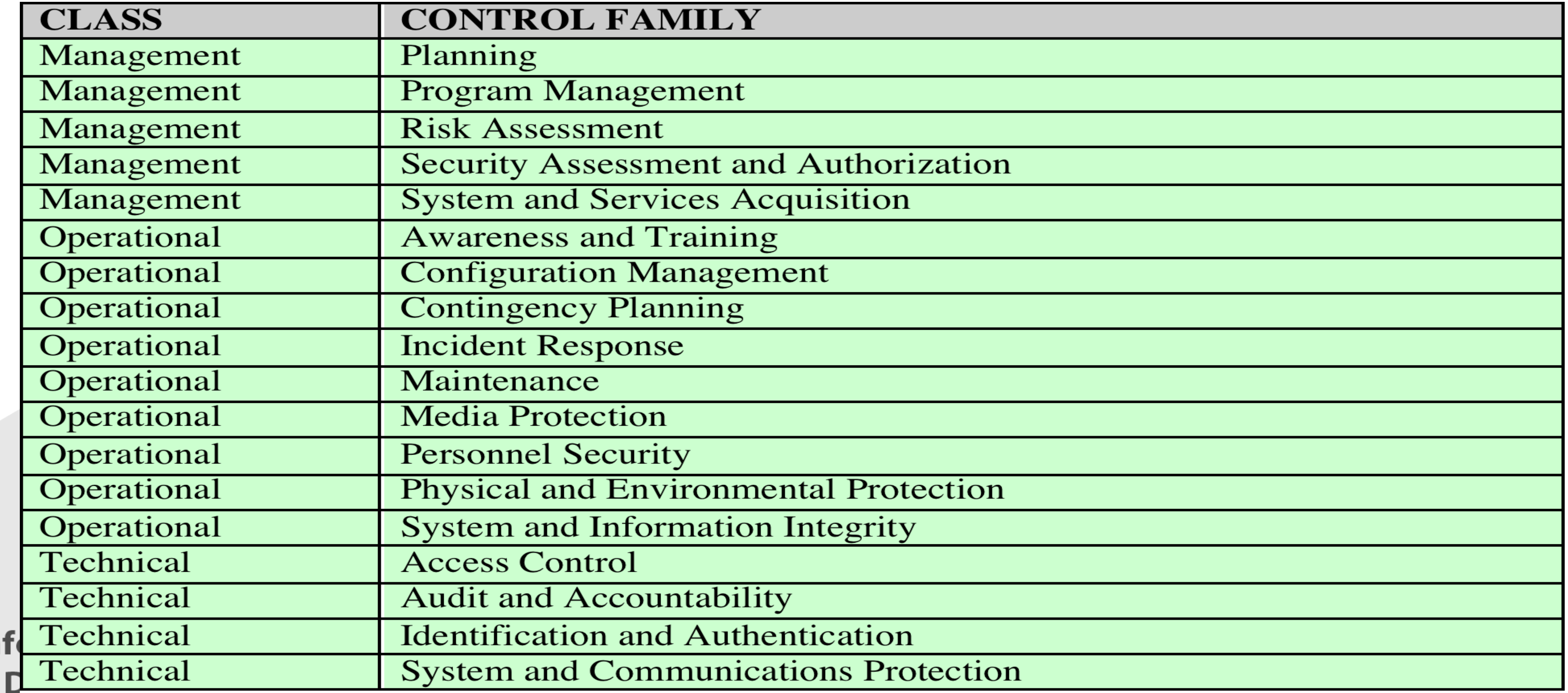
Figure 15.2 Technical Security Controls

Control Classes

- Each of the control classes may include the following:

- Supportive controls
  - Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls
- Preventative controls
  - Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability
- Detection and recovery controls
  - Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources

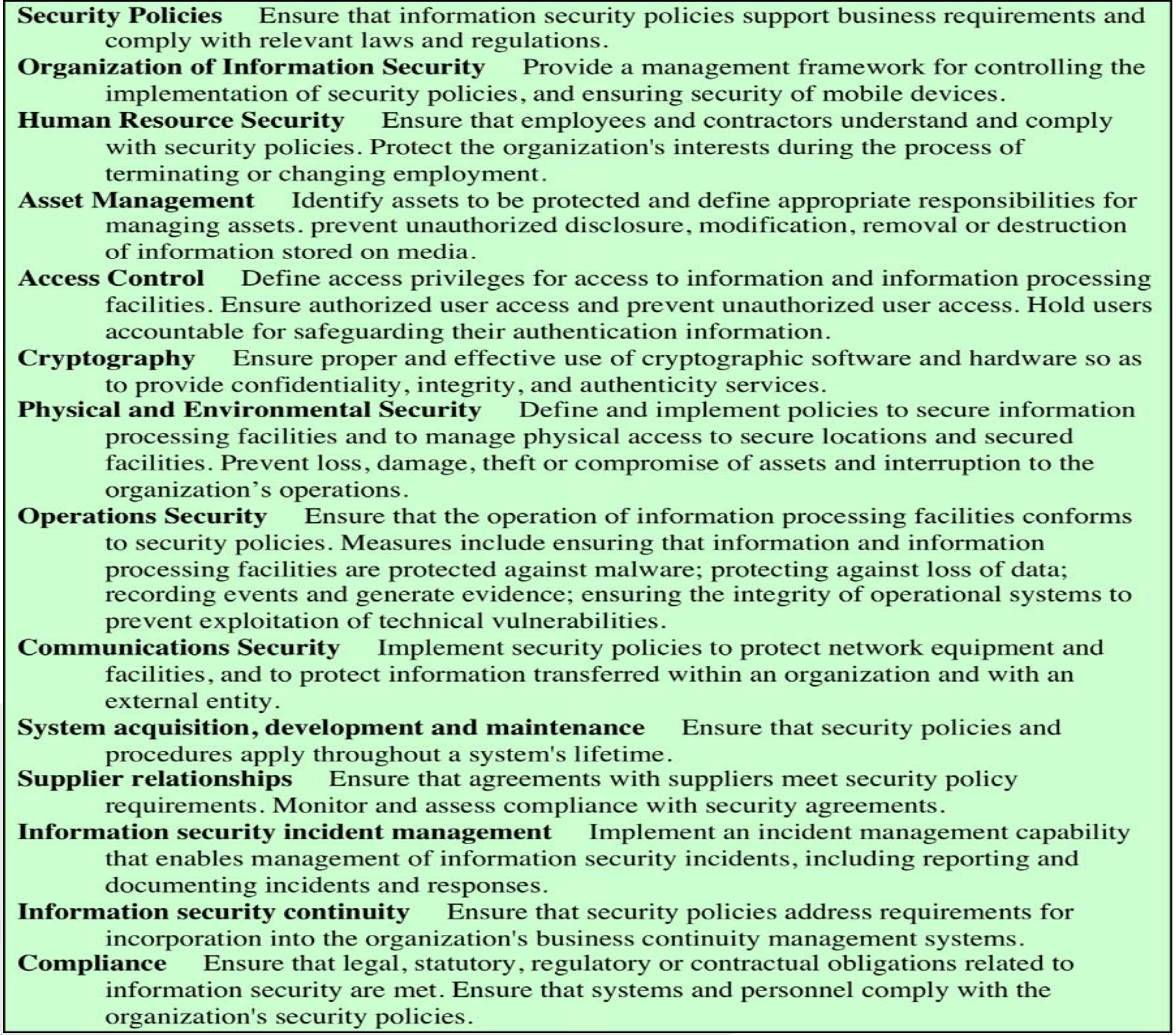
Table 15.1
NIST SP800-53 Security Controls



CLASS	CONTROL FAMILY
Management	Planning
Management	Program Management
Management	Risk Assessment
Management	Security Assessment and Authorization
Management	System and Services Acquisition
Operational	Awareness and Training
Operational	Configuration Management
Operational	Contingency Planning
Operational	Incident Response
Operational	Maintenance
Operational	Media Protection
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	System and Information Integrity
Technical	Access Control
Technical	Audit and Accountability
Technical	Identification and Authentication
Technical	System and Communications Protection

Table 15.2

27002 Security Controls



Security Policies Ensure that information security policies support business requirements and comply with relevant laws and regulations.

Organization of Information Security Provide a management framework for controlling the implementation of security policies, and ensuring security of mobile devices.

Human Resource Security Ensure that employees and contractors understand and comply with security policies. Protect the organization's interests during the process of terminating or changing employment.

Asset Management Identify assets to be protected and define appropriate responsibilities for managing assets. prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

Access Control Define access privileges for access to information and information processing facilities. Ensure authorized user access and prevent unauthorized user access. Hold users accountable for safeguarding their authentication information.

Cryptography Ensure proper and effective use of cryptographic software and hardware so as to provide confidentiality, integrity, and authenticity services.

Physical and Environmental Security Define and implement policies to secure information processing facilities and to manage physical access to secure locations and secured facilities. Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Operations Security Ensure that the operation of information processing facilities conforms to security policies. Measures include ensuring that information and information processing facilities are protected against malware; protecting against loss of data; recording events and generate evidence; ensuring the integrity of operational systems to prevent exploitation of technical vulnerabilities.

Communications Security Implement security policies to protect network equipment and facilities, and to protect information transferred within an organization and with an external entity.

System acquisition, development and maintenance Ensure that security policies and procedures apply throughout a system's lifetime.

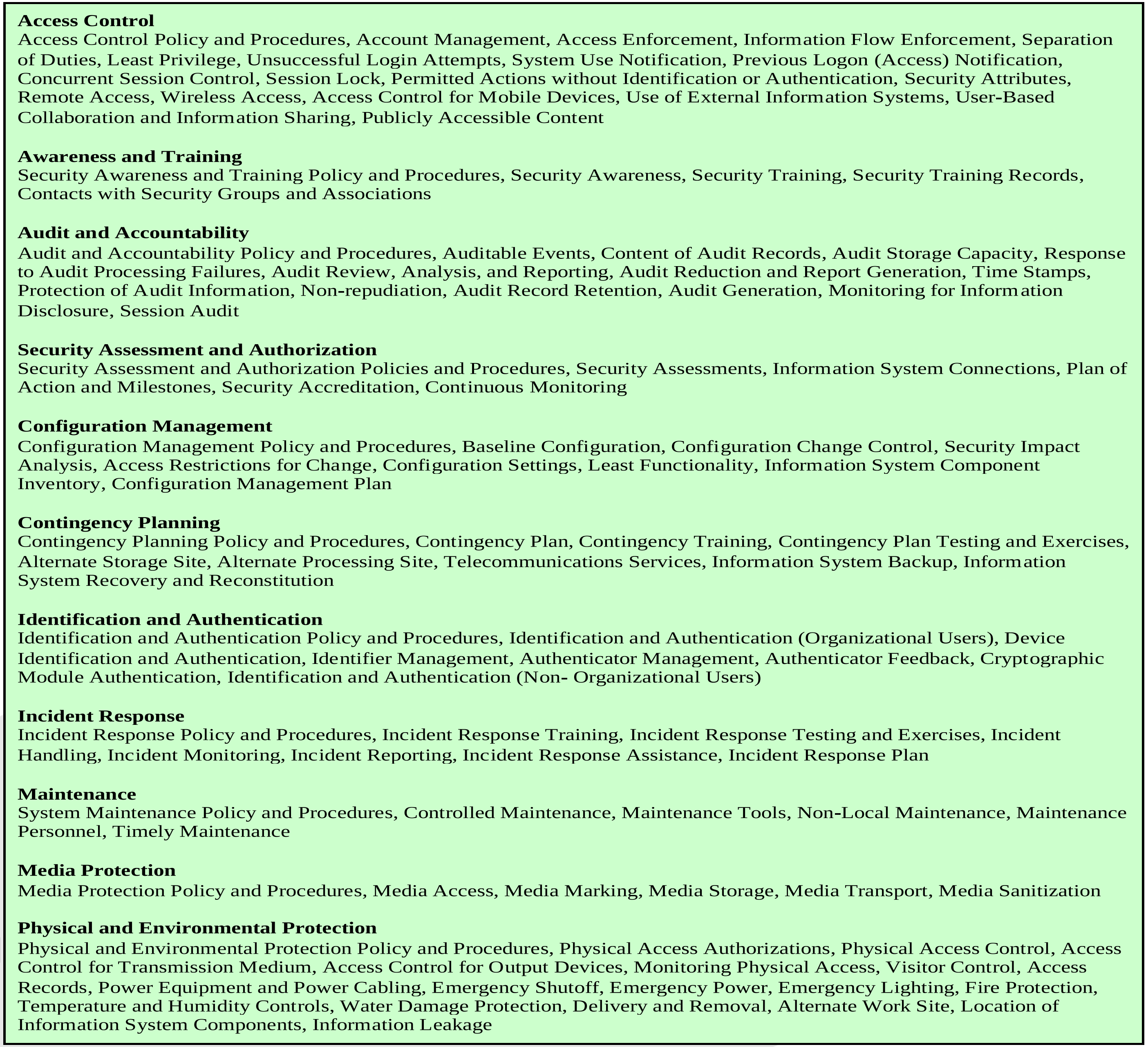
Supplier relationships Ensure that agreements with suppliers meet security policy requirements. Monitor and assess compliance with security agreements.

Information security incident management Implement an incident management capability that enables management of information security incidents, including reporting and documenting incidents and responses.

Information security continuity Ensure that security policies address requirements for incorporation into the organization's business continuity management systems.

Compliance Ensure that legal, statutory, regulatory or contractual obligations related to information security are met. Ensure that systems and personnel comply with the organization's security policies.

(Table can be found on page 493 in the textbook.)



Access Control
Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Previous Logon (Access) Notification, Concurrent Session Control, Session Lock, Permitted Actions without Identification or Authentication, Security Attributes, Remote Access, Wireless Access, Access Control for Mobile Devices, Use of External Information Systems, User-Based Collaboration and Information Sharing, Publicly Accessible Content

Awareness and Training
Security Awareness and Training Policy and Procedures, Security Awareness, Security Training, Security Training Records, Contacts with Security Groups and Associations

Audit and Accountability
Audit and Accountability Policy and Procedures, Auditable Events, Content of Audit Records, Audit Storage Capacity, Response to Audit Processing Failures, Audit Review, Analysis, and Reporting, Audit Reduction and Report Generation, Time Stamps, Protection of Audit Information, Non-repudiation, Audit Record Retention, Audit Generation, Monitoring for Information Disclosure, Session Audit

Security Assessment and Authorization
Security Assessment and Authorization Policies and Procedures, Security Assessments, Information System Connections, Plan of Action and Milestones, Security Accreditation, Continuous Monitoring

Configuration Management
Configuration Management Policy and Procedures, Baseline Configuration, Configuration Change Control, Security Impact Analysis, Access Restrictions for Change, Configuration Settings, Least Functionality, Information System Component Inventory, Configuration Management Plan

Contingency Planning
Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing and Exercises, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution

Identification and Authentication
Identification and Authentication Policy and Procedures, Identification and Authentication (Organizational Users), Device Identification and Authentication, Identifier Management, Authenticator Management, Authenticator Feedback, Cryptographic Module Authentication, Identification and Authentication (Non- Organizational Users)

Incident Response
Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing and Exercises, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance, Incident Response Plan

Maintenance
System Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Non-Local Maintenance, Maintenance Personnel, Timely Maintenance

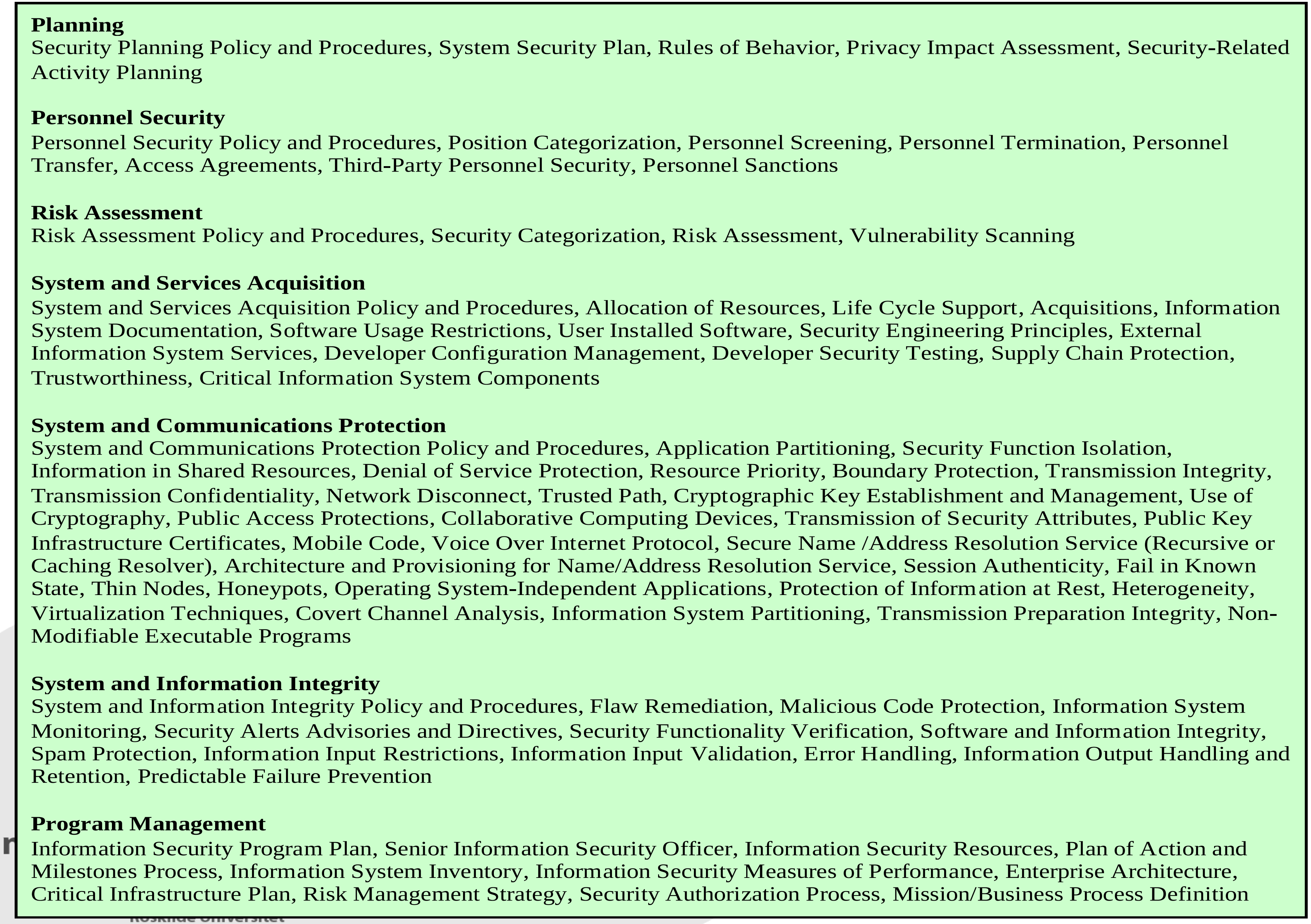
Media Protection
Media Protection Policy and Procedures, Media Access, Media Marking, Media Storage, Media Transport, Media Sanitization

Physical and Environmental Protection
Physical and Environmental Protection Policy and Procedures, Physical Access Authorizations, Physical Access Control, Access Control for Transmission Medium, Access Control for Output Devices, Monitoring Physical Access, Visitor Control, Access Records, Power Equipment and Power Cabling, Emergency Shutoff, Emergency Power, Emergency Lighting, Fire Protection, Temperature and Humidity Controls, Water Damage Protection, Delivery and Removal, Alternate Work Site, Location of Information System Components, Information Leakage

Table 15.3

Detailed NIST SP800-53 Security Controls

(Table is on page 494-495 in the textbook)



Planning
Security Planning Policy and Procedures, System Security Plan, Rules of Behavior, Privacy Impact Assessment, Security-Related Activity Planning

Personnel Security
Personnel Security Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Third-Party Personnel Security, Personnel Sanctions

Risk Assessment
Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Vulnerability Scanning

System and Services Acquisition
System and Services Acquisition Policy and Procedures, Allocation of Resources, Life Cycle Support, Acquisitions, Information System Documentation, Software Usage Restrictions, User Installed Software, Security Engineering Principles, External Information System Services, Developer Configuration Management, Developer Security Testing, Supply Chain Protection, Trustworthiness, Critical Information System Components

System and Communications Protection
System and Communications Protection Policy and Procedures, Application Partitioning, Security Function Isolation, Information in Shared Resources, Denial of Service Protection, Resource Priority, Boundary Protection, Transmission Integrity, Transmission Confidentiality, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Cryptography, Public Access Protections, Collaborative Computing Devices, Transmission of Security Attributes, Public Key Infrastructure Certificates, Mobile Code, Voice Over Internet Protocol, Secure Name /Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity, Fail in Known State, Thin Nodes, Honeypots, Operating System-Independent Applications, Protection of Information at Rest, Heterogeneity, Virtualization Techniques, Covert Channel Analysis, Information System Partitioning, Transmission Preparation Integrity, Non-Modifiable Executable Programs

System and Information Integrity
System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, Information System Monitoring, Security Alerts Advisories and Directives, Security Functionality Verification, Software and Information Integrity, Spam Protection, Information Input Restrictions, Information Input Validation, Error Handling, Information Output Handling and Retention, Predictable Failure Prevention

Program Management
Information Security Program Plan, Senior Information Security Officer, Information Security Resources, Plan of Action and Milestones Process, Information System Inventory, Information Security Measures of Performance, Enterprise Architecture, Critical Infrastructure Plan, Risk Management Strategy, Security Authorization Process, Mission/Business Process Definition

Table 15.3

Continued

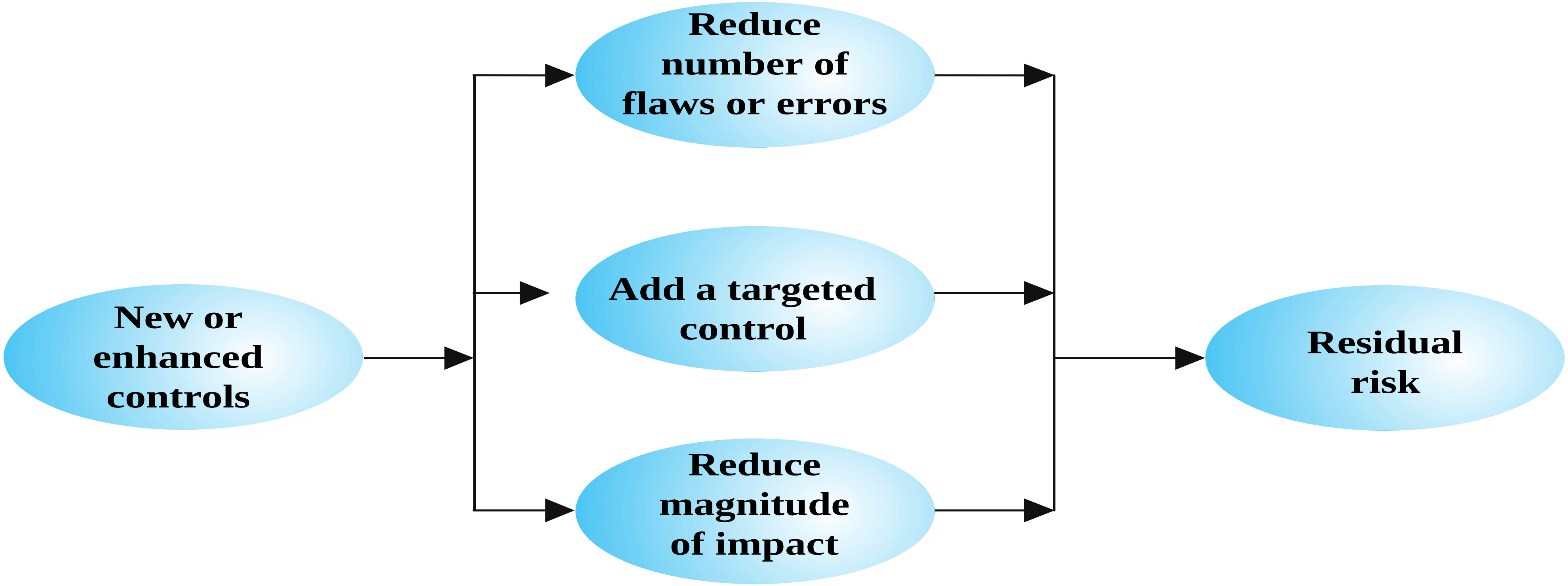
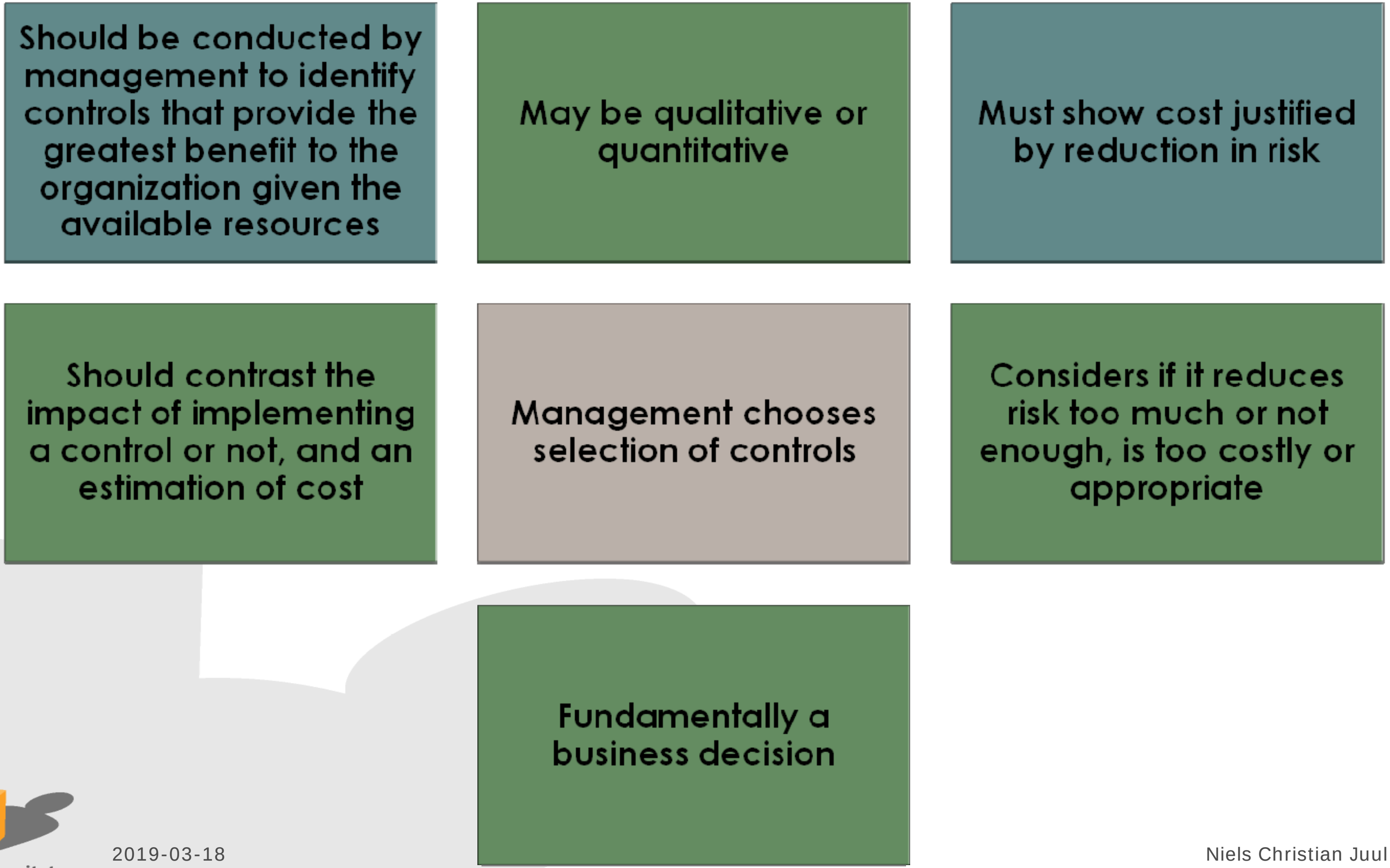


Figure 15.3 Residual Risk

Cost-Benefit Analysis



Should be conducted by management to identify controls that provide the greatest benefit to the organization given the available resources

May be qualitative or quantitative

Must show cost justified by reduction in risk

Should contrast the impact of implementing a control or not, and an estimation of cost

Management chooses selection of controls

Considers if it reduces risk too much or not enough, is too costly or appropriate

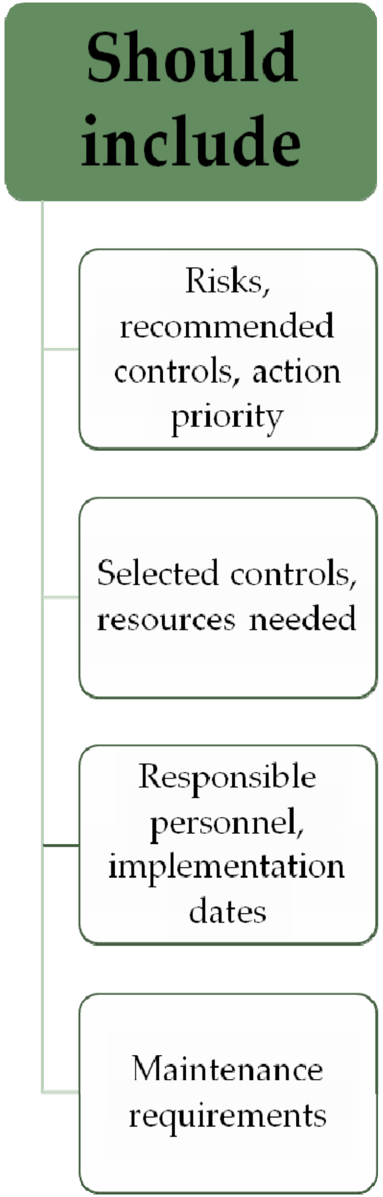
Fundamentally a business decision

Agenda

1. Intro
2. Organizational IT Security Policy, Ch. 14.1-2
3. Risk Assessment, Overview, Ch. 14.3
4. Detailed Risk Analysis, Ch. 14.4
5. Case: Silver Mine, Ch. 14.5
6. Security Controls, Ch. 15.2 (Monica)
7. **Security Planning, Ch. 15.3**
8. Implementing Controls and Risk Management, Ch. 15.4-5
9. Silver Mine Case, Ch. 15.6

IT Security Plan

- Provides details of:
  - What will be done
  - What resources are needed
  - Who is responsible
- Goal is to detail the actions needed to improve the identified deficiencies in the risk profile



Should include

Risks, recommended controls, action priority

Selected controls, resources needed

Responsible personnel, implementation dates

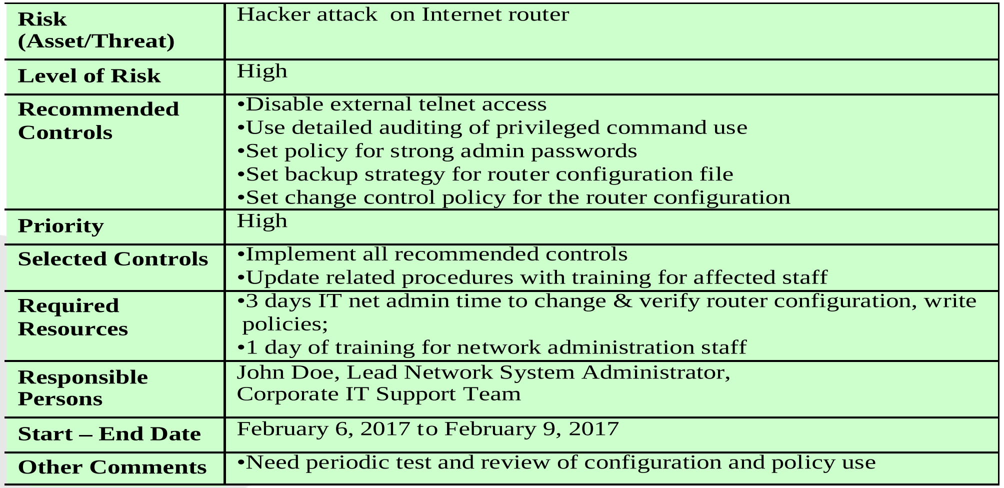
Maintenance requirements

Table 15.4 Implementation Plan - example

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Implement all recommended controls •Update related procedures with training for affected staff
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	February 6, 2017 to February 9, 2017
Other Comments	•Need periodic test and review of configuration and policy use

Exercise: Roskilde case

1. Identify an important asset, that RUC needs to care about
2. What are the treats to that asset?
3. Which vulnerabilities?
4. What are the likelihood of the risk?
5. What are the risk consequences and the cost of addressing the risk?
6. **Make an Implementation Plan (Table 15.4) for this risk**



Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Implement all recommended controls •Update related procedures with training for affected staff
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	February 6, 2017 to February 9, 2017
Other Comments	•Need periodic test and review of configuration and policy use

Learning outcome

Be able to

- manage information security in an organization
- conduct a thorough risk analysis wrt organizational information security
- select relevant security controls
- create an security implementation plan

Exam themes/questions:

- What is Security Policy and how should it be managed?
- How to conduct a Detailed Security Risk Assessment?
- How to make a Security Implementation Plan?

IT-security

Next week:

Course book

- Chapter 15.4-6(from today)
- Selected parts of Chapter 16, 17, 18

Student presentations, eg.

- 17.3 on e-mail policy (compare to RUC)