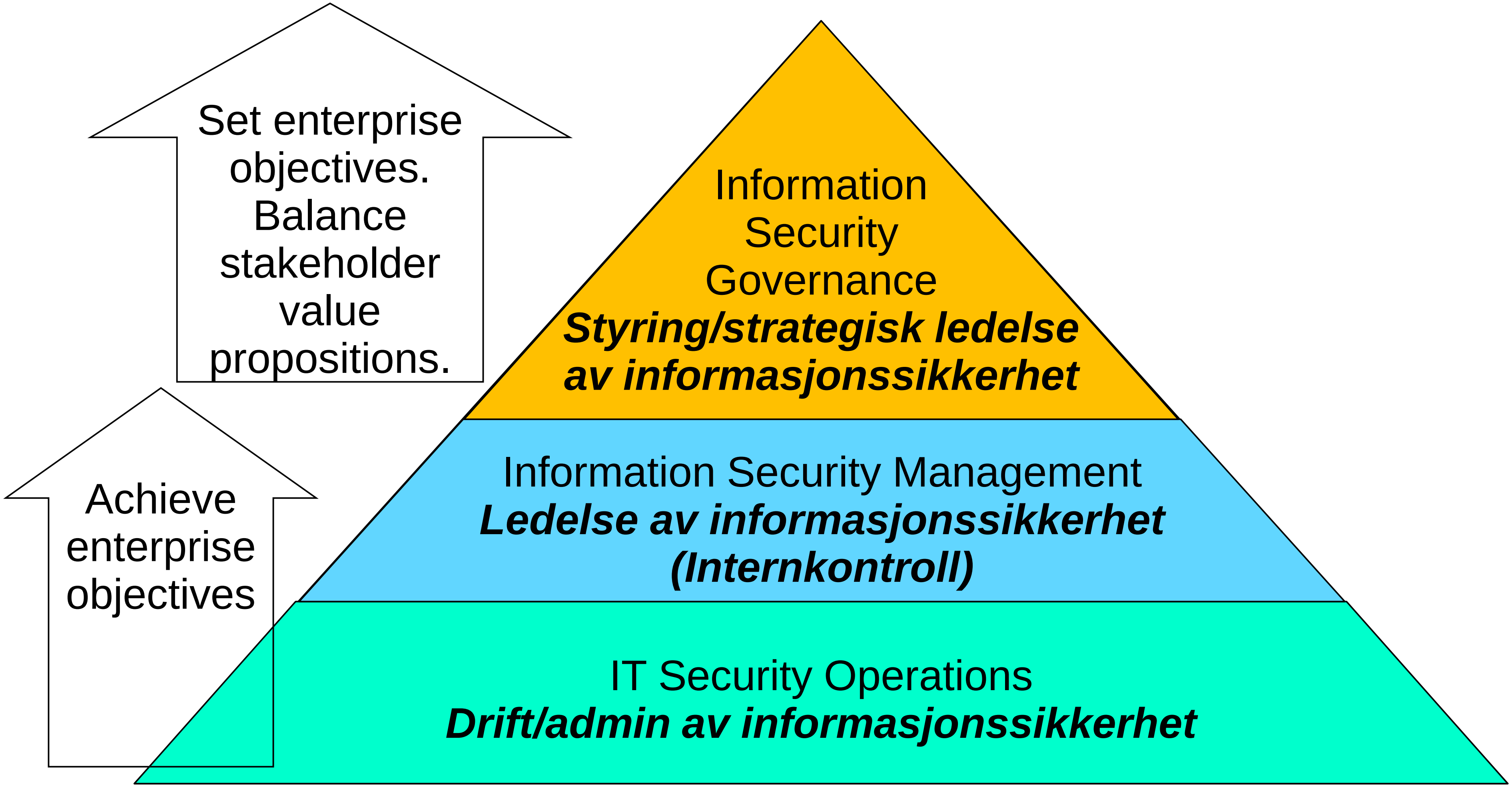
INF2120 Information Security

Lecture 05:
- Information Security Management
- Human Factors for Information Security

Audun Jøsang

University of Oslo, Autumn 2018

Security Management Levels



Set enterprise objectives. Balance stakeholder value propositions.

Achieve enterprise objectives

Information Security Governance
Styring/strategisk ledelse av informasjonssikkerhet

Information Security Management
Ledelse av informasjonssikkerhet (Internkontroll)

IT Security Operations
Drift/admin av informasjonssikkerhet

Information Security Governance
Styring/strategist ledelse av informasjonssikkerhet

> 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

Merk:

Begrepet: *“information security management”* oversettes offisielt til *“ledelse av informasjonssikkerhet”*. Vær oppmerksom på at frem til 2014 ble *“information security management”* oversatt til “*styring av informasjonssikkerhet*”, og at mange organisasjoner (f.eks. NSM) fortsetter med det.

Det særnorske begrepet *“internkontroll”* er omtrent ekvivalent med *“ledelse av informasjonsikkerhet”.*

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

Goals of information security governance as defined by COBIT and ISACA

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

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

ISACA - Mål for styring av IT-sikkerhet

1. Strategisk tilpasning av sikkerhetsprogrammet
   – IS-aktiviteter skal støtte organisasjonens helhetlige strategi.
2. Risikohåndtering
   – Avdekke trusler, sårbarheter og risiko. Deretter bruke adekvate virkemidler for å redusere risiko til et akseptabelt nivå.
3. Verdiskapning
   – Søk optimal balanse mellom reduksjon av risiko og tap, og kostnader forbundet med sikkerhetsvirkemidler.
4. Ressursbruk
   – Arbeidet med informasjonssikkerhet skal gjøres effektivt
5. Målbarhet
   – Effekten av sikkerhetsarbeidet skal måles

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

- Leaders understand security risks and get regular reviews

Leaders take responsibility

- Visible leaders who set clear goals and priorities

Risk-based priorities

- Tolerances to risk understood and established

Roles & responsibilities defined

- Clear segregation of duties

Information security management
Ledelse av informasjonssikkerhet (Internkontroll)

Includes:

- 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)
- Inventory and classification of resources and Information
- Threat and risk assessment
- Reporting and coordination with top level management
- Deployment and maintenance of security controls
- Security education and training
- Incident response and business continuity planning

Security Management

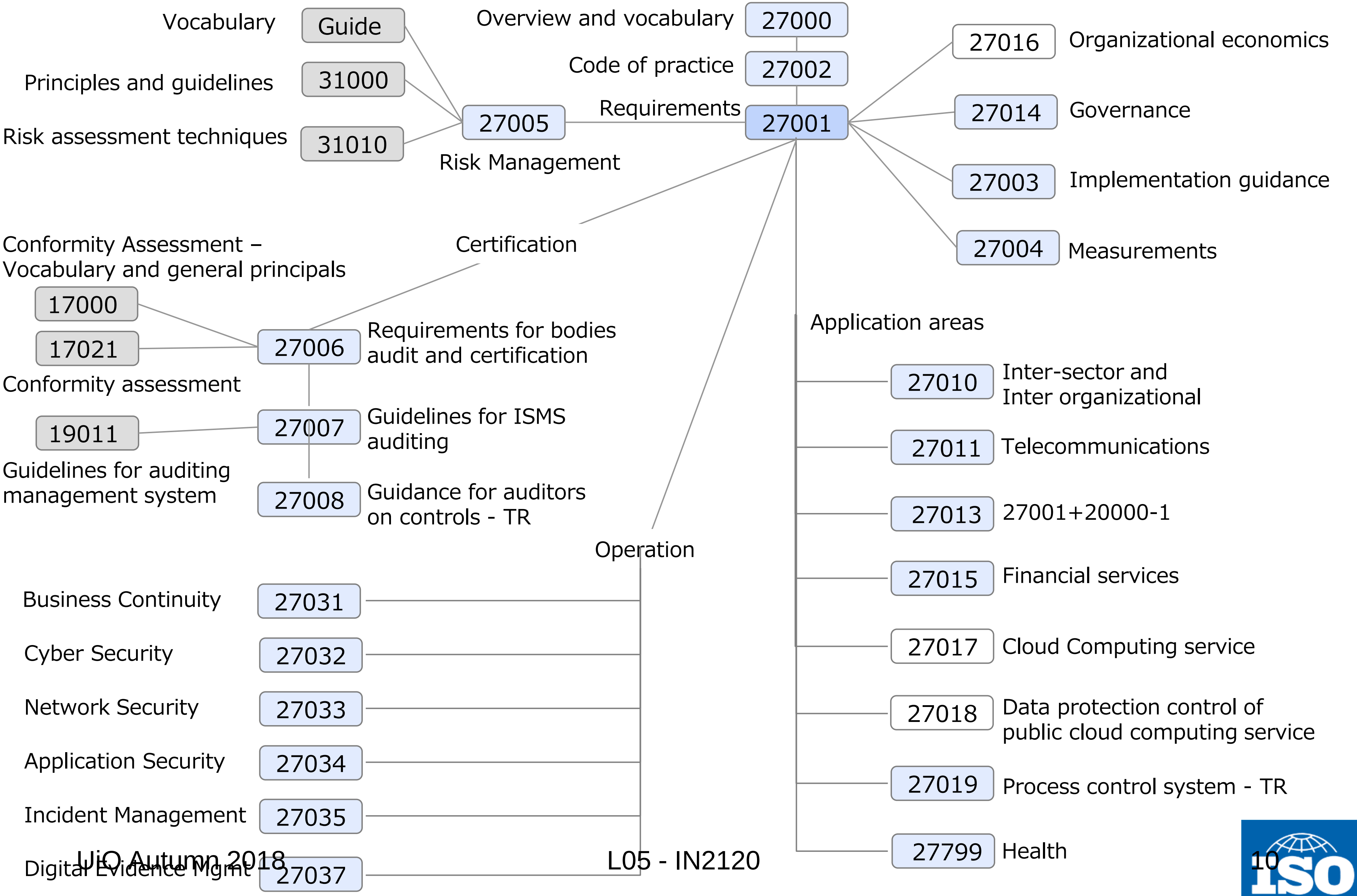
IS Management Standards

- 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
- Norge – NSM
  - Veileder i sikkerhetsstyring
  - Risikovurdering for sikring

https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

ISO/IEC 27000 family of standards and related standards

as of Oct. 2013



Evolution of ISO 27001 & 27002 Standards

- **1995**

BS 7799: Code of Practice for Information Security Management

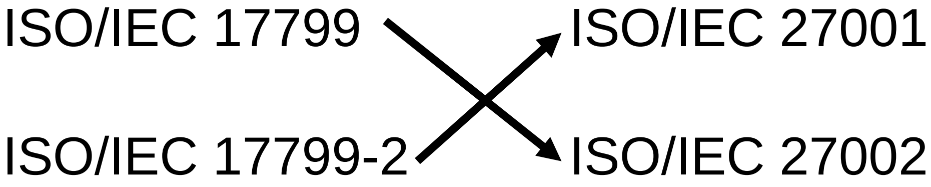
- **1999**

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

- **2013**

ISO Management Standards Alignment

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

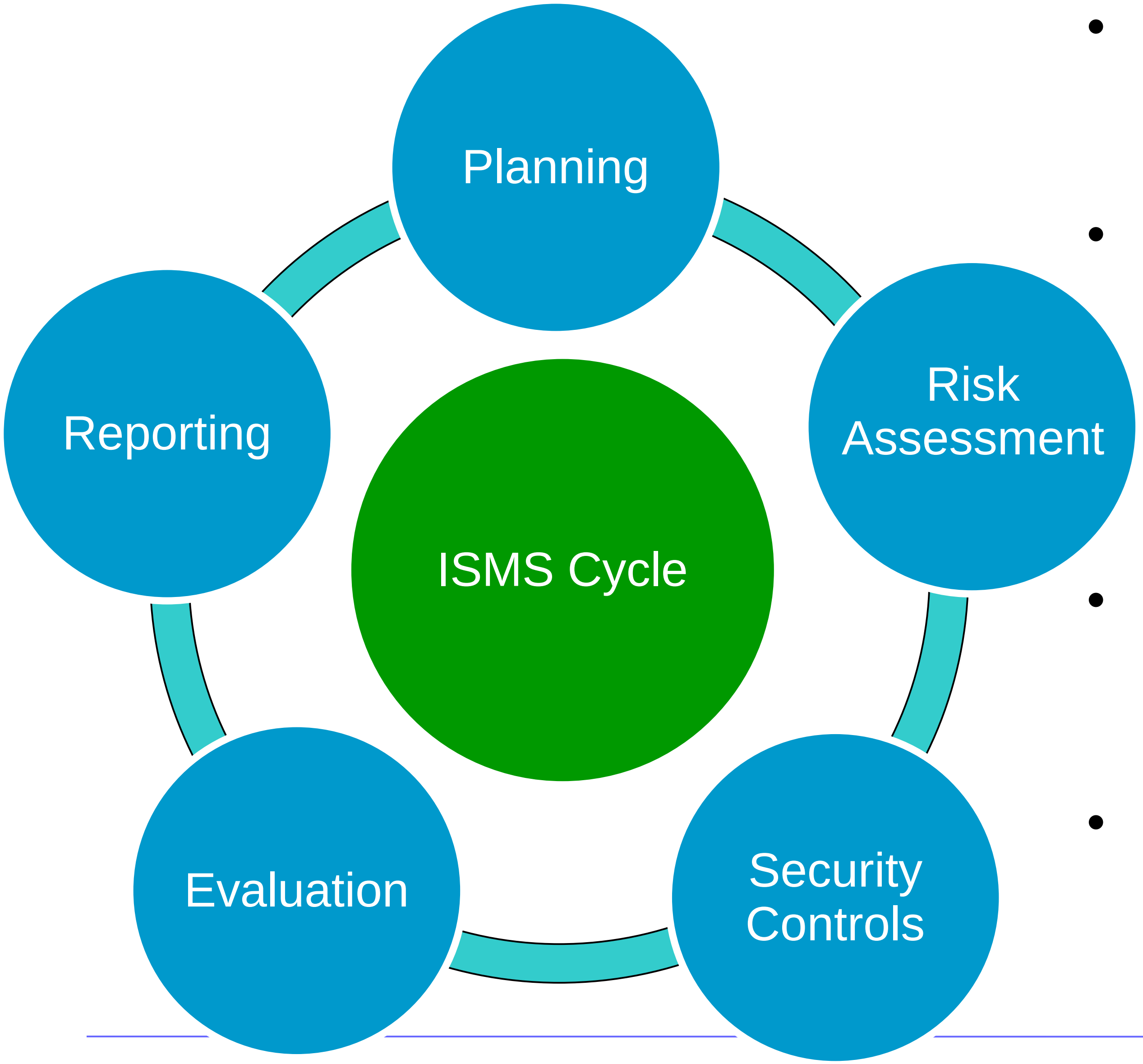
- **2018**

Major changes to ISO/IEC 27001: ISMS planned

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

IS Management System Cycle



- The ISMS cycle is an interpretation of ISMS (ISO 27001).
- Source: NSM (Nasjonal Sikkerhets-myndighet).
- The steps in the cycle are done in parallel.
- Good IS management requires that all steps are implemented

CISSP 7th Ed. IS Program Phases

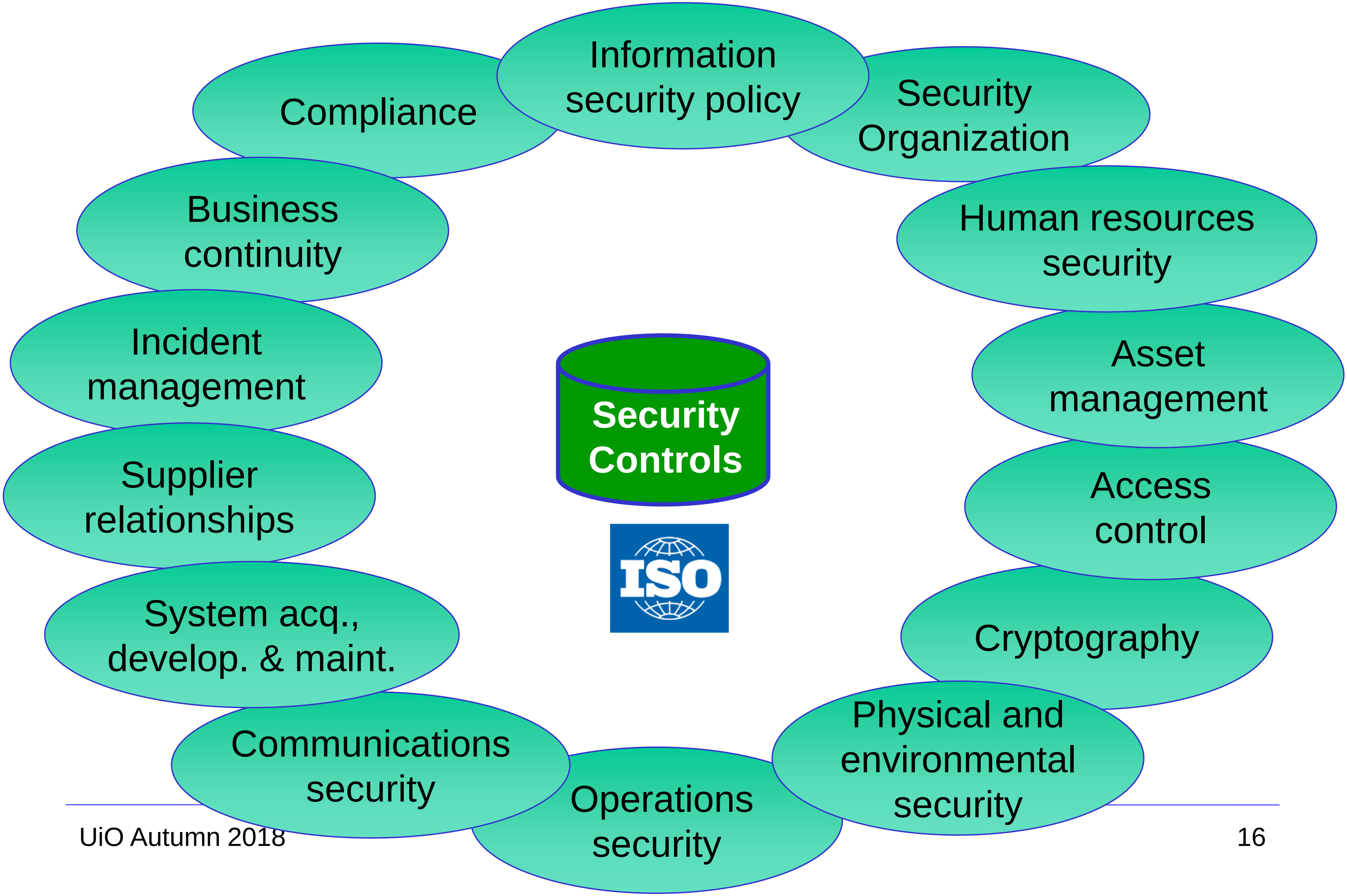
CISSP 7th Ed. (p.41) **IS program phases**	**Description**
1. Plan and organise	• Establish mgmt commitment and high level IS policy • Define roles and committees, • Assess threats, vulnerabilities and risk • Identify and plan security solutions and controls
2. Implement	• Assign roles and responsibilities • 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.

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).”

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 security

Communications security

System acq., develop. & maint.

Supplier relationships

Incident management

Business continuity

Compliance

Security Controls

ISO

20 CSC: Critical Security Controls

- Alternative to ISO/IEC 27002
- 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®

20 Critical Security Controls

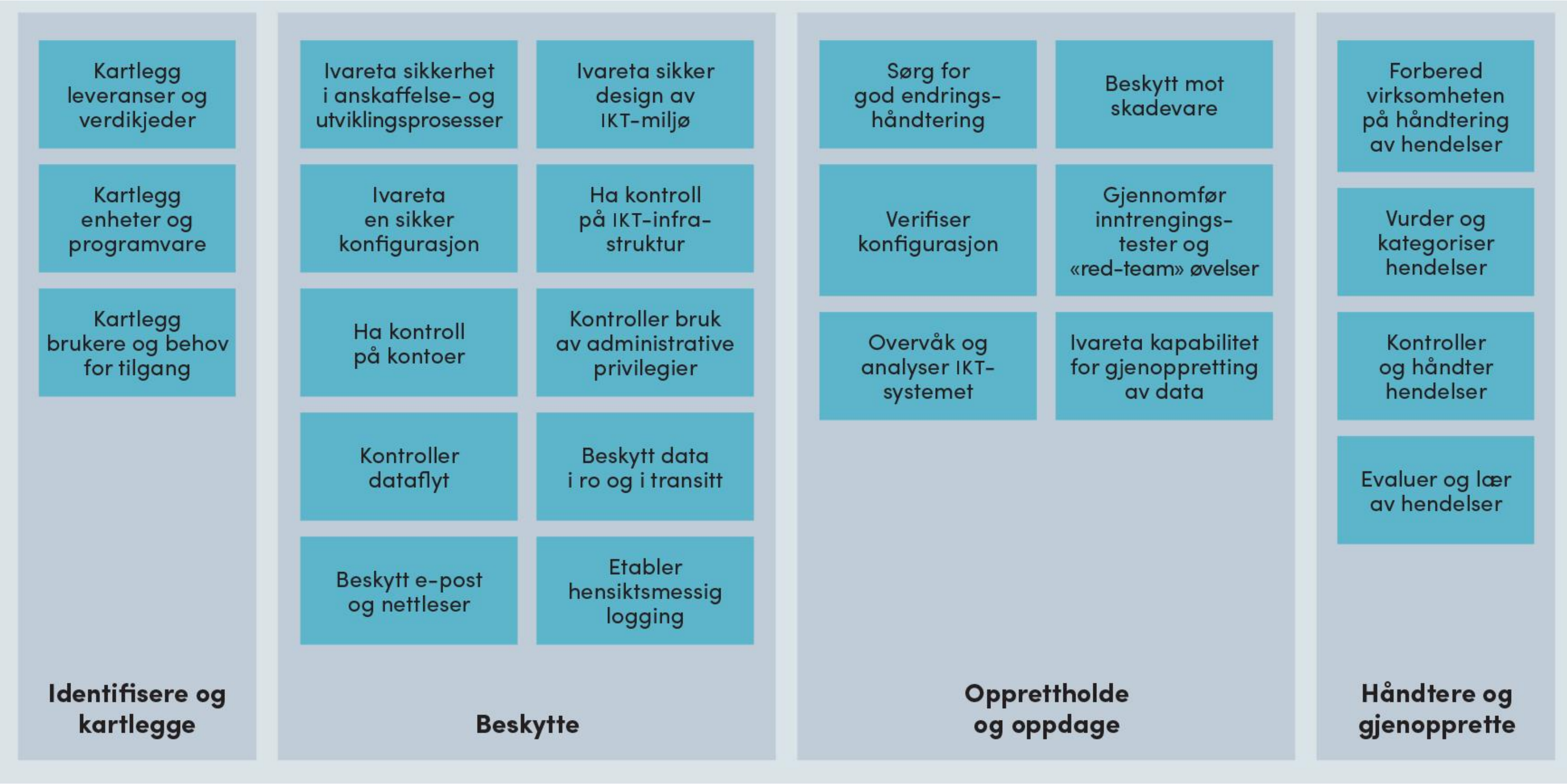
CIS Center for Internet Security®

- Inventory of Hardware
- Inventory of Software
- Continuous Vulnerability Management
- Control of Admin. Privileges
- Secure Configuration
- Analysis of Audit Logs
- Email and Browser Protections
- Malware Defences
- Control of Ports, Protocols and Services
- Data Recovery Capabilities
- Configuration of Firewalls, Routers, and Switches
- Boundary Defense
- Data Protection
- Need-to-know Access Control
- Wireless Access Control
- Account Control
- Security Awareness
- Application Security
- Incident Response
- Pentesting

Grunnprinsipper for IKT-sikkerhet

Oversettelse og sammendrag av ISO/IEC 27002

https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/



Identifisere og kartlegge

- Kartlegg leveranser og verdikjeder
- Kartlegg enheter og programvare
- Kartlegg brukere og behov for tilgang

Beskytte

- Ivareta sikkerhet i anskaffelse- og utviklingsprosesser
- Ivareta sikker design av IKT-miljø
- Ivareta en sikker konfigurasjon
- Ha kontroll på IKT-infra-struktur
- Ha kontroll på kontoer
- Kontroller bruk av administrative privilegier
- Kontroller dataflyt
- Beskytt data i ro og i transitt
- Beskytt e-post og nettleser
- Etabler hensiktsmessig logging

Opprettholde og oppdage

- Sørg for god endrings-håndtering
- Beskytt mot skadevare
- Verifiser konfigurasjon
- Gjennomfør inntrengings-tester og «red-team» øvelser
- Overvåk og analyser IKT-systemet
- Ivareta kapabilitet for gjenoppretting av data

Håndtere og gjenopprette

- Forbered virksomheten på håndtering av hendelser
- Vurder og kategoriser hendelser
- Kontroller og håndter hendelser
- Evaluer og lær av hendelser

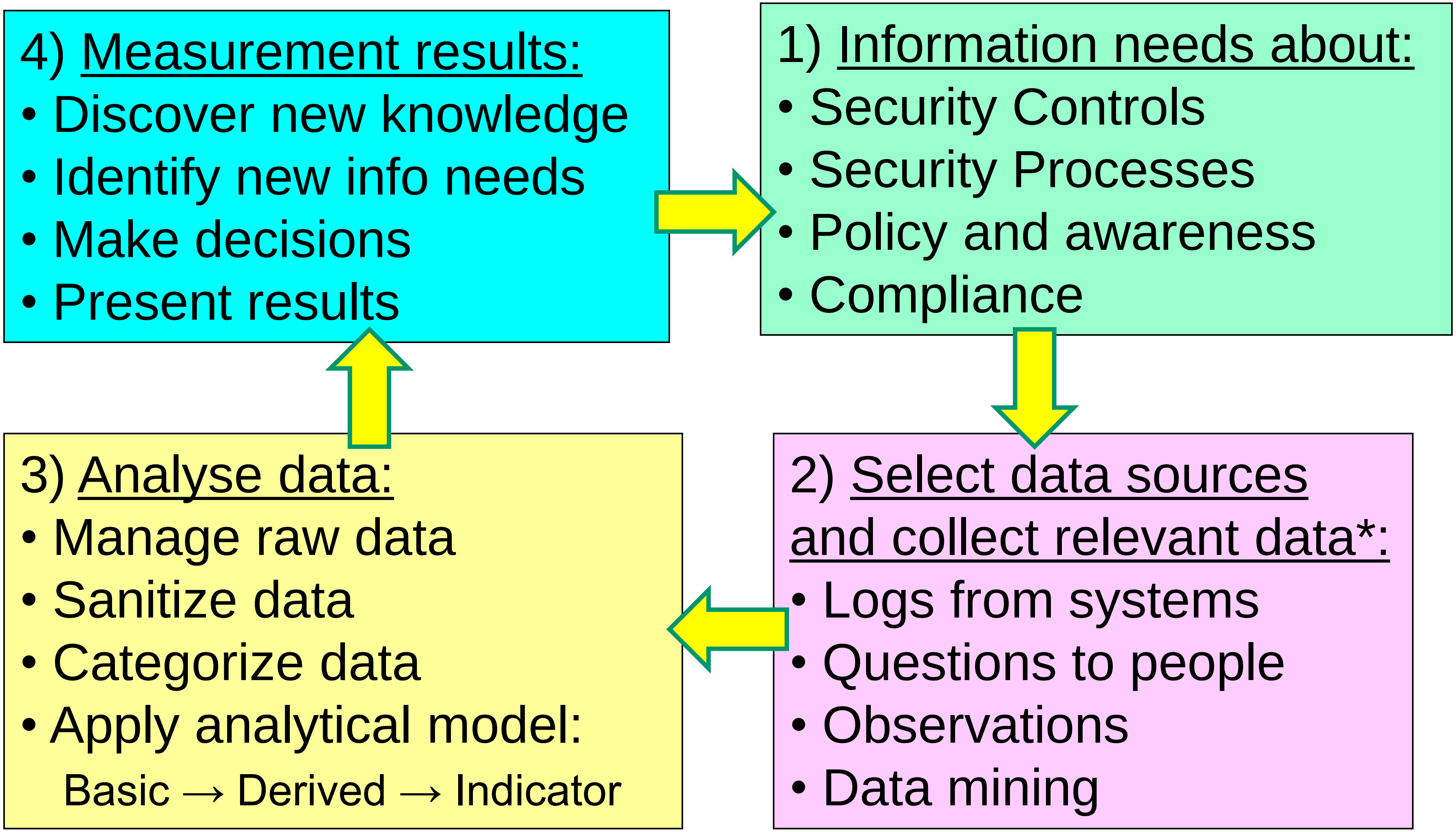
Evaluation of the ISMS through Security Measurements

- 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

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.”

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:

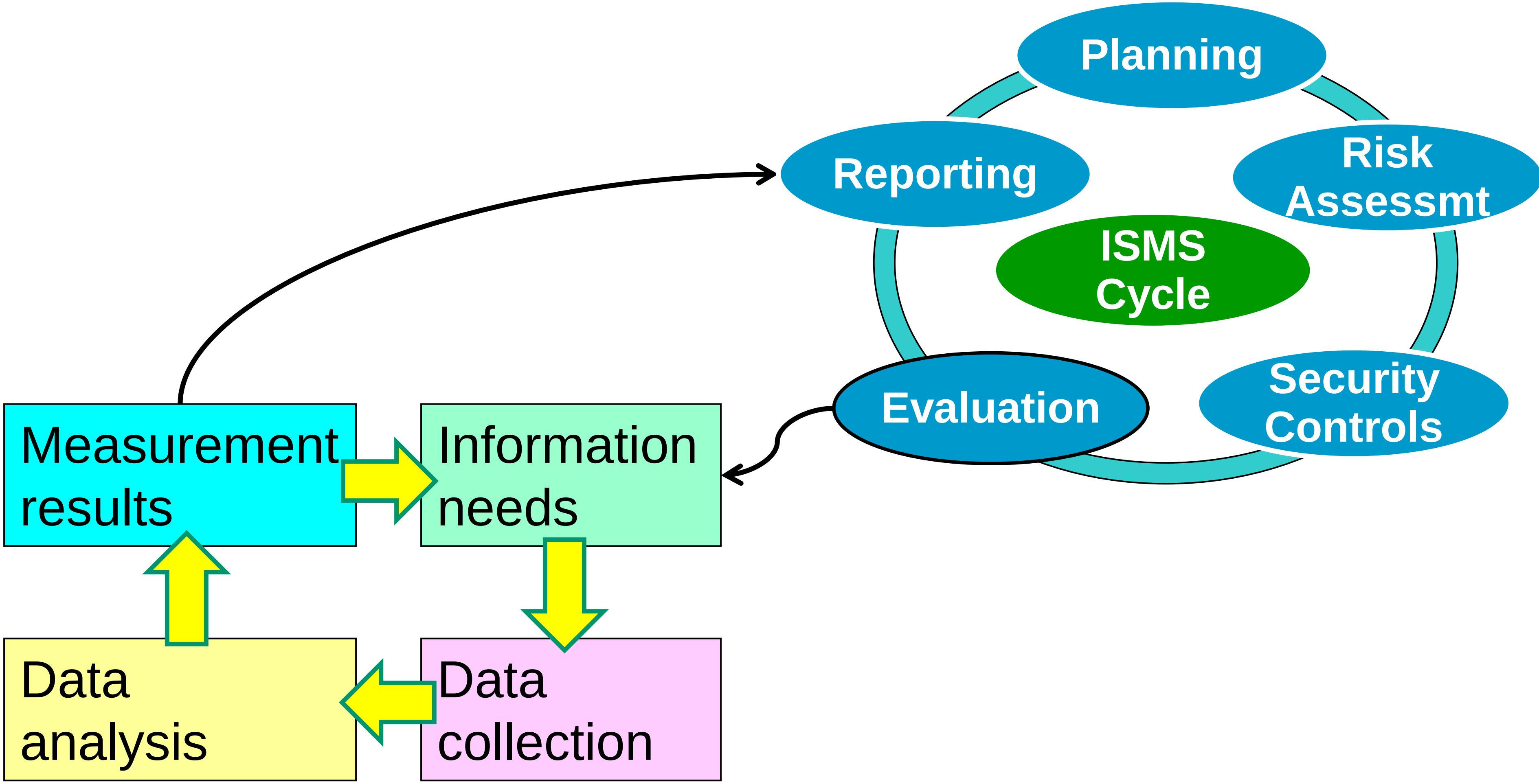
Basic → Derived → Indicator

4) Measurement results:

- Discover new knowledge
- Identify new info needs
- Make decisions
- Present results

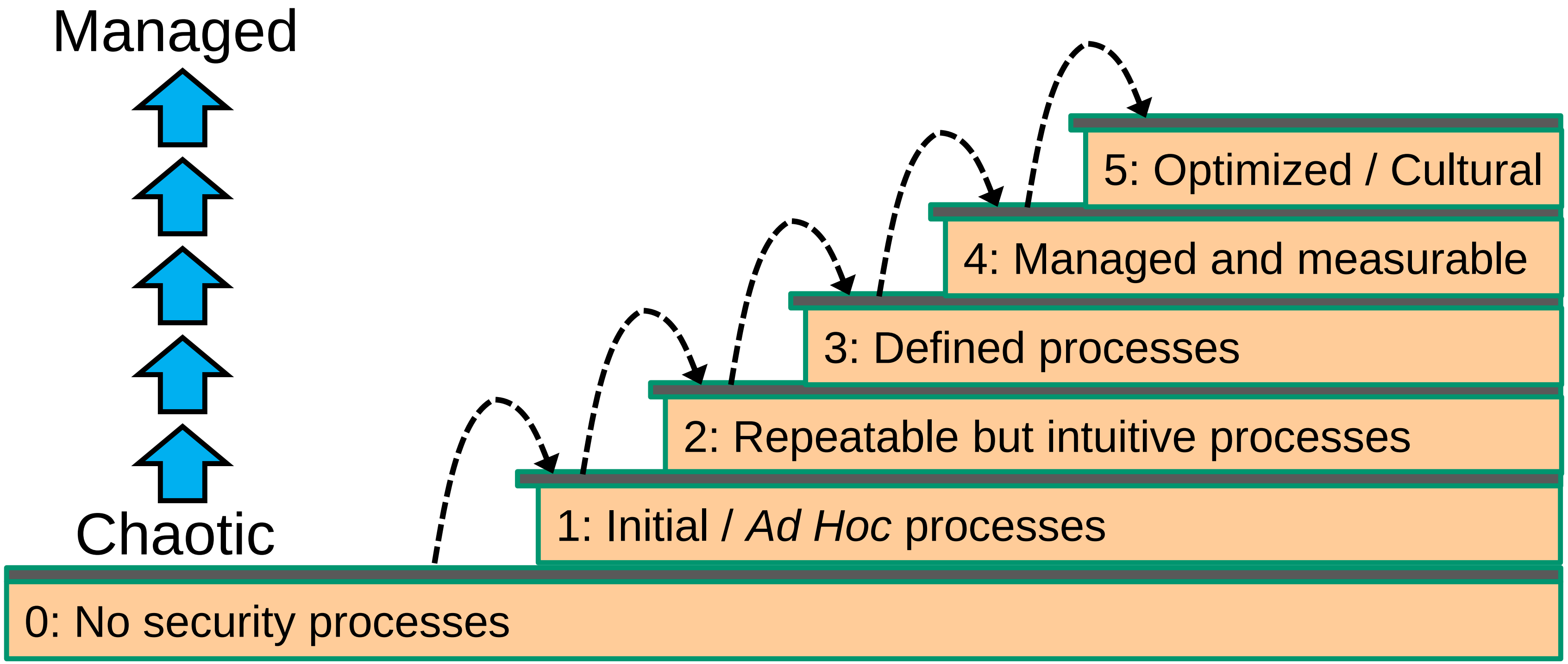
*) Called Objects of measurement in ISO 27004

Measurement – ISMS integration



CMMI
Capability Maturity Model Integration for Information Security Management

Considerable time and effort needed to reach each next level in the maturity model for IS management.


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

CMM levels 1 - 3

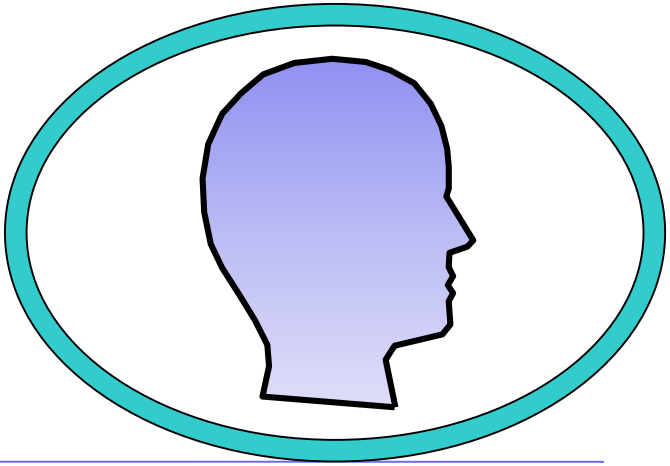
1. Initial / Ad Hoc
   - + Processes are ad-hoc and disorganised.
   - + Risks are considered on an ad hoc basis, but no formal processes exist.
2. Repeatable but intuitive
   - + Processes follow a regular pattern.
   - + Emerging understanding of risk and the need for security
3. Defined process
 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

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

The human factor in information security

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



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?

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 about insider threats
- Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO 2015)
  - https://www.nsr-org.no/krisino/
  - 28% of enterprises had experienced insider attacks.

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
- Always try to stay on good terms with staff.

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.
- Staff who lose their job due to redundancy are at greater risk to become insider attackers. To mitigate this risk:
  - The redundancy process must be seen as fair
  - Try to keep a good dialogue
  - … even with staff who feel being treated badly
- During exit interview, review the original employment agreement (i.e. non-compete, wrongful disclosure, etc.

Social engineering attacks

Where people are the defence

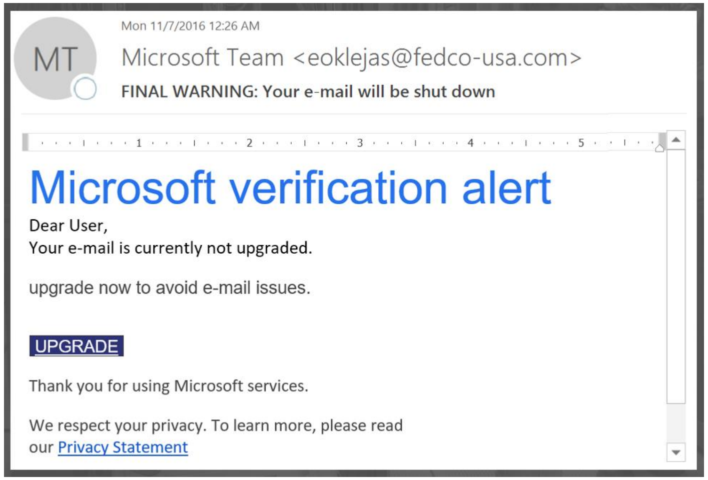
Social Engineering Attacks

- 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

Types of Social Engineering Attacks

- Technical Social-Engineering Attacks
  - Electronic contact with victims
  - Email, telephone, messaging, social networks, websites
  - Multi-channel attacks



Mon 11/7/2016 12:26 AM

Microsoft Team <eoklejas@fedco-usa.com>

FINAL WARNING: Your e-mail will be shut down

Microsoft verification alert

Dear User,
Your e-mail is currently not upgraded.

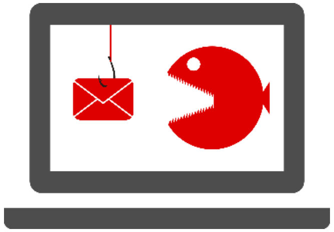
upgrade now to avoid e-mail issues.

Thank you for using Microsoft services.

We respect your privacy. To learn more, please read our Privacy Statement

- In-Person Social-Engineering Attacks
  - Manipulate people face-to-face in person
  - Convince victims to perform actions which compromise security
  - Open doors, give physical access, provide IT resources

Phishing Attacks



- A kind of social-engineering attack in which criminals use spoofed emails to trick people into sharing sensitive information or installing malware on their computer
- Phases
  1. Sending phishing email, getting through spam-filters, and landing in victim’s inbox
     - Increasingly difficult to get through email filtering (SPF, DKIM, DMARC)
     - Content must be sufficiently credible to trick the user
  2. The victim taking the suggested action in the message
     - Got to a fake website
     - Replying with sensitive information
     - Installing malware
  3. The criminals exploiting and monetizing the stolen information

Types of Phishing

- **Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- **Spear Phishing** – Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect
- **Whaling** – Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access
- **Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source

Detect a Phishing Scam

- Spelling errors (e.g., “passward”), lack of punctuation or poor grammar
- Hyperlinked URL differs from the one displayed, or it is hidden
- Threatening language that calls for immediate action
- Requests for personal information
- Announcement indicating you won a prize or lottery
- Requests for donations

- Be skeptical, use common sense

Protect Yourself → Refuse the Bait

- STOP. THINK. CONNECT.
  - Before you click, look for common baiting tactics, ask colleagues
- Be extremely careful about clicking on links in an email
  - User your computer mouse to hover over each link to verify its actual destination, even if the message appears to be from a trusted source
  - Pay attention to the URL and look for a variation in spelling or different domain (e.g., ndsu.edu vs. ndsu.com)
  - Consider navigating to familiar sites on your own instead of using links within messages
- Examine websites closely
  - Malicious websites may look identical to legitimate sites
  - Look for “https://” or a lock icon in the address bar before entering any sensitive information on a website

In case you took the bait:
Protect Yourself → Take Action Now

If you suspect that …	**You should…**
You interacted with, or replied to a phishing scam	→ Immediately contact your help desk, or other relevant entity.
You might have revealed or shared personal or financial information	→ Immediately change the password(s) for your account(s). If you use the same password for multiple accounts and sites, change it for each account. Do not reuse that password in the future. → Watch for signs of identity theft by reviewing your bank and credit card statements for unauthorized charges and activity. If you notice anything unusual, immediately contact your credit card or bank. → Consider reporting the attack to the police.

IN-PERSON SOCIAL ENGINEERING TACTICS

- Neuro-Linguistic Programming (NLP)
- Develop Trust
- Induce strong affect
- Information overload
- Reciprocation
- Diffusion of responsibility and moral duty
- Authority
- Commitment creep

SE Tactics:
Neuro-Linguistic Programming (NLP)

- Mirror their target’s body language
  - Match the voice, tone and body language of their victim.
  - Match the breathing rate, voice and vocabulary
  - Use common industry or company jargon
- Produces an affective connection with the target on a subconscious level
- Frequently used by salespeople to get clients to like them

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

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 loose your job”)
  - Confusion (contradictory statements)

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

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

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

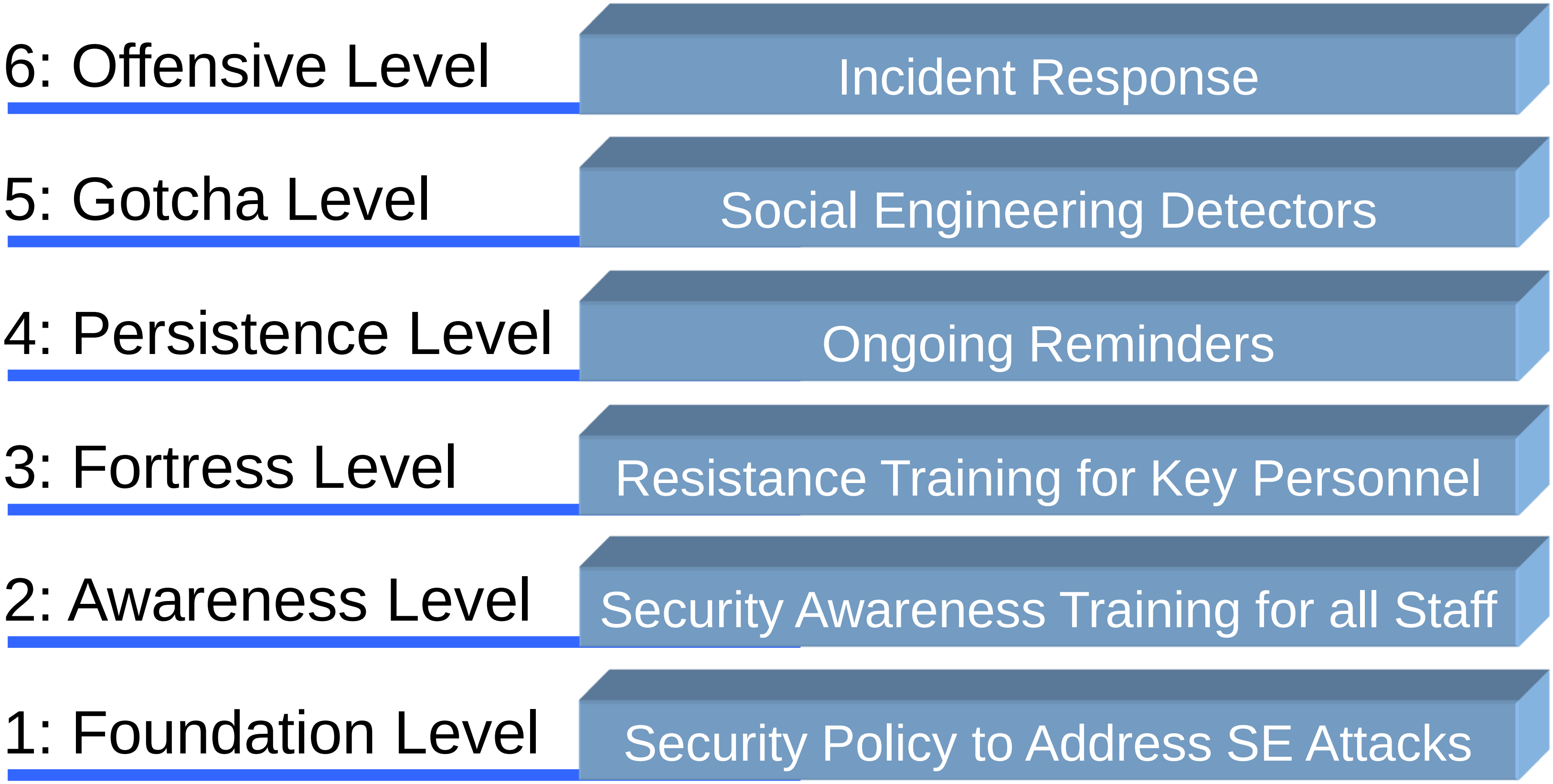
SE Tactics: Authority

- 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)

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

Multi-Level Defence against Social Engineering Attacks



6: Offensive Level	Incident Response
5: Gotcha Level	Social Engineering Detectors
4: Persistence Level	Ongoing Reminders
3: Fortress Level	Resistance Training for Key Personnel
2: Awareness Level	Security Awareness Training for all Staff
1: Foundation Level	Security Policy to Address SE Attacks

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

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

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

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,

SE Defence: Persistence

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

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

SE Defence: Offensive

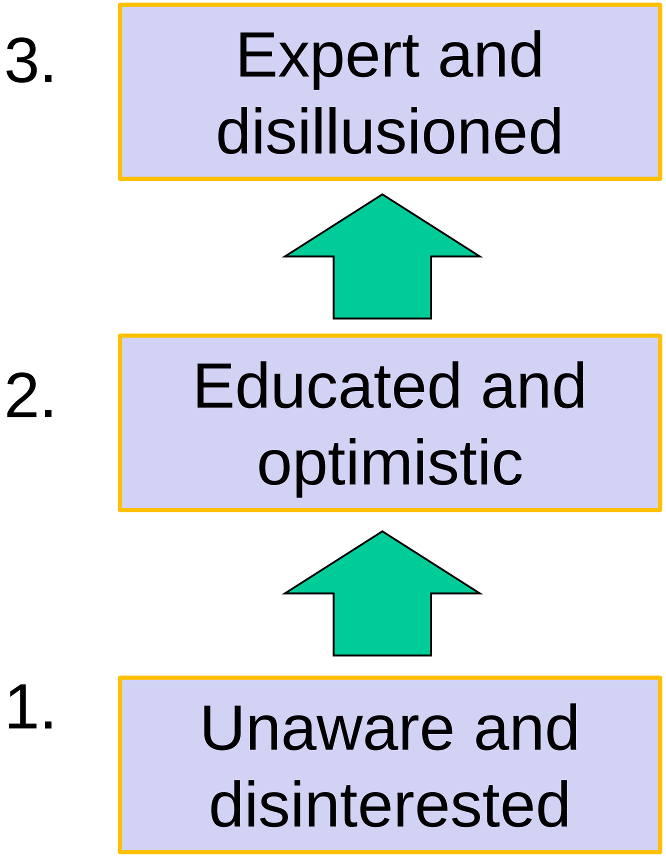
- Incident response
  - – Well defined process for reporting and reacting to
    - Possible SE attack events,
    - Cases of successful SE attacks
- Reaction should be vigilant and aggressive
  - – Go after SE attacker
  - – Proactively warn other potential victims

Security Usability

Security Learning

- Good and intuitive security metaphors facilitate learning
  - E.g.: “*digital signature”, “Trojan horse malware”*
- Bad metaphors can be misleading
  - E.g.: “*firewall”* ?, it would be better to say: “*checkpoint”*
- *Security usability* is different from traditional *usability*
  - You can’t use a system if you don’t know how to operate it.
  - You can still use a system even if you don’t know how to **securely** operate it.
- Security can not be made totally transparent to the user
  - The user must understand certain security concepts and be able to make informed security decisions.
- Security learning can be difficult
  - It takes time to thoroughly understand security

Stages of security learning
(Security is often more complex 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 realise that it can never be made totally secure.”*
- *“I understand it now, it’s simple, and I know how to make it totally secure”*
- *“I don’t understand it, and I don’t want to know about it. Why can’t security simply be transparent?”*

End of Lecture