CSE413 – Security of Information Systems 2020

PhD Furkan Gözükara, Toros University

https://github.com/FurkanGozukara/Security-of-Information-Systems-CSE413-2020

Lecture 2

Information Security Management and Human Factors for Information Security

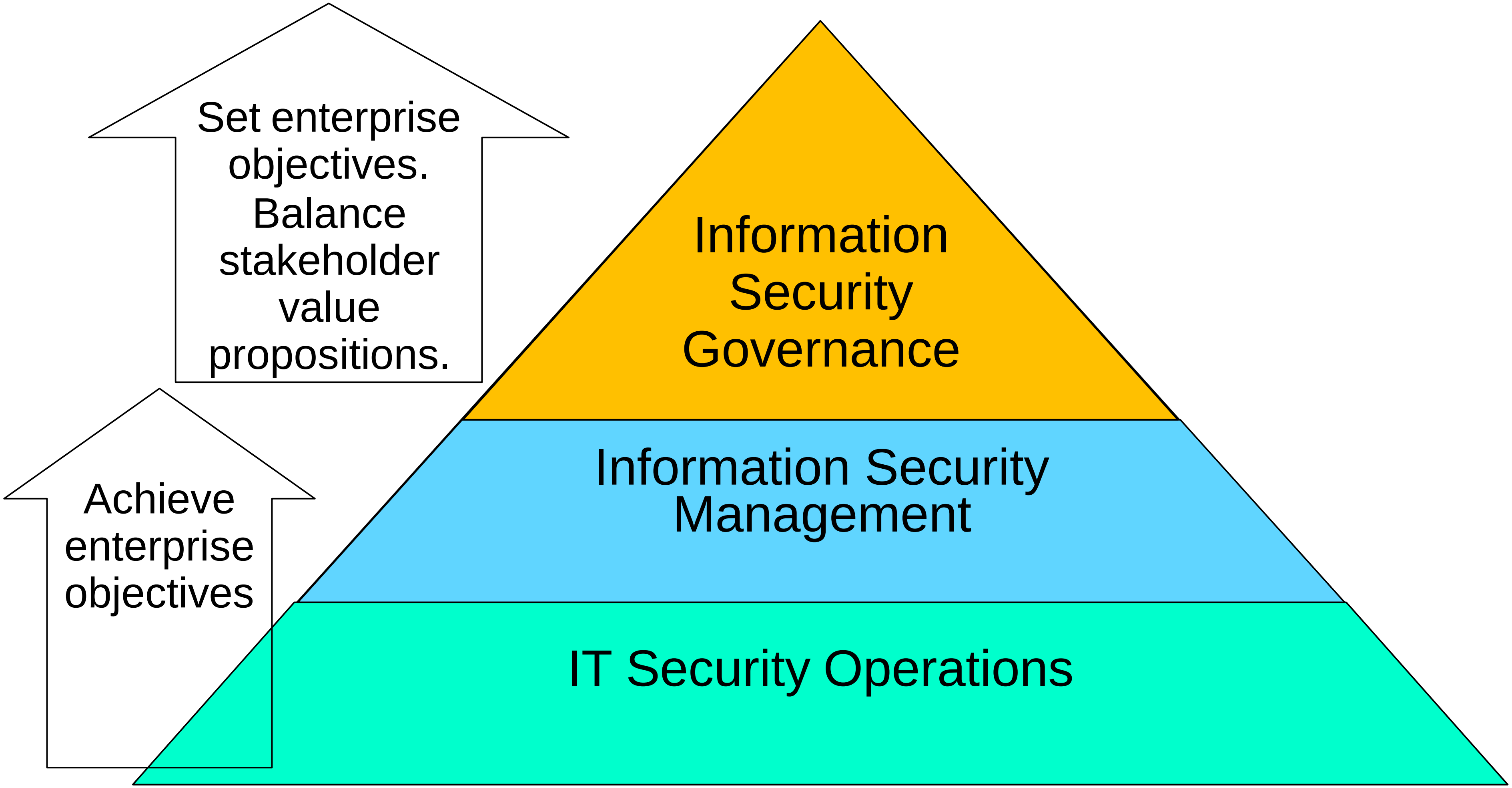
Composed from Prof. Audun Jøsang, University of Oslo, Information Security 2018 Lectures

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Corporate Responsibilities

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Security Management Levels


Set enterprise objectives. Balance stakeholder value propositions.
Achieve enterprise objectives
Information Security Governance
Information Security Management
IT Security Operations

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Information Security Governance

IS governance provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme.

- IT Governance Institute

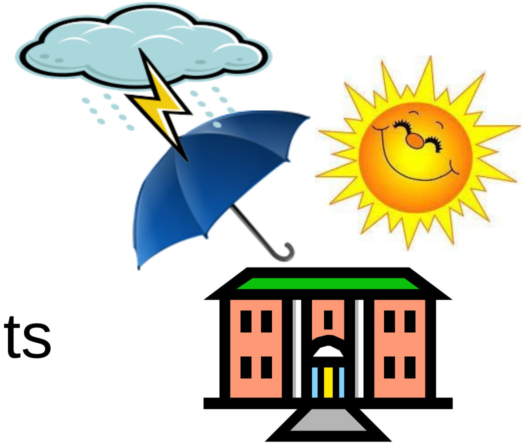
Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lect

Security Governance

Benefits of IT Security Governance

Protecting assets = creating value

- Trust from customers, partners, investors, own staff
- Reputation, brand, image
- Competitive advantage
- Prevention and reduction of losses
- Business continuity & resilience
  - In case of disasters and major incidents
- Increase shareholder value



Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lec

Security Governance

Goals of information security governance as defined by COBIT and ISACA

1. Strategic alignment of security program
2. Risk management
3. Value delivery
4. Resource management
5. Performance measurement

http://www.isaca.org/knowledge-center/research/documents/information-security-govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lec

Security Governance

Characteristics of good IS Governance

Managed as a business-wide issue

- ➢ Alignment of frameworks, policies and activities

Viewed as business requirement

- ➢ Seen as essential for sustainable business operations

Leaders are informed

- ➢ Visible leaders who understand risks and get regular reviews

Leaders take responsibility

- ➢ Leaders set clear goals and priorities

Risk-based priorities

- ➢ Tolerances to risk understood and established

Roles & responsibilities defined

- ➢ Clear segregation of duties

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lect

Security Governance

Information security management

Includes:

- Risk management and reporting
- Development and maintenance of security policies
  - Documented goals, rules and practice for IS
- Planning and organisation of the security activities
  - Information Security Management System (ISMS)
- Information classification
- Integration of security procedures, standards & guidelines
- Deployment and maintenance of security controls
- Security education and training
- Disaster recovery and business continuity planning
- Coordination with top level management

Security Management

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

IS Management Standards

- ISO/IEC 27K security standards:
  - ISO: International Standards Organization
  - ISO 27001: Information Security Management System (ISMS)
  - ISO 27002: Code of practice for information security controls
  - + many more
  - ISO/IEC standards cost money
- USA
  - NIST (National Institute for Standards and Technology) Special Publications 800 ,
  - Cover similar topics as ISO27K
  - NIST standards are free

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Evolution of ISO 27001 & 27002 Standards

- **1995**

BS 7799 Code of Practice for Information Security Management

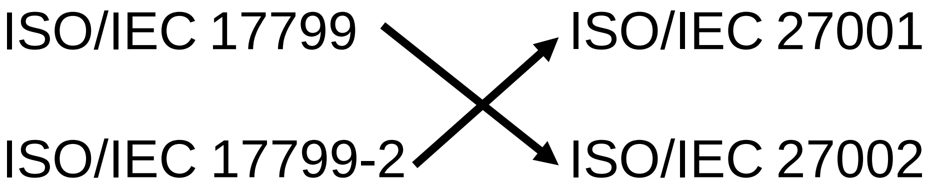
- **1999**

BS 7799-2 Information Security Management System (ISMS)

- **2001**

BS 7799 → ISO/IEC 17799
BS 7799-2 → ISO/IEC 17799-2

- **2005**



ISO/IEC 17799
ISO/IEC 17799-2
ISO/IEC 27001
ISO/IEC 27002

- **2013**

ISO Management Standards Alignment

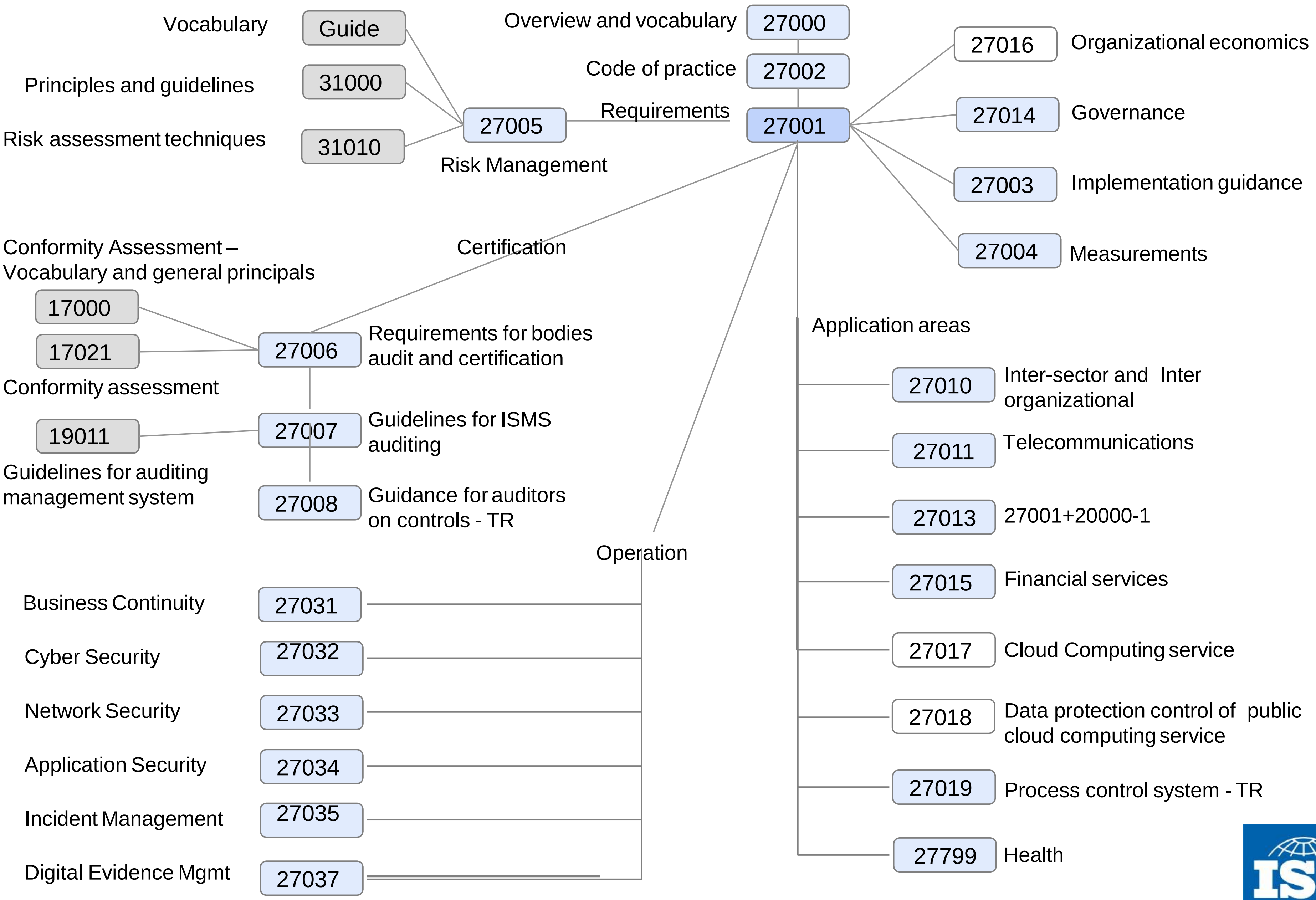
- ISO/IEC 27001 ISMS
- ISO/IEC 27002 Code of Practice for Information Security Controls

- **2017**

Latest update, minor changes

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

ISO/IEC 27000 family of standards and related standards *as of Oct. 2013*



Vocabulary — Guide

Principles and guidelines — 31000

Risk assessment techniques — 31010

27005 — Risk Management

Requirements

Overview and vocabulary — 27000

Code of practice — 27002

27001

27016 — Organizational economics

27014 — Governance

27003 — Implementation guidance

27004 — Measurements

Certification

Conformity Assessment – Vocabulary and general principals — 17000

17021 — Conformity assessment

27006 — Requirements for bodies audit and certification

19011 — Guidelines for auditing management system

27007 — Guidelines for ISMS auditing

27008 — Guidance for auditors on controls - TR

Operation

Business Continuity — 27031

Cyber Security — 27032

Network Security — 27033

Application Security — 27034

Incident Management — 27035

Digital Evidence Mgmt — 27037

Application areas

27010 — Inter-sector and Inter organizational

27011 — Telecommunications

27013 — 27001+20000-1

27015 — Financial services

27017 — Cloud Computing service

27018 — Data protection control of public cloud computing service

27019 — Process control system - TR

27799 — Health

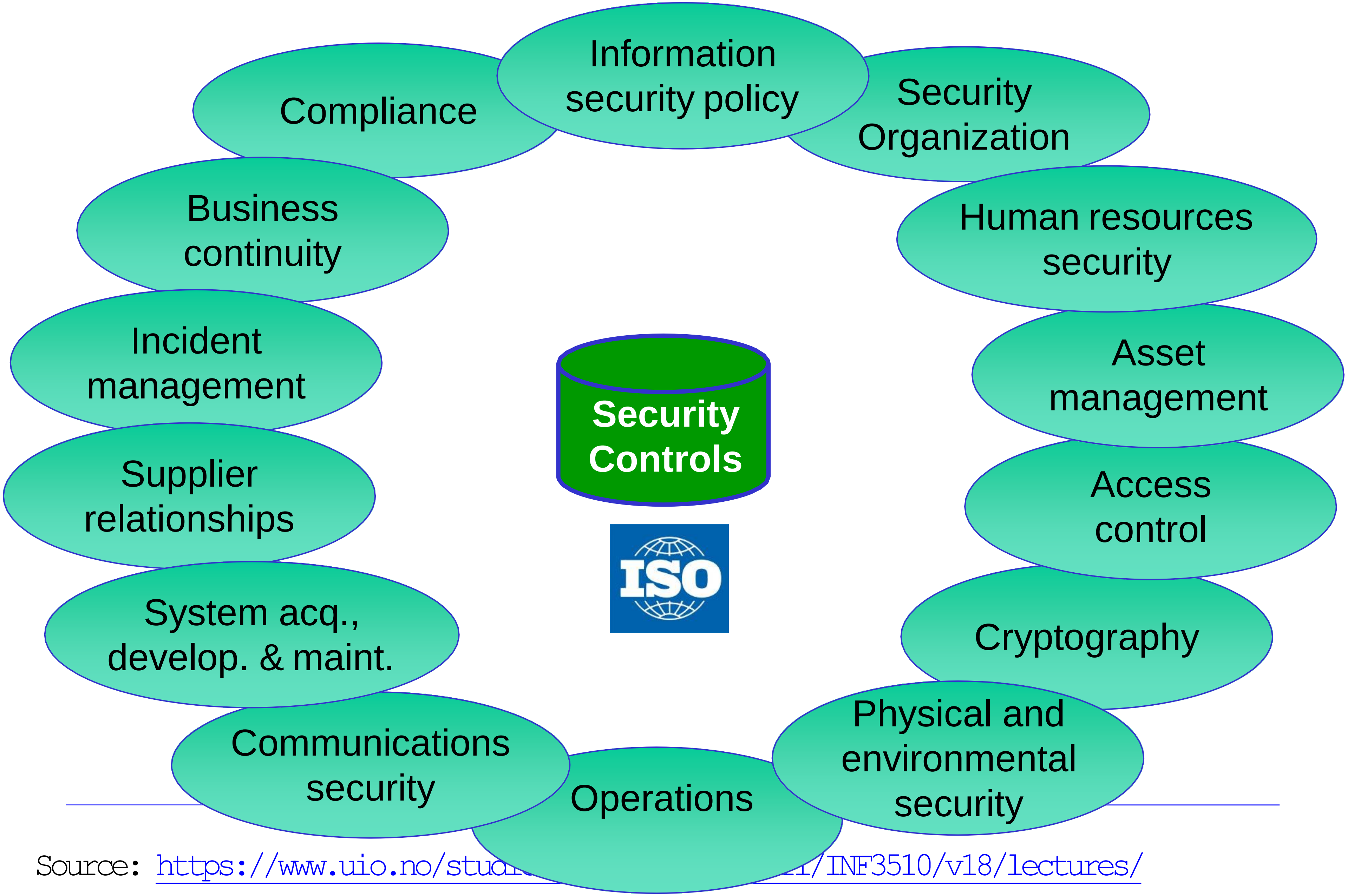
ISO/IEC 27002– What is it?

Code of practice for information security controls

- ISO 27002 provides a checklist of general security controls to be considered implemented/used in organizations
  - Contains 14 categories (control objectives) of security controls
  - Each category contains a set of security controls
  - In total, the standard describes 113 generic security controls
- Not all controls are relevant to every organisation
- Objective of ISO 27002:
- "… gives guidelines for […] information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)."

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

The 14 Control Objectives of ISO/IEC 27002:2013



Information security policy

Security Organization

Human resources security

Asset management

Access control

Cryptography

Physical and environmental security

Operations

Communications security

System acq., develop. & maint.

Supplier relationships

Incident management

Business continuity

Compliance

Security Controls

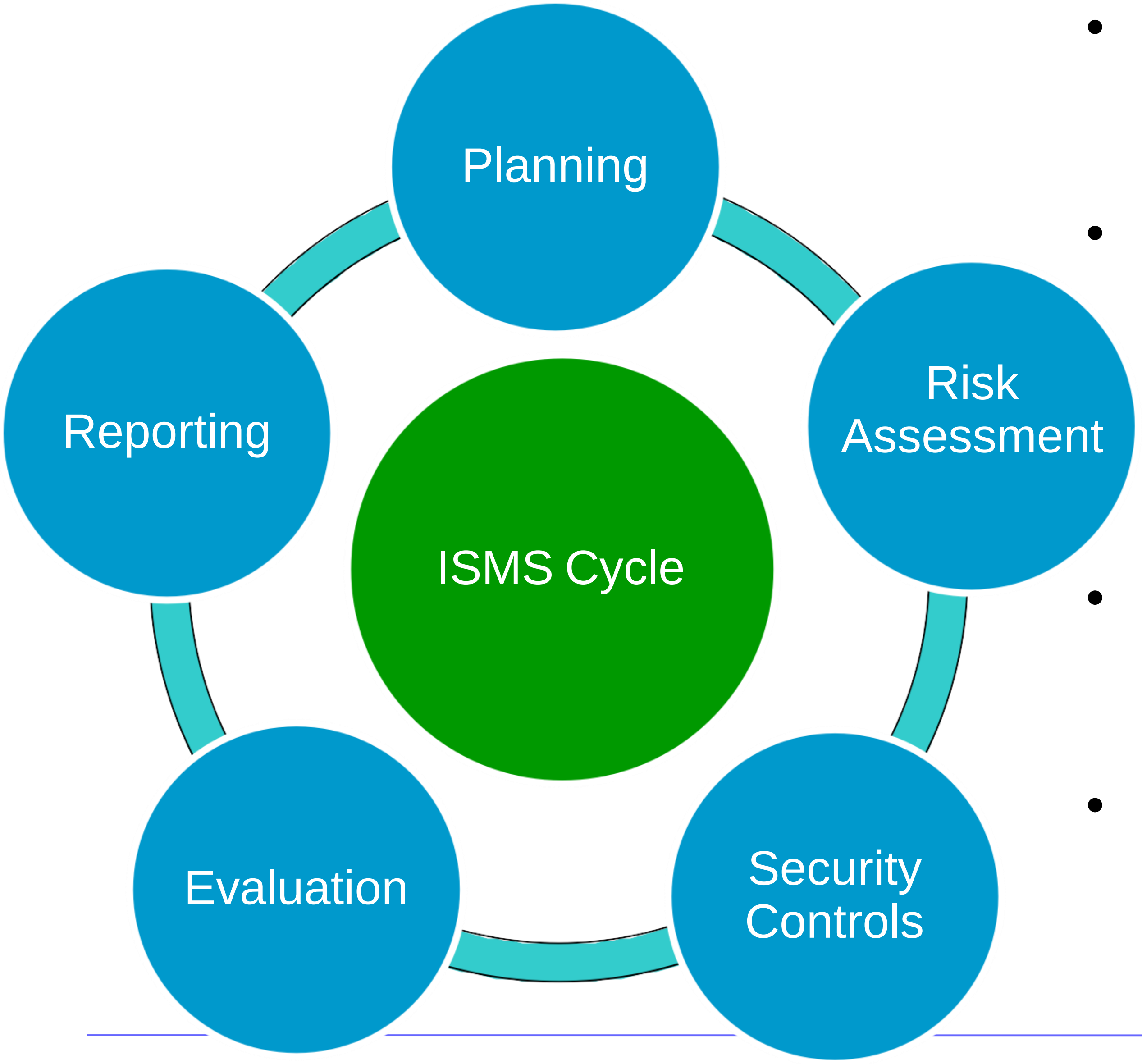
Source: https://www.uio.no/studi 1/INF3510/v18/lectures/

ISO/IEC 27001:2013- What is it?

- ISO 27001 specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization.
- ISMS is a holistic approach to IS management
  - … not an IT system
- While the ISO 27002 (code of practice) defines a set of security goals and controls, ISO 27001 (ISMS) defines how to manage the implementation of security controls.
- Organizations can be certified against ISO 27001
  - … but not against ISO 27002
- ISO 27001 is to be used in conjunction with ISO 27002

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

IS Management System Cycle



- IS management cycle as an interpretation of ISMS (ISO 27001).
- Source: NSM (Nasjonal Sikkerhets-myndighet).

- The steps in the cycle can be performed in parallel.
- Good IS management requires that all steps are implemented by the organisation

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

CISSP 7th Ed. IS Program Phases

CISSP 7th Ed. (p.41) IS program phases	Description
1. Plan and organise	• Establish mgmt commitment and high level IS policy • Define roles and committees, • Assess threats, vulnerabilities and risk • Identify and plan security solutions and controls
2. Implement	• Assign roles and responsibilities • Develop specific IS policies and procedures • Implement security solutions and controls
3. Operate and maintain	• Execute security operations tasks • Carry out internal and external audit • Develop monitoring and metrics for security controls
4. Monitor and evaluate	• Review audits, monitoring and metrics • Assess goal accomplishment • Identify areas for improvement, and integrate in phase 1.

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

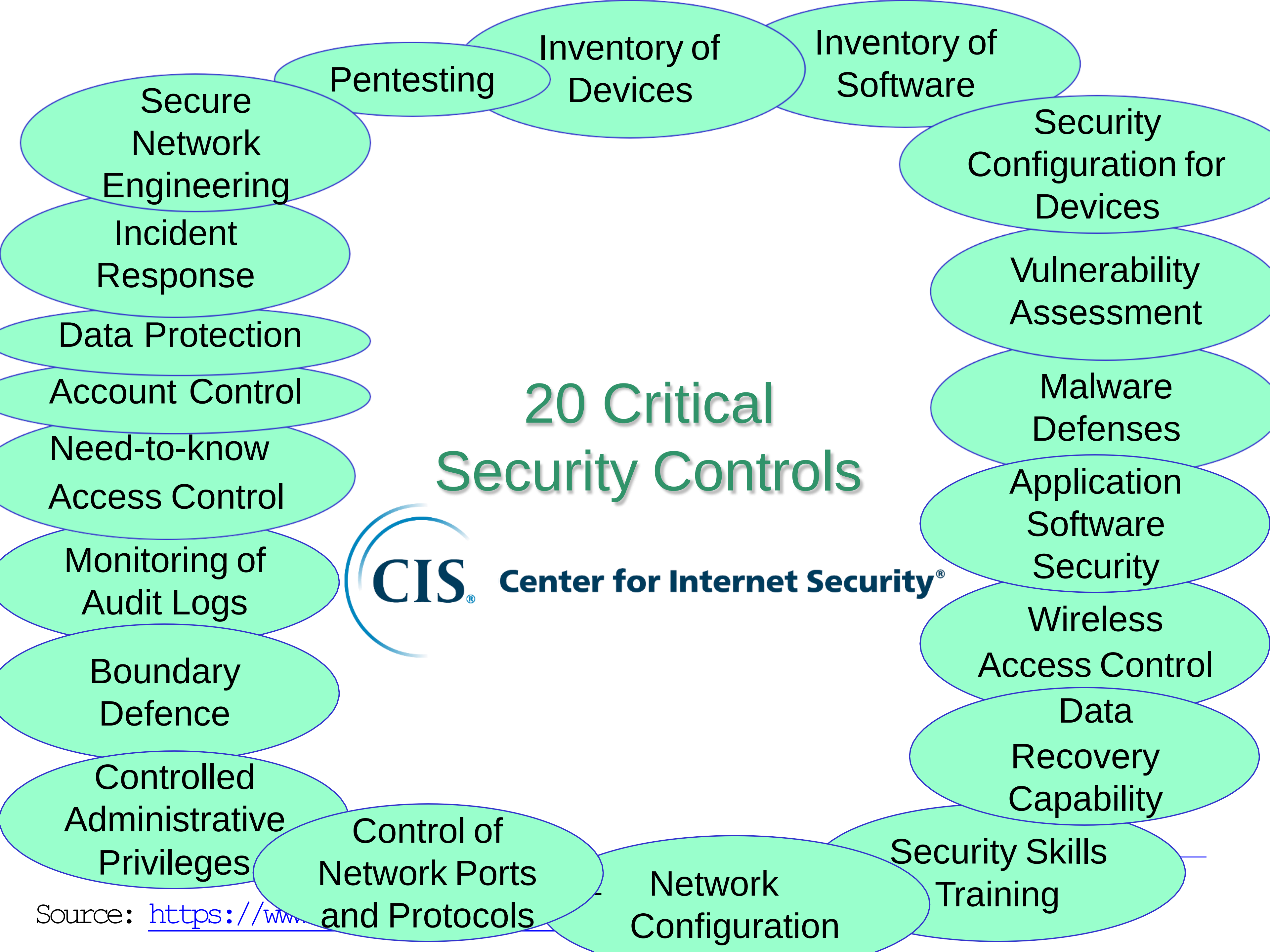
20 CSC: Critical Security Controls

- 20 essential security controls
- https://www.cisecurity.org/controls/
- Description of each control:
  - Why control is critical
  - How to implement controls
    - Specific tasks
  - Procedures and tools
    - Advice on implementation
  - Effectiveness metrics
  - Automation metrics
    - How to automate effectiveness metrics
  - Effectiveness tests
  - System entity relationship diagram
    - Relevant architecture integration

CIS Center for Internet Security®

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

20 Critical Security Controls



CIS Center for Internet Security®

- Inventory of Devices
- Inventory of Software
- Security Configuration for Devices
- Vulnerability Assessment
- Malware Defenses
- Application Software Security
- Wireless Access Control
- Data Recovery Capability
- Security Skills Training
- Network Configuration
- Control of Network Ports and Protocols
- Controlled Administrative Privileges
- Boundary Defence
- Monitoring of Audit Logs
- Need-to-know Access Control
- Account Control
- Data Protection
- Incident Response
- Secure Network Engineering
- Pentesting

Source: https://www.

Evaluation of the ISMS through Security Measurements

- What is the effectiveness of a security control ?
    - – You have to measure it to know it.
    - Security measurements provide
  - – info about how well security controls work
  - – basis for comparing effect of controls on risks
  - – benchmark for assessing security investments

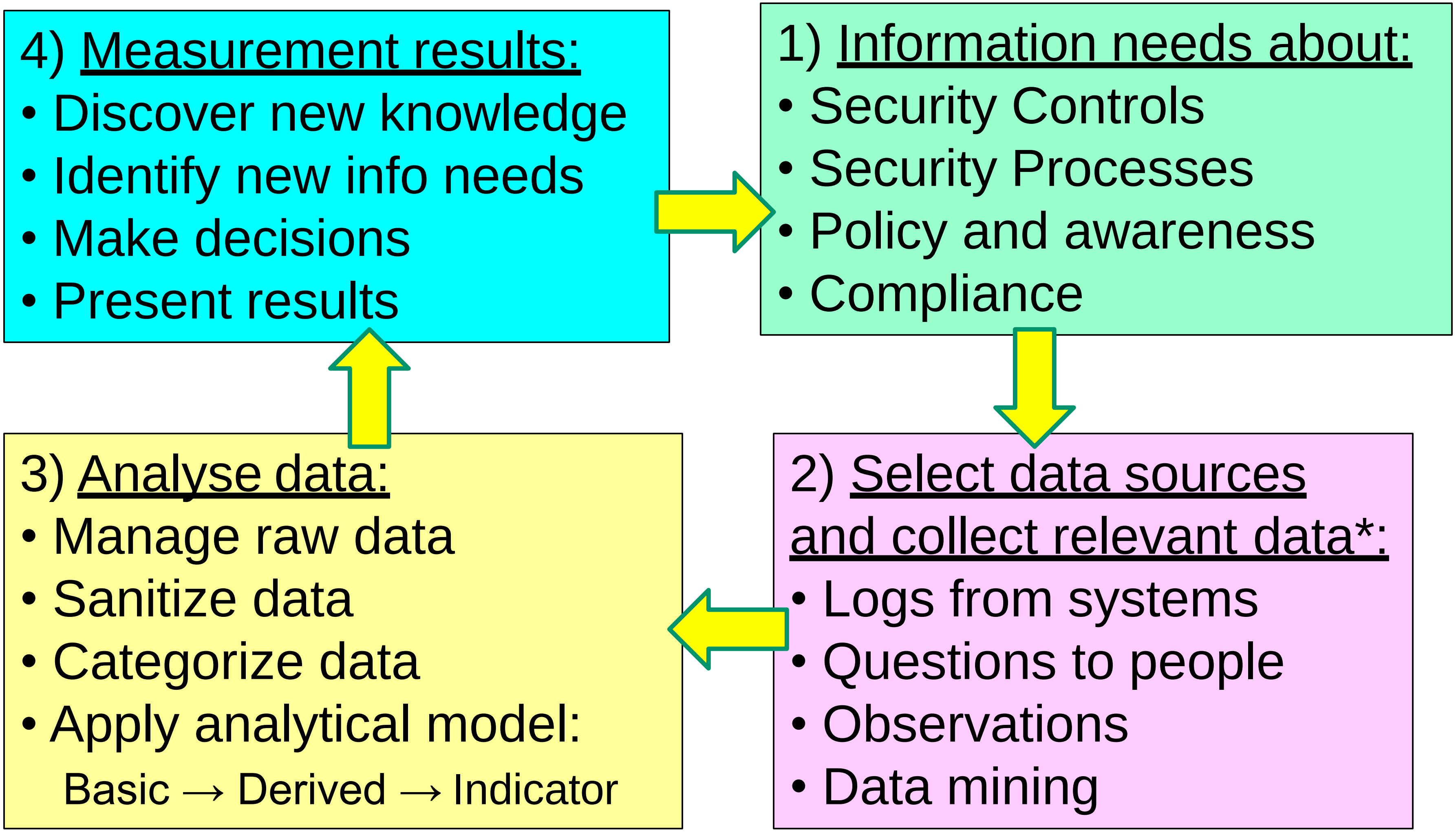
Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Why do we care: Example

- **The CEO asks**, *"Is our network perimeter secure?"*
- **Without metrics:**
  "Well, we installed a firewall, so it must be."
- **With metrics:**
  "Yes, our evidence tells us that we are. Look at our intrusion statistics before and after we completed that firewall project. It's down 80%. We are definitely more secure today than we were before."

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

IS Measurement Model (ISO 27004)



1) Information needs about:
- Security Controls
- Security Processes
- Policy and awareness
- Compliance

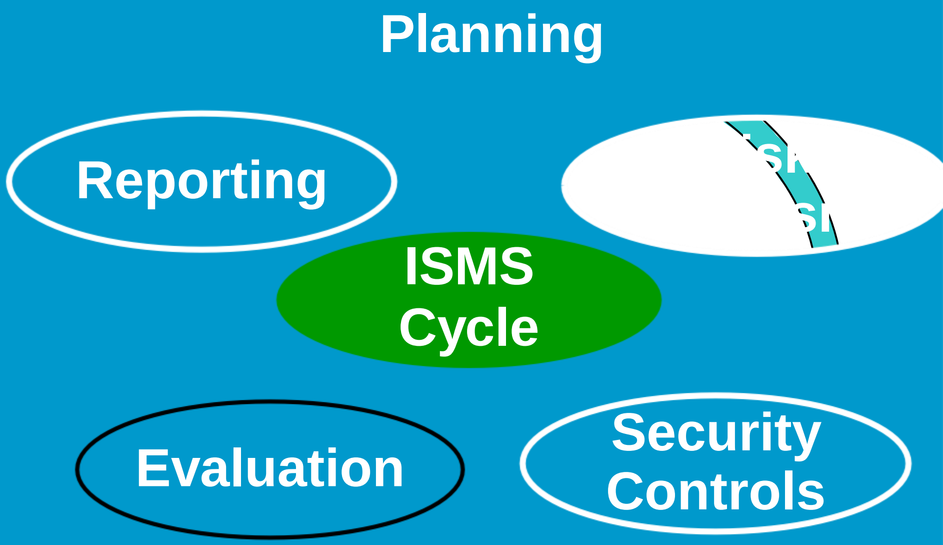
2) Select data sources and collect relevant data*:
- Logs from systems
- Questions to people
- Observations
- Data mining

3) Analyse data:
- Manage raw data
- Sanitize data
- Categorize data
- Apply analytical model:

Basic → Derived → Indicator

4) Measurement results:
- Discover new knowledge
- Identify new info needs
- Make decisions
- Present results

*) Called Objects of measurement in ISO 27004



Planning

Reporting

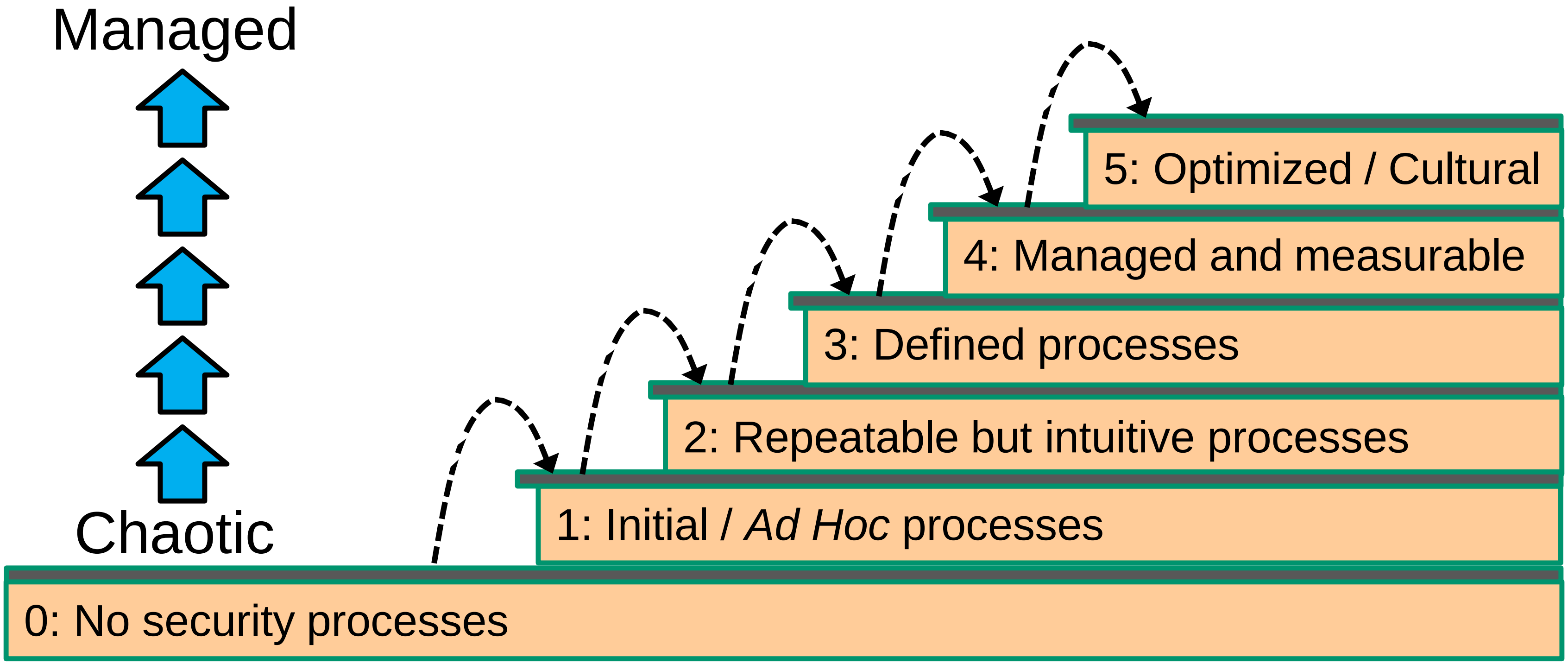
ISMS Cycle

Evaluation

Security Controls

CMMI
Capability Maturity Model Integration

Considerable effort and time is required to reach each next level in the maturity model.



Managed
Chaotic
5: Optimized / Cultural
4: Managed and measurable
3: Defined processes
2: Repeatable but intuitive processes
1: Initial / *Ad Hoc* processes
0: No security processes

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

CMM levels 1 - 3

1. Initial / Ad Hoc
   - + Processes are ad-hoc and disorganised.
   - + Risks are considered on an ad hoc basis, but no formal processes exist.
2. Repeatable but intuitive
   - + Processes follow a regular pattern.
   - + Emerging understanding of risk and the need for security
3. Defined process
   - + Processes are documented and communicated.
   - + Company-wide risk management.’
   - + Awareness of security and security policy

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

CMM levels 4 - 5

4. Managed and measurable
   - + Processes are monitored and measured.
   - + Risks assessment standard procedures
   - + Roles and responsibilities are assigned
   - + Policies and standards are in place
5. Optimized
   - + Security culture permeates organisation
   - + Organisation-wide security processes are implemented, monitored and followed

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

The human factor in information security

- ❖Personnel integrity
  - ❖Making sure personnel do not become attackers
- ❖Personnel as defence
  - ❖Making sure personnel do not fall victim to social engineering attacks
- ❖Security usability
  - ❖Making sure users operate security correctly

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Personnel Integrity

Preventing employees from becoming attackers

- Consider:
  - Employees
  - Executives
  - Customers
  - Visitors
  - Contractors & Consultants
- All these groups obtain some form of access privileges
- How to make sure privileges are not abused?

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Personnel crime statistics

- Organisations report that a large proportion of computer
  crimes originate from inside

- US Statistics (PWC) 2014, 2015, 2016
  - http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
  - https://insights.sei.cmu.edu/insider-threat/2017/01/2016-us-state-of-cybercrime-highlights.html
  - 28% had insider attacks, 32% very concerned about insider threats
- Australian Statistics (CERT Australia) 2015
  - http://apo.org.au/research/cyber-crime-and-security-survey-report-2013
  - 14% had insider attacks, 60% very concerned avout insider threats

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Strengthening employee integrity

- Difficult to determine long term integrity of staff at hiring
  - Integrity can change, influenced by events
- All personnel should follow security awareness training
- Reminders about security policy and warnings about consequences of intentional breach of policy
  - Will strengthen power of judgment
- Personnel in highly trusted positions must be supported, trained and monitored
- Support and monitor employees in difficult situations:
    - conflict, loss of job, personal problems
- Stay on good terms with staff leaving the company !

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Personnel Departure

- Different reasons for departure
  - Voluntary
  - Redundancy
  - Termination
- Different types of actions
  - Former employee may keep some privileges
  - Revoke all privileges
  - Escort to the exit.
- During exit interview, terms of original employment agreement reviewed (i.e. non-compete, wrongful disclosure, etc.

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Social engineering attacks

Where people are the defence

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Social Engineering Attacks

- According to Kevin Mitnick:
  - “The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you.”
  - “What I found personally to be true was that it’s easier to manipulate people rather than technology. Most of the time, organisations overlook that human element”.

From “How to hack people”, BBC NewsOnline, 14 Oct 2002

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Develop Trust

- People are naturally helpful and trusting
- Ask during seemingly innocent conversations
- Slowly ask for increasingly important information
- Learn company lingo, names of key personnel, names of servers and applications
- Cause a problem and subsequently offer your help to
  fix it (aka. reverse social engineering)
- Talk negatively about common enemy
- Talk positively about common hero

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Induce strong affect

- Heightened emotional state makes victim
  - Less alert
  - Less likely to analyse deceptive arguments
      - Triggered by attacker by creating
        - Excitement (“you have won a price”)
  - Fear (“you will lose your job”)
  - Confusion (contradictory statements)

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Information overload

- Reduced the target's ability to scrutinize arguments proposed by the attacker
- Triggered by
  - Providing large amounts of information to produce sensory overload
  - Providing arguments from an unexpected angle, which forces the victim to analyse the situation from new perspective, which requires additional mental processing

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Reciprocation

- Exploits our tendency to return a favour
  - Even if the first favour was not requested
  - Even if the return favour is more valuable
- Double disagreement
  - If the attacker creates a double disagreement, and gives in on one, the victim will have a tendency to give in on the other
- Expectation
  - If the victim is requested to give the first favour, he will believe that the attacker becomes a future ally

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics:
Diffusion of responsibility and moral duty

- Make the target feel the he or she will not be held responsible for actions
- Make the target feel that satisfying attacker’s request is a moral duty

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Authority

- People are conditioned to obey authority
  - Milgram and other experiments
  - Considered rude to even challenge the veracity of authority claim
- Triggered by
  - Faking credentials
  - Faking to be a director or superior
  - Skilful acting (con artist)

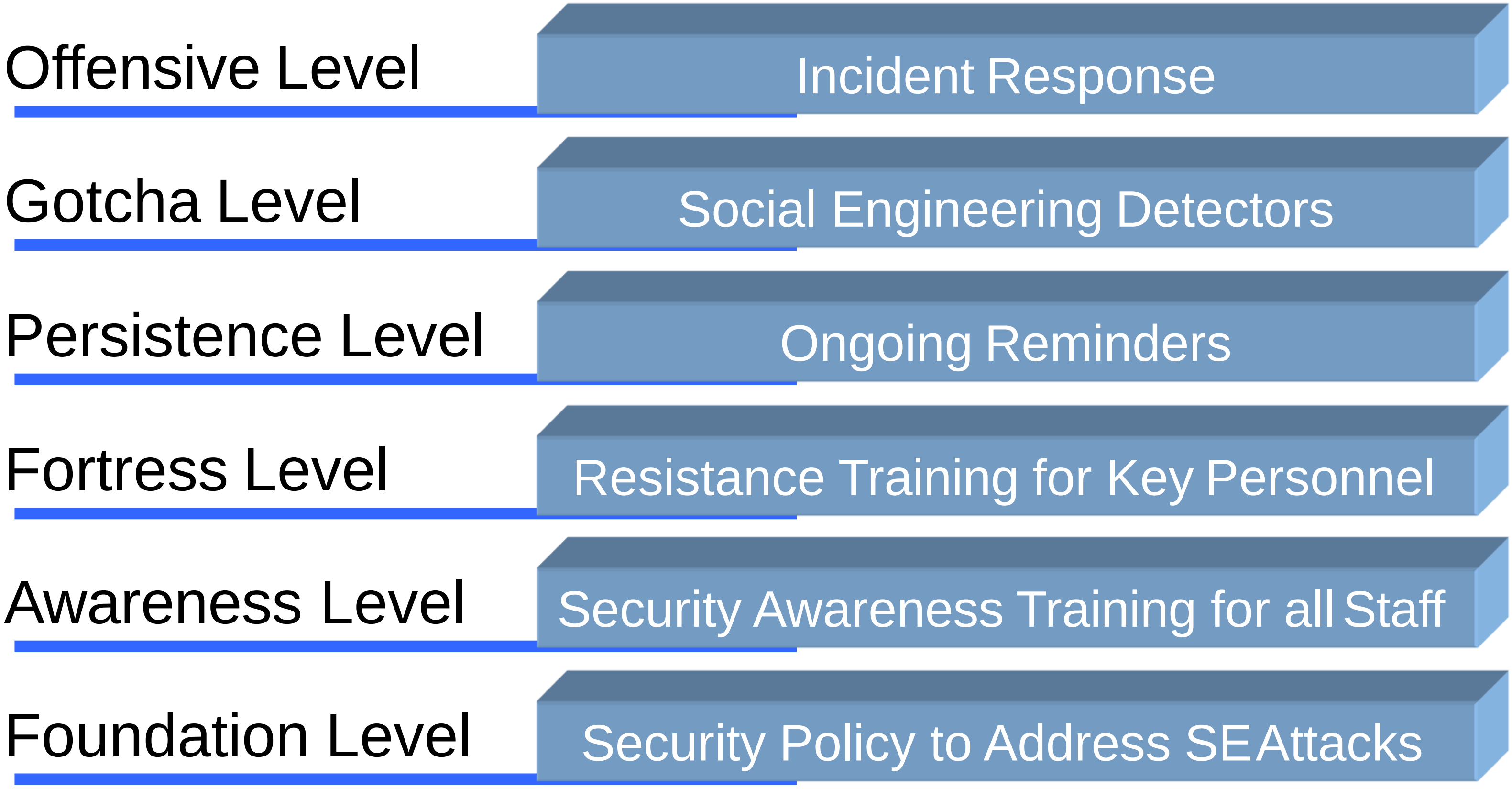
Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Tactics: Commitment creep

- People have a tendency to follow commitments, even when recognising that it might be unwise.
- It’s often a matter of showing personal consistency and integrity
- Triggered e.g. by creating a situation where one commitment naturally or logically follows another.
  - First request is harmless
  - Second request causes the damage

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Multi-Level Defence against Social Engineering Attacks



Offensive Level	Incident Response
Gotcha Level	Social Engineering Detectors
Persistence Level	Ongoing Reminders
Fortress Level	Resistance Training for Key Personnel
Awareness Level	Security Awareness Training for all Staff
Foundation Level	Security Policy to Address SE Attacks

Source: David Gragg: http://www.sans.org/rr/whitepapers/engineering/

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Foundation

- The security policy must address SE attacks
  - Policy is always the foundation of information security
    - Address e.g.: Shredding, Escorting, Authority obedience
- Ban practice that is similar to social attack patterns
  - Asking for passwords over phone is a typical SE attack method

    → Therefore never provide passwords over the phone
  - Calling a user and pretending to represent IT department is a typical SE attack

    → Therefore never call user, or make it possible/mandatory for user to authenticate the IT Department
  - Calling IT dep. and pretending to be user is a typical SE attack

    → Therefore make it possible/mandatory for IT department to authenticate the user

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Awareness

- Security awareness training for all staff
  - Understanding SE tactics
  - Learn to recognise SE attacks
  - Know when to say “no”
  - Know what is sensitive
  - Understand their responsibility
  - Understand the danger of casual conversation
  - Friends are not always friends
  - Passwords are personal
  - Uniforms are cheap
- Awareness of policy shall make personnel feel that the only choice is to resist SE attempts

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Fortress

- Resistance training for key personnel
  - Consider: Reception, Help desk, Sys.Admin., Customer service,
- Fortress training techniques
  - Inoculation
    - Expose to SE arguments, and learn counterarguments
  - Forewarming
    - of content and intent
  - Reality check:
    - Realising own vulnerability,

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Persistence

- Ongoing reminders
  - SE resistance will quickly diminish after a training session
  - Repeated training
  - Reminding staff of SE dangers
    - Posters
    - Messages
    - Tests

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Gotcha

- Social Engineering Detectors
  - Filters and traps designed to expose SE attackers
- Consider:
  - The justified Know-it-all
    - Person who knows everybody
  - Centralised log of suspicious events
    - Can help discover SE patterns
  - Call backs mandatory by policy
  - Key questions, e.g. personal details
  - “Please hold” mandatory by policy
    - Time to think and log event
  - Deception
    - Bogus question
    - Login + password of “alarm account” on yellow sticker

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

SE Defence: Offensive

- Incident response
  - – Well defined process for reporting and reacting to
    - Possible SE attack events,
    - Cases of successful SE attacks
- Reaction should be vigilant and aggressive
  - – Go after SE attacker
  - – Proactively warn other potential victims

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Security awareness training

- Back up and protection of work related information
- Passwords
- Email and web hygiene and acceptable use
- Recognising social engineers
- Recognising and reporting security incidents
- Responsibilities and duties for security
- Consequences of negligence or misbehaviour
- Security principles for system and business processes

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Security Usability

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Kerckhoffs - 1883

The father of security usability

- Auguste Kerckhoffs. La cryptographie militaire. Journal des sciences militaires, IX(38):5-38, 1883.
- Most famous for *"don't do security by obscurity"*
- Also defined security usability principles

> *It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants.*

> *Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.*

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

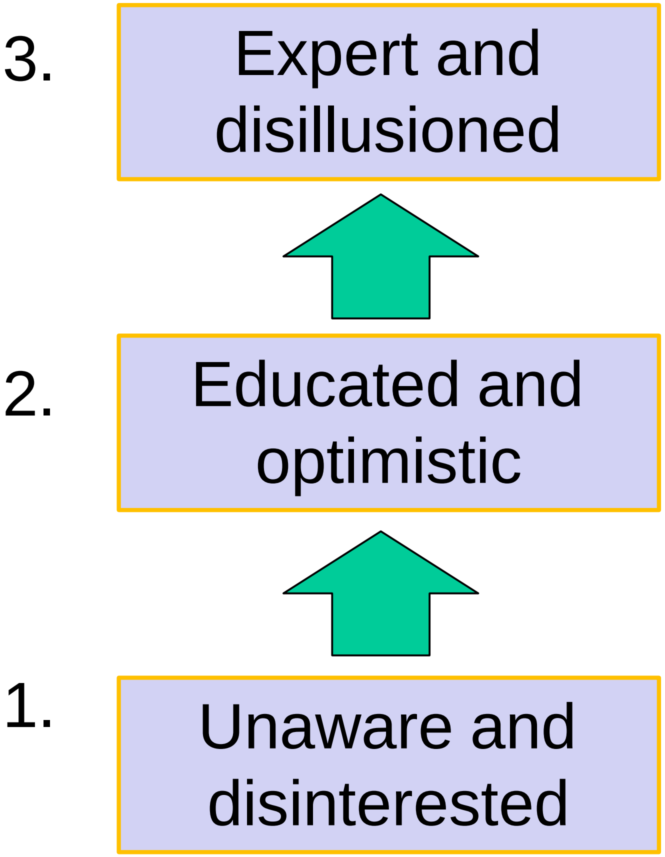
Security Learning

- Good metaphors are important for learning
- Many security concepts do not have intuitive metaphors
- Better avoid metaphors than use bad ones
- Define new security concepts
  - and give them semantic content
- Security learning design
  - Design systems to facilitate good security learning
  - Largely unexplored field

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Stages of security learning

(Security is often more complicated than you think)



3. Expert and disillusioned

2. Educated and optimistic

1. Unaware and disinterested

- *“This is far more complex than I first thought. I actually don’t think this can ever be made secure.”*
- *“I understand it now, it’s simple, and I know how to operate it”*
- *“I don’t understand it, and I don’t want to know about it. Why can’t security simply be transparent?”*

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

Remarks on security usability

- Security usability is difficult to get right
  - Not the same as IT usability
- Security can never be made 100% transparent
  - Security learning is needed, but a challenge
- Security decisions often made without basis
  - Better support for security decisions is needed
- Knowledge about security usability is available
  - User-friendly security can be designed

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

End of Lecture

Source: https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/