2019-03-18

IT Security #7

Implementing Security Controls
Physical and Human Security & Audit

Niels Christian Juul

Theme C (iii) on Management issues

Informatik
Datalogi
Roskilde Universitet

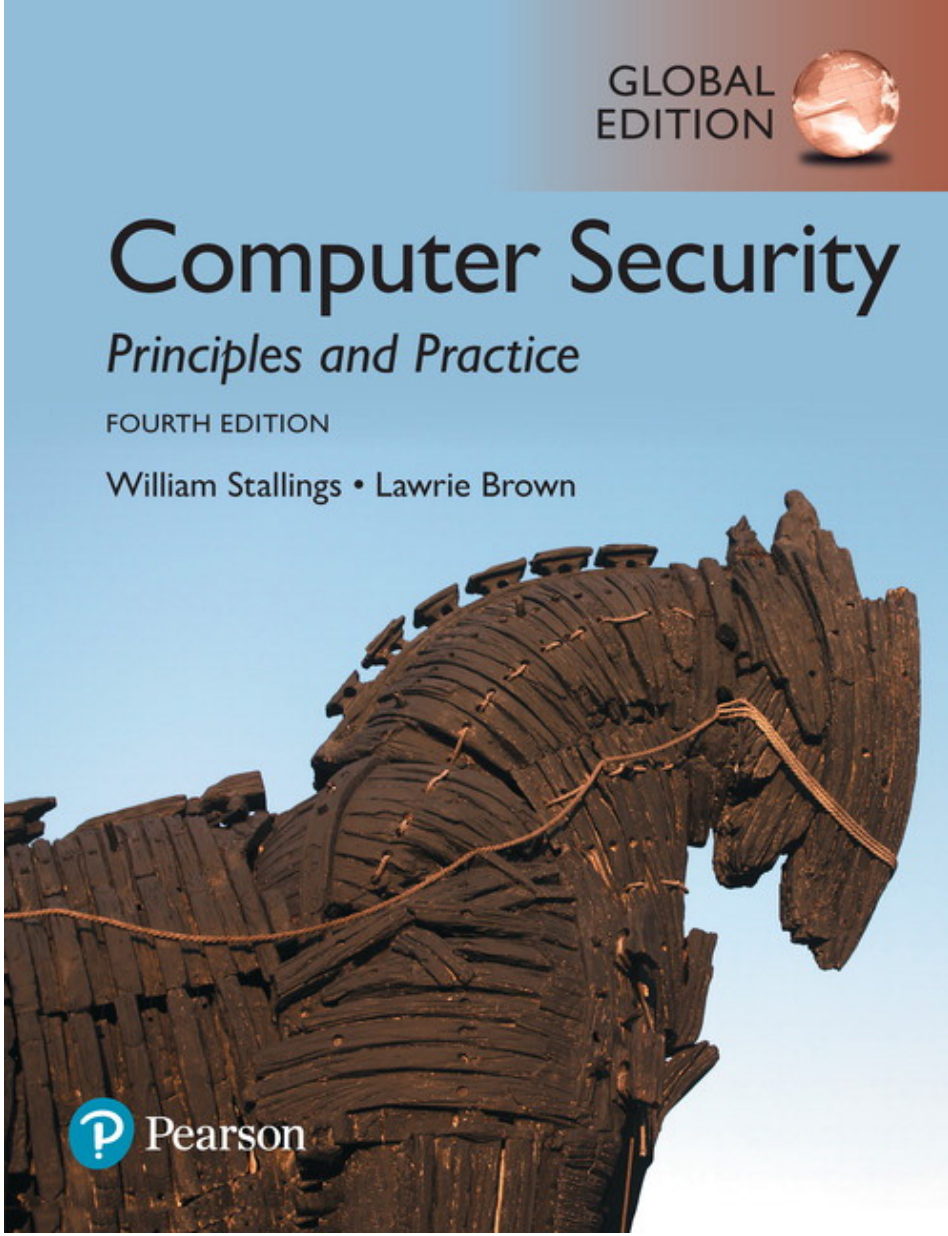
Roskilde Universitet
Niels Christian Juul
Hus 08.2-071
Universitetsvej 1
4000 Roskilde
ncjuul@ruc.dk

IT-security

Course book
(selected parts of)

- Chapter 15 (15.4-5)
- Chapter 16 (16.1-16.4)
- Chapter 17 (17.1-3)
- Chapter 18 (18.1)

today



Learning outcome

Be able to

- create an security implementation plan
- establish a plan for site and physical security
- manage the human elements of security
- evaluate, establish and manage an Internet security policy for employees

Exam themes/questions:

- How to make a Security Implementation Plan?
- Physical and Human security threats and how to cope with them
- Internet/E-mail security policy - from theory to examples

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Security Plan Implementation

IT security plan documents:

- What needs to be done for each selected control
- Personnel responsible
- Resources and time frame

Identified personnel:

- Implement new or enhanced controls
- May need system configuration changes, upgrades or new system installation
- May also involve development of new or extended procedures
- Need to be encouraged and monitored by management

When implementation is completed management authorizes the system for operational use

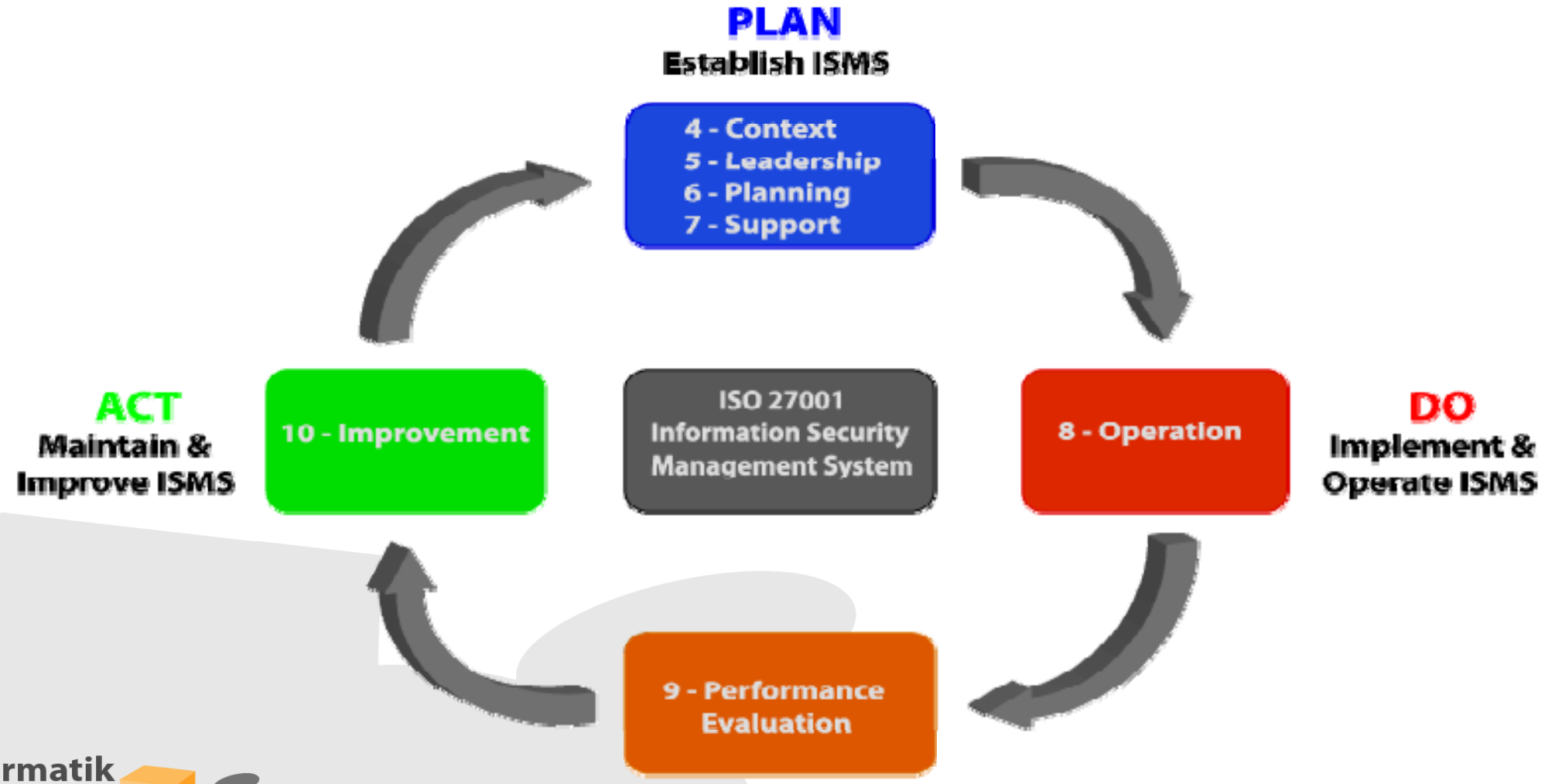
Implementation Follow-Up

- Security management is a cyclic process
  - Constantly repeated to respond to changes in the IT systems and the risk environment
- Need to monitor implemented controls
- Evaluate changes for security implications
- Otherwise increase chance of security breach

This follow-up stage includes a number of aspects:

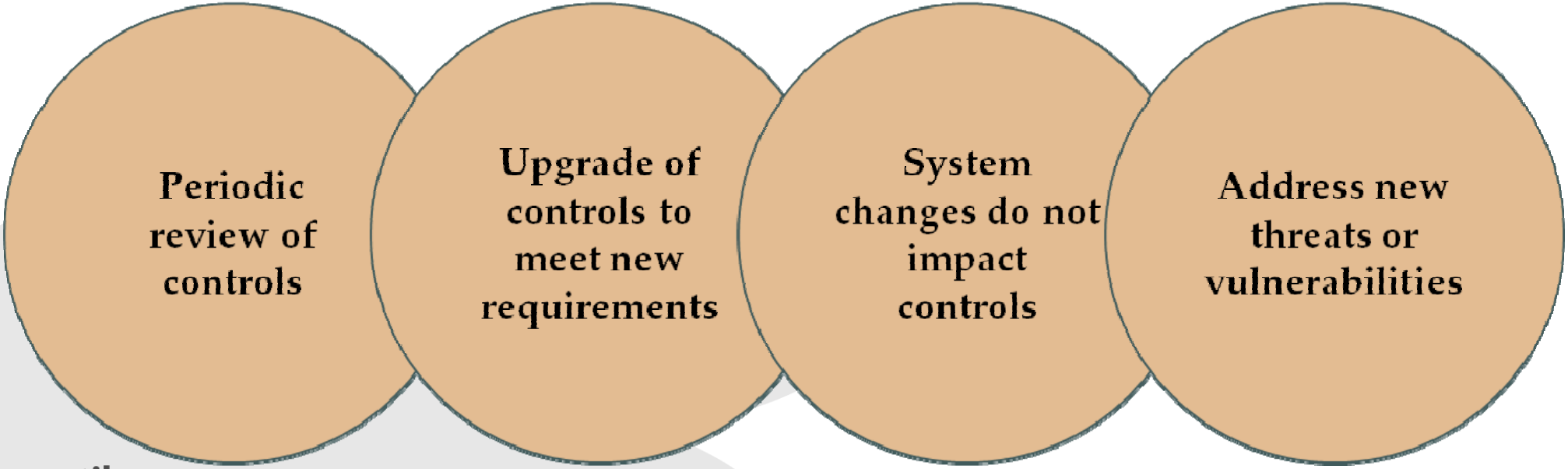
- Maintenance of security controls
- Security compliance checking
- Change and configuration management
- Incident handling

Information Security Management System



Maintenance

- Need continued maintenance and monitoring of implemented controls to ensure continued correct functioning and appropriateness
- Goal is to ensure controls perform as intended

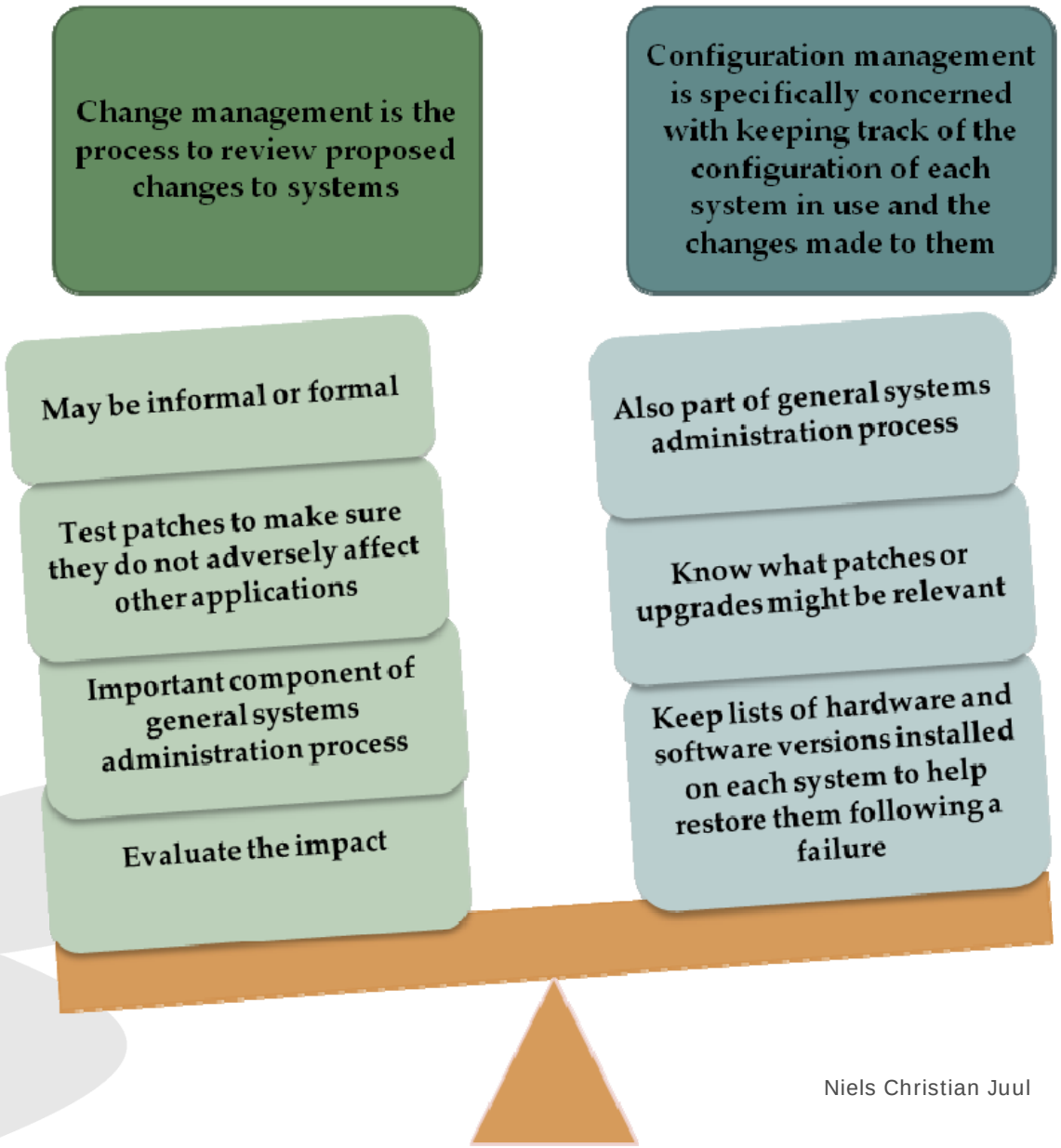


Tasks

Security Compliance

- Audit process to review security processes
- Goal is to verify compliance with security plan
- Use internal or external personnel
- Usually based on use of checklists which verify:
  - Suitable policies and plans were created
  - Suitable selection of controls were chosen
  - That they are maintained and used correctly
- Often as part of wider general audit

Change and Configuration Management



Summary, Chapter 15

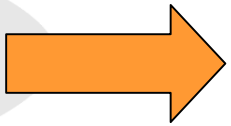
- Implementation of controls
  - Implementation of security plan
  - Security awareness and training
- Monitoring risks
  - Maintenance
  - Security compliance
  - Change and configuration management
  - Incident handling

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. **Silver Star Mine Case, Ch 15.6**
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Case Study: Silver Star Mines

- Given risk assessment, the next stage is to identify possible controls
- Based on assessment it is clear many categories are not in use
- General issue of systems not being patched or upgraded
- Need contingency plans
- SCADA: add intrusion detection system
- Info integrity: better centralize storage
- Email: provide backup system



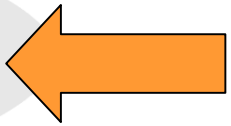
Case: Systems not updated and patched on regular basis!

Such controls include:

- Configuration management policy and procedures
- Baseline configuration
- System maintenance policy and procedures
- Periodic maintenance
- Flaw remediation
- Malicious code protection
- Spam and spyware protection

Developing contingency plans:

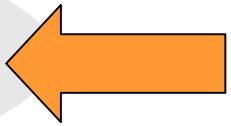
- Audit monitoring, analysis, and reporting
- Audit reduction and report generation
- Contingency planning policy and procedures
- Incident response policy and procedures
- Information system backup
- Information system recovery and reconstitution



SCADA

The top-priority risk relates to the reliability and integrity of the Supervisory Control and Data Acquisition (SCADA) nodes and network.

- Limit update options
- SCADA-Network isolation (firewalls?, IDS?)



Silver Star Mines: Implementation Plan

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls
All risks (generally applicable)		1. Configuration and periodic maintenance policy for servers 2. Malicious code (SPAM, spyware) prevention 3. Audit monitoring, analysis, reduction, and reporting on servers 4. Contingency planning and incident response policies and procedures 5. System backup and recovery procedures	1	1. 2. 3. 4. 5.
Reliability and integrity of SCADA nodes and network	High	1. Intrusion detection and response system	2	1.
Integrity of stored file and database information	Extreme	1. Audit of critical documents 2. Document creation and storage policy 3. User security education and training	3	1. 2. 3.
Availability and integrity of Financial, Procurement, and Maintenance/ Production Systems	High	-	-	(general controls)
Availability, integrity and confidentiality of e-mail	High	1. Contingency planning – backup e-mail service	4	1.

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. **Physical Security Overview & Threats , Ch. 16.1-2**
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Physical and Infrastructure Security

Logical security

- Protects computer-based data from software-based and communication-based threats

Physical security

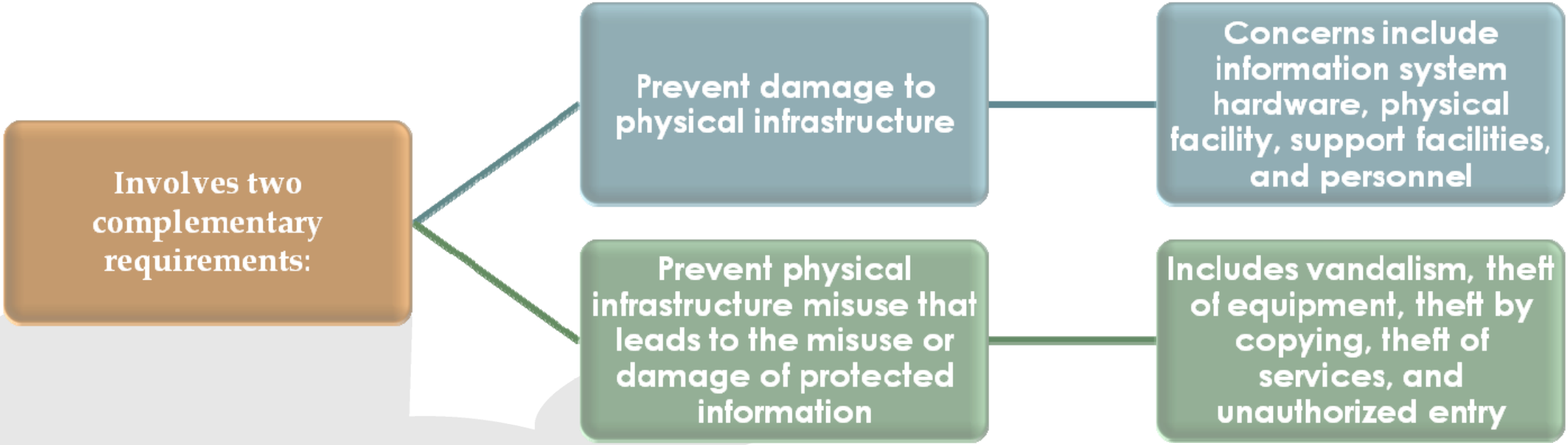
- Also called infrastructure security
- Protects the information systems that contain data and the people who use, operate, and maintain the systems
- Must prevent any type of physical access or intrusion that can compromise logical security

Premises security

- Also known as corporate or facilities security
- Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations
- Provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards

Physical Security – Overview

- Protect physical assets that support the storage and processing of information



Physical Security Threats

Physical situations and occurrences that threaten information systems:

- Environmental threats
- Technical threats
- Human-caused threats

Table 16.1 Characteristics of Natural Disasters

	Warning	Evacuation	Duration
Tornado	Advance warning of potential; not site specific	Remain at site	Brief but intense
Hurricane	Significant advance warning	May require evacuation	Hours to a few days
Earthquake	No warning	May be unable to evacuate	Brief duration; threat of continued aftershocks
Ice storm/ blizzard	Several days warning generally expected	May be unable to evacuate	May last several days
Lightning	Sensors may provide minutes of warning	May require evacuation	Brief but may recur
Flood	Several days warning generally expected	May be unable to evacuate	Site may be isolated for extended period

Source: ComputerSite Engineering, Inc.

Water Damage

Primary danger is an electrical short

A pipe may burst from a fault in the line or from freezing

Sprinkler systems set off accidentally

Floodwater leaving a muddy residue and suspended material in the water

Due diligence should be performed to ensure that water from as far as two floors above will not create a hazard

Chemical, Radiological, and Biological Hazards

- Pose a threat from intentional attack and from accidental discharge
- Discharges can be introduced through the ventilation system or open windows, and in the case of radiation, through perimeter walls
- Flooding can also introduce biological or chemical contaminants

Dust and Infestation

Dust

- Often overlooked
- Rotating storage media and computer fans are the most vulnerable to damage
- Can also block ventilation
- Influxes can result from a number of things:
  - Controlled explosion of a nearby building
  - Windstorm carrying debris
  - Construction or maintenance work in the building

Infestation

- Covers a broad range of living organisms:
  - High-humidity conditions can cause mold and mildew
  - Insects, particularly those that attack wood and paper

Technical Threats

- Electrical power is essential to run equipment
- Power utility problems:
  - Under-voltage - dips/brownouts/outages, interrupts service
  - Over-voltage - surges/faults/lightening, can destroy chips
  - Noise - on power lines, may interfere with device operation

Electromagnetic interference (EMI)

- Noise along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations
- Noise can be transmitted through space as well as through power lines
- Can cause intermittent problems with computers

Human-Caused Threats

- Less predictable, designed to overcome prevention measures, harder to deal with

Include:

- Unauthorized physical access
  - Information assets are generally located in restricted areas
  - Can lead to other threats such as theft, vandalism or misuse
- Theft of equipment/data
  - Eavesdropping and wiretapping fall into this category
  - Insider or an outsider who has gained unauthorized access
- Vandalism of equipment/data
- Misuse of resources

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. **Physical Security Counter-measures, Ch. 16.3-4**
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Physical Security Prevention and Mitigation Measures

- One prevention measure is the use of cloud computing
- Inappropriate temperature and humidity
  - Environmental control equipment, power supply
- Fire and smoke
  - Alarms, preventative measures, fire mitigation
  - Smoke detectors, no smoking
- Water
  - Manage lines, equipment location, cutoff sensors
- Other threats
  - Appropriate technical counter-measures, limit dust entry, pest control

Fire Counter-measures:

1. Choice of site to minimize likelihood of disaster. The IS area should be chosen to minimize fire, water, and smoke hazards from adjoining areas.
2. Air conditioning and other ducts designed so as not to spread fire. There are standard guidelines and specifications for such designs.
3. Positioning of equipment to minimize damage.
4. Good housekeeping. Records and flammables must not be stored in the IS area. Tidy installation if IS equipment is crucial.
5. Hand-operated fire extinguishers readily available, clearly marked, and regularly tested.
6. Automatic fire extinguishers installed. Installation should be such that the extinguishers are unlikely to cause damage to equipment or danger to personnel.

Fire Counter-measures (cont.):

7. Fire detectors. The detectors sound alarms inside the IS room and with external authorities, and start automatic fire extinguishers after a delay to permit human intervention.
8. Equipment power-off switch. This switch must be clearly marked and unobstructed. All personnel must be familiar with power-off procedures.
9. Emergency procedures posted.
10. Personnel safety. Safety must be considered in designing the building layout and emergency procedures.
11. Important records stored in fireproof cabinets or vaults.
12. Records needed for file reconstruction stored off the premises.
13. Up-to-date duplicate of all programs stored off the premises.
14. Contingency plan for use of equipment elsewhere should the computers be destroyed.
15. Insurance company and local fire department should inspect the facility.

Mitigation Measures for Technical Threats

- **Uninterruptible Power Supply (UPS)** should be employed for each piece of critical equipment
- **Emergency Power Source** for longer blackouts for critical equipment, eg. a generator
- **Electrical filters and shielding** can be used to deal with electromagnetic interference

Mitigation Measures to Human-Caused Physical Threats

Physical access control

- Restrict building access
- Controlled areas patrolled or guarded
- Locks or screening measures at entry points
- Equip movable resources with a tracking device
- Power switch controlled by a security device
- Intruder sensors and alarms
- Surveillance systems that provide recording and real-time remote viewing

Recovery from Physical Security Breaches

Most essential element of recovery is redundancy

- Provides for recovery from loss of data
- Ideally all important data should be available off-site and updated as often as feasible
- Can use batch encrypted remote backup
- For critical situations a remote hot-site that is ready to take over operation instantly can be created

Physical equipment damage recovery

- Depends on nature of damage and cleanup
- May need disaster recovery specialists

Summary, Chapter 16

- Overview
- Physical security threats
  - Natural disasters
  - Environmental threats
  - Technical threats
  - Human-caused physical threats
- Recovery from physical security breaches
- Physical security prevention and mitigation measures
  - Environmental threats
  - Technical threats
  - Human-caused physical threats

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. **Human Security Awareness, Training and Education, Ch. 17.1**
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Security Awareness, Training, and Education

- The topic of security awareness, training, and education is mentioned prominently in a number of standards and standards-related documents, including
- ISO 27002 (Code of Practice for Information Security Management) and
- NIST SP 800-100 (Information Security Handbook: A Guide for Managers).

Benefits to Organizations

Security awareness, training, and education programs provide four major benefits to organizations:

- Improving employee behavior
- Increasing employee accountability
- Mitigating liability for employee behavior
- Complying with regulations and contractual obligations

Human Factors

Employee behavior is a critical concern in ensuring the security of computer systems and information assets

Principal problems associated with employee behavior are:

Errors and omissions	**Fraud**	**Actions by disgruntled employees**

Human Factors counter-measures

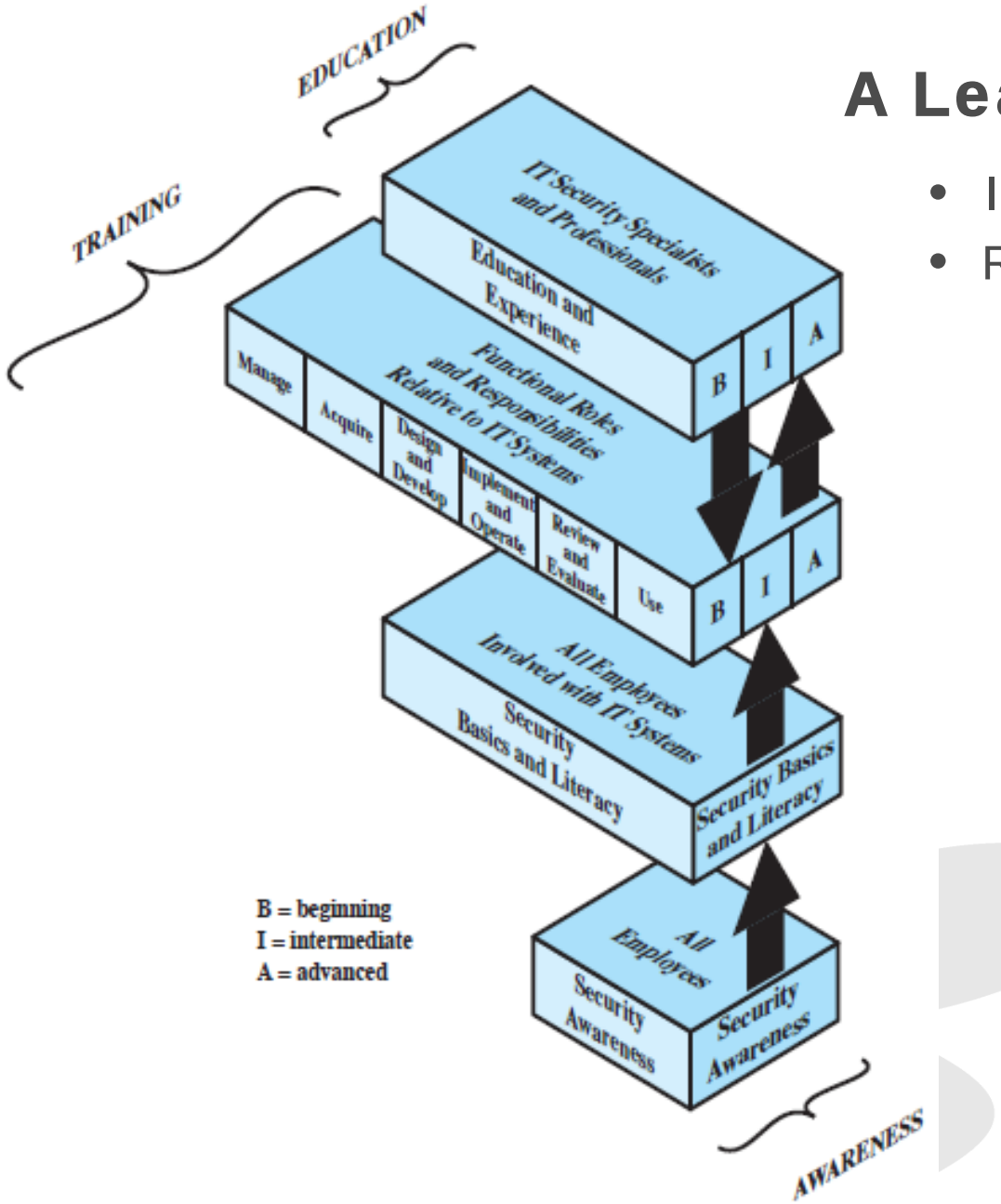
The effect of

security awareness, training, and education programs

- increasing employees' knowledge of their **accountability** and of potential penalties
- limiting an organization's **liability**
- comply with **regulations and contractual obligations**

A Learning Continuum

- Individual
- Role-based



Four layers:

- Education and experience
- Roles and responsibilities relative to IT systems
- Security basics and literacy
- Security awareness

Table 17.1
Comparative Framework

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Objective	Recognition	Skill	Understanding
Teaching method	**Media** —Videos —Newsletters —Posters, etc.	**Practical instruction** —Lecture —Case study workshop —Hands-on practice	**Theoretical instruction** —Discussion seminar —Background reading
Test measure	True/false Multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short term	Intermediate	Long term

Awareness

- Seeks to inform and focus an employee's attention on security issues within the organization
  1. Aware of their responsibilities for maintaining security and the restrictions on their actions
  2. Users understand the importance of security for the well-being of the organization
  3. Promote enthusiasm and management buy-in
- Program must be tailored to the needs of the organization and target audience
- Must continually promote the security message to employees in a variety of ways
- Should provide a security awareness policy document to all employees

Security awareness policy document

The policy should establish three things:

1. Participation in an awareness program is required for every employee. This will include an orientation program for new employees as well as periodic awareness activities.
2. Every one will be given sufficient time to participate in awareness activities.
3. Responsibility for managing and conducting awareness activities is clearly spelled out.

NIST SP 800-100 (*Information Security Handbook: A Guide for Managers)* describes the content of awareness programs, in general terms, as follows:

"Awareness tools are used to promote information security and inform users of threats and vulnerabilities that impact their division or department and personal work environment by explaining the *what* but not the *how* of security, and communicating what is and what is not allowed. Awareness not only communicates information security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness is used to explain the rules of behavior for using an agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems."

Goals for a security awareness program

1. Raise staff awareness of information technology security issues in general.
2. Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.
3. Explain organizational security policies and procedures.
4. Ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.
5. Train staff to meet the specific security responsibilities of their positions.
6. Inform staff that security activities will be monitored.
7. Remind staff that breaches in security carry consequences.
8. Assure staff that reporting of potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making behavior).
9. Communicate to staff that the goal of creating a trusted system is achievable.

Training

Designed to teach people the skills to perform their IT-related tasks more securely	• *What* people should do and *how* they should do it
General users	• Focus is on good computer security practices
Programmers, developers, system maintainers	• Develop a security mindset in the developer
Management-level	• How to make tradeoffs involving security risks, costs, benefits
Executive-level	• Risk management goals, measurement, leadership

Training

For **general users**, training focuses on good computer security practices, including the following:

- Protecting the physical area and equipment (e.g., locking doors, caring for CD-ROMs and DVDs and portable USB storage devices)
- Protecting passwords (if used) or other authentication data or tokens (e.g., never divulge PINs)
- Reporting security violations or incidents (e.g., whom to call if a virus is suspected)
- Identifying possibly suspicious phishing or spam emails and attachments, knowing how to handle them, and who to contact for assistance

Programmers, developers, and system maintainers require more specialized or advanced training, including the following:

- Develop a security mindset in the developer.
- Show the developer how to build security into development life cycle, using well-defined checkpoints.
- Teach the developer how attackers exploit software and how to resist attack.
- Provide analysts with a toolkit of specific attacks and principles with which to interrogate systems.

Training

Designed to teach people the skills to perform their IT-related tasks more securely	• *What* people should do and *how* they should do it
General users	• Focus is on good computer security practices
Programmers, developers, system maintainers	• Develop a security mindset in the developer
Management-level	• How to make tradeoffs involving security risks, costs, benefits
Executive-level	• Risk management goals, measurement, leadership

Education

- Most in depth program
- Targeted at security professionals whose jobs require expertise in security
- Fits into employee career development category
- Often provided by outside sources
  - College courses
  - Specialized training programs

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. **Employment practices and Policies, Ch. 17.2**
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Employment Practices and Policies

- Managing personnel with potential access is an essential part of information security
- Employee involvement:
  - Unwittingly aid in the commission of a violation by failing to follow proper procedures
  - Forgetting security considerations
  - Not realizing that they are creating a vulnerability
  - Knowingly violate controls or procedures

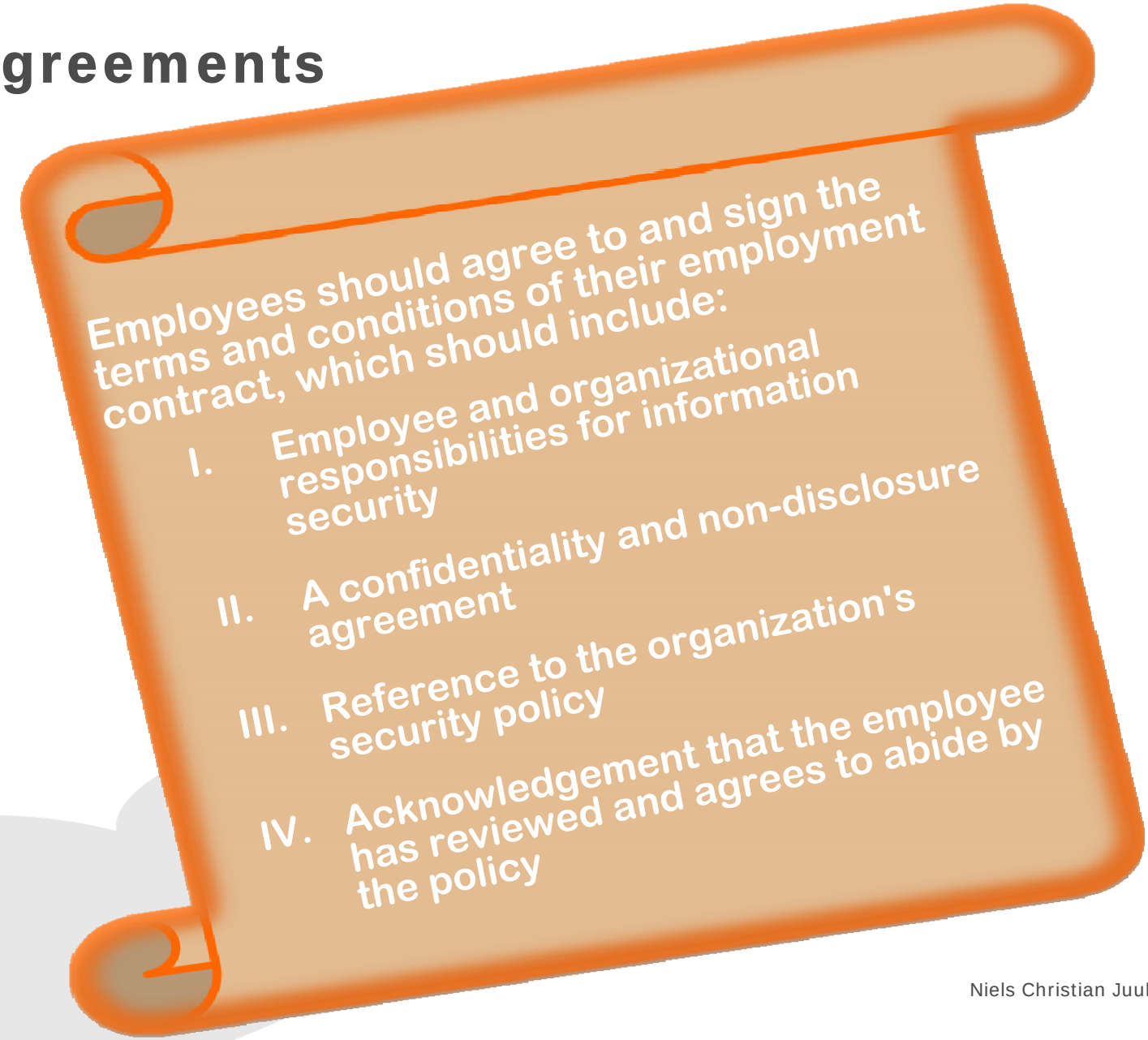
Threats from internal users includes:

- Gaining unauthorized access or enabling others to gain unauthorized access
- Altering data
- Deleting production and backup data
- Crashing systems
- Destroying systems
- Misusing systems for personal gain or to damage the organization
- Holding data hostage
- Stealing strategic or customer data for corporate espionage or fraud schemes

Security in the Hiring Process

- Objective:
  - “To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities”
- Need appropriate background checks and screening
  - Investigate accuracy of details
- For highly sensitive positions:
  - Have an investigation agency do a background check
  - Criminal record and credit check

Employment Agreements



During Employment

Objectives with respect to current employees:

- Ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security
- Are equipped to support the organizational security policy in their work
- Reduce the risk of human error

During Employment

Two essential elements of personnel security during employment are:

- A comprehensive security policy document
- An ongoing awareness and training program

During Employment

Security principles:

- Least privilege
- Separation of duties
- Limited reliance on key employees

During Employment

Objectives with respect to current employees:

- Ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security
- Are equipped to support the organizational security policy in their work
- Reduce the risk of human error

Two essential elements of personnel security during employment are:

- A comprehensive security policy document
- An ongoing awareness and training program

Security principles:

- Least privilege
- Separation of duties
- Limited reliance on key employees

Termination of Employment

Objectives:

- Ensure employees, contractors, and third party users exit organization or change employment in an orderly manner
- The return of all equipment and the removal of all access rights are completed

Actions:

- Removing the person's name from all lists of authorized access
- Explicitly informing guards that the ex-employee is not allowed into the building without special authorization by named employees
- Removing all personal access codes. If appropriate, changing lock combinations, reprogramming access card systems, and replacing physical locks
- Recovering all assets, including employee ID, portable USB storage devices, documents, and equipment.
- Notifying, by memo or e-mail, appropriate departments

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. **E-mail and Internet Use Policies, Ch. 17.3 (Student)**
9. Security Auditing, Ch. 18.1

Email and Internet Use Policies

- Organizations are incorporating specific e-mail and Internet use policies into their security policy document
- Concerns for employers:
  1. Work time consumed in non-work-related activities
  2. Computer and communications resources may be consumed, compromising the mission that the IT resources are designed to support
  3. Risk of importing malware
  4. Possibility of harm, harassment, inappropriate online conduct
  5. E-mail and the Internet may be used as tools of harassment by one employee against another.
  6. Inappropriate online conduct by an employee may damage the reputation of the organization.

Suggested Policies

Business use only

Policy scope

Content ownership

Privacy

Standard of conduct

Reasonable personal use

Unlawful activity prohibited

Security policy

Company policy

Company rights

Disciplinary action

Projects
Services to employees
The Rectorate
RUC Digital
Reception and Servicedesk
Self-service
IT support and AV Centre
Journalisation
Free software
List of IT systems
Guides
IT Security
- Vejledninger
- Handling of personal data
RUC HR

IT Security

The IT Security function attends to planning and control tasks regarding IT security and information and counselling tasks concerning IT security.

Administration

- IT security for Roskilde University
- IT Security Folder
- Function description for IT security consultant

Guidelines

- Monitoring of IT systems
- Guidelines for the use of email and internet at Roskilde University
- Guidelines for accepted use
- Guidelines for the use of email
- Guidelines for working with information and data at RUC

Procedures

- Fysisk adgangssikring på RUC
- Antivirus software

RU Guidelines....

- Roskilde University maintains a set of Guidelines for IT security and use of email/internet on intra.ruc.dk at:

  https://intra.ruc.dk/nc/en/employees/services-to-employees/ruc-digital/it-security/

  (yields also students in contrast to the URL naming)
- Monitoring of IT systems
- Guidelines for the use of email and internet at Roskilde University
- Guidelines for accepted use
- Guidelines for the use of email
- Guidelines for working with information and data at RUC

Summary, Chapter 17

- Security awareness, training, and education
  - Motivation
  - A learning continuum
  - Awareness
  - Training
  - Education
- Employment practices and policies
  - Security in the hiring process
  - During employment
  - Termination of employment
- E-Mail and Internet use policies
  - Motivation
  - Policy issues
  - Guidelines for developing a policy

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. **Security Auditing, Ch. 18.1**

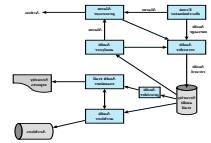
Table 18.1 Security Audit Terminology (RFC 4949)

Security audit An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

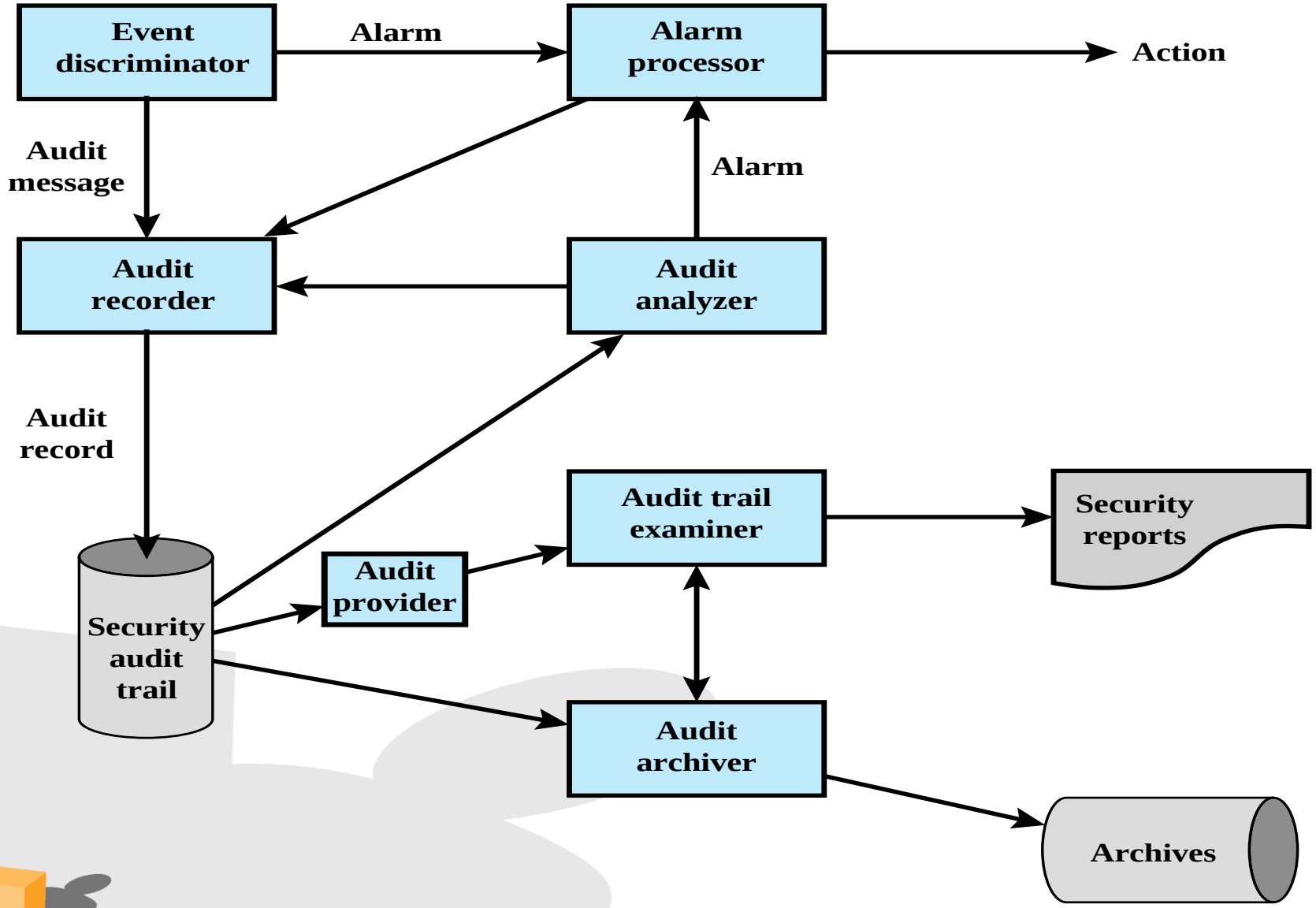
The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises.

Security Audit Trail A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Elements of the security auditing function



- **Event discriminator:** This is logic embedded into the software of the system that monitors system activity and detects security-related events that it has been configured to detect.
- **Audit recorder**: For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission as being in the form of a message. The audit could also be done by recording the event in a shared memory area.
- **Alarm processor**: Some of the events detected by the event discriminator are defined to be alarm events. For such events an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm. This action is itself an auditable event and so is transmitted to the audit recorder.
- **Security audit trail:** The audit recorder creates a formatted record of each event and stores it in the security audit trail.
- **Audit analyzer**: The security audit trail is available to the audit analyzer, which, based on a pattern of activity, may define a new auditable event that is sent to the audit recorder and may generate an alarm.
- **Audit archiver**: This is a software module that periodically extracts records from the audit trail to create a permanent archive of auditable events.
- **Archives:** The audit archives are a permanent store of security-related events on this system.
- **Audit provider:** The audit provider is an application and/or user interface to the audit trail.
- **Audit trail examiner:** The audit trail examiner is an application or user who examines the audit trail and the audit archives for historical trends, for computer forensic purposes, and for other analysis.
- **Security reports:** The audit trail examiner prepares human-readable security reports.


Event discriminator
Alarm
Alarm processor
Action
Audit message
Alarm
Audit recorder
Audit analyzer
Audit record
Audit trail examiner
Security reports
Audit provider
Security audit trail
Audit archiver
Archives

Event Definition

- Must define the set of events that are subject to audit

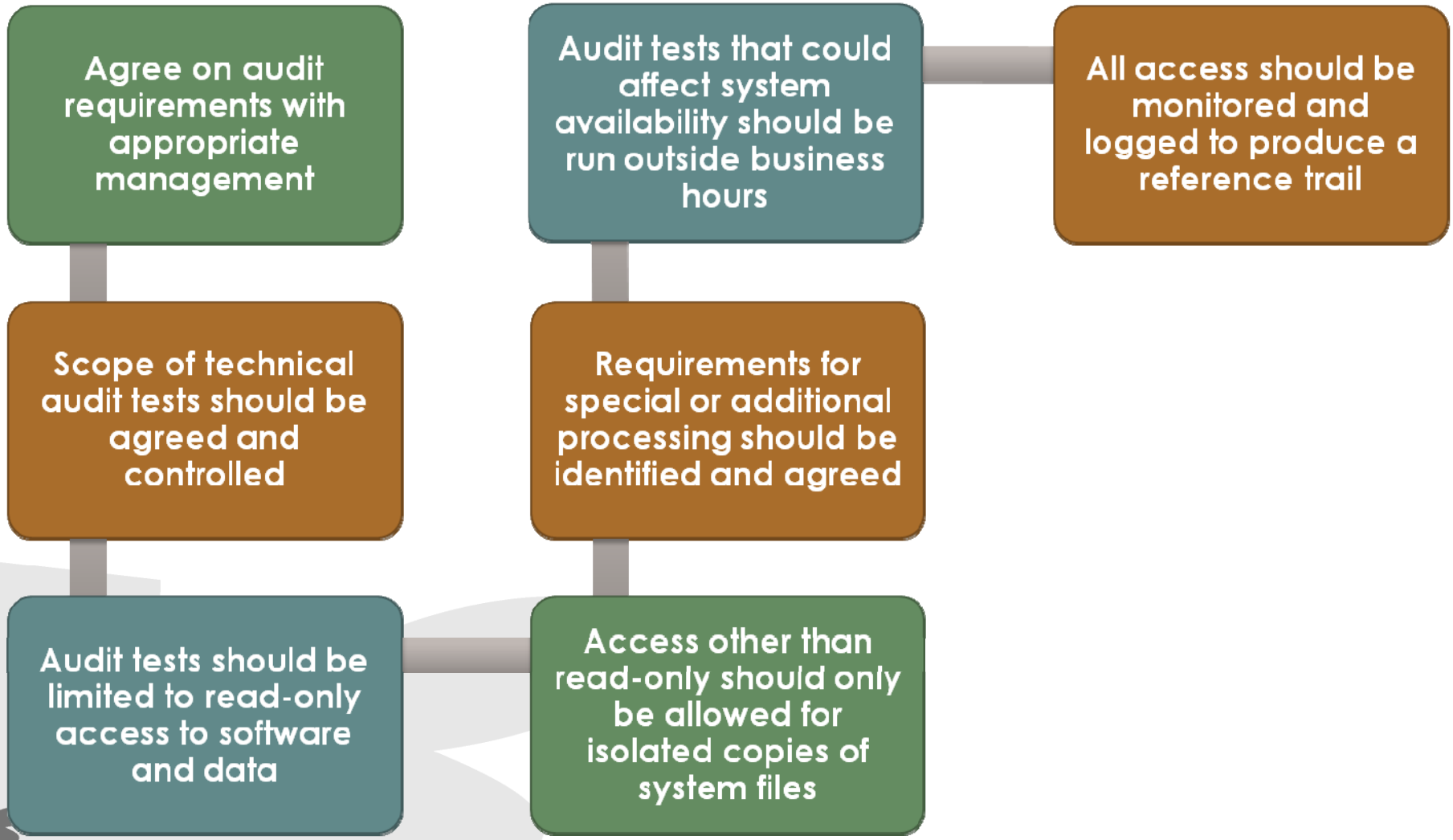
Common criteria suggests:

- Introduction of objects
- Deletion of objects
- Distribution or revocation of access rights or capabilities
- Changes to subject or object security attributes
- Policy checks performed by the security software
- Use of access rights to bypass a policy check
- Use of identification and authentication functions
- Security-related actions taken by an operator/user
- Import/export of data from/to removable media

Event Detection

- Appropriate hooks must be available in the application and system software to enable event detection
- Monitoring software needs to be added to the system and to appropriate places to capture relevant activity
- An event recording function is needed, which includes the need to provide for a secure storage resistant to tampering or deletion
- Event and audit trail analysis software, tools, and interfaces may be used to analyze collected data as well as for investigating data trends and anomalies
- There is an additional requirement for the security of the auditing function
- Auditing system should have a minimal effect on functionality

Implementation Guidelines



Summary, Chapter 18

- Security auditing architecture
  - Security audit and alarms model
  - Security auditing functions
  - Requirements
  - Implementation guidelines

Agenda

1. Intro
2. Implementing Controls and Risk Management, Ch 15.4-5
3. Silver Star Mine Case, Ch 15.6
4. Physical Security Overview & Threats , Ch. 16.1-2
5. Physical Security Counter-measures, Ch. 16.3-4
6. Human Security Awareness, Training and Education, Ch. 17.1
7. Employment practices and Policies, Ch. 17.2
8. E-mail and Internet Use Policies, Ch. 17.3 (Student)
9. Security Auditing, Ch. 18.1

Learning outcome

Be able to

- create an security implementation plan
- establish a plan for site and physical security
- manage the human elements of security
- evaluate, establish and manage an Internet security policy for employees

Exam themes/questions:

- How to make a Security Implementation Plan?
- Physical and Human security threats and how to cope with them
- Internet/E-mail security policy - from theory to examples