ECOM6023

eFinancial Services

LECTURE 7:
Information Security for eFinancial Services

Dr. Juergen Rahmel 2020-21

HSBC Germany / Hong Kong
IETC Information Engineering – Teaching and Coaching Ltd.

L7 – Information Security

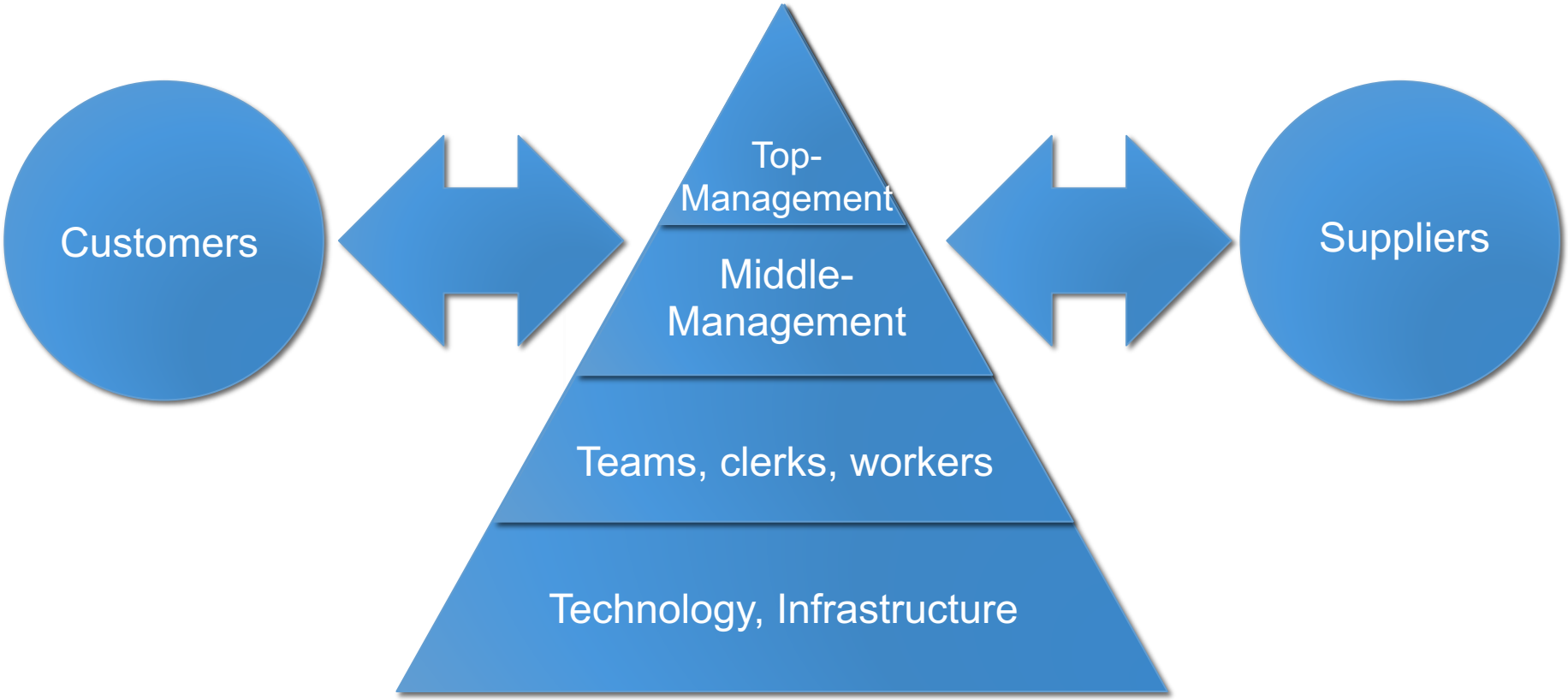
Topics

- **Introduction**
- The three targets of Information Security
- Data Protection
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - ISO 27001/2
  - PCI SSC / PCI DSS
- Summary

L7 - Information Security

Introduction

Where does Information Security happen for a company?



L7 - Information Security

Introduction

Words of caution:

„We have to stop looking for the magic preventive technology that will avoid the threats, and embrace processes that will help us manage the risks“

(Bruce Schneier)

Thus:

We can do a lot for Information Security and risk prevention.

But the result will never be 100%.

The key insight every manager needs to develop:

- Strike a balance between **proactive** and **reactive** mechanisms

This balance is specific for every company / business / industry

L7 - Information Security

Introduction

This overview lecture aims to have a '**Coaching-Character**':

- Nothing of the content is rocket science
- Nothing (hopefully) is far away from common sense
- The lecture shall clarify the scope and methods of Information Security and Risk
- After the lecture, you should see clearer
  - what topics might be relevant for you, your role / department / company
  - who the many stakeholders of Information Security are
  - Which effects a security function should have in your environment
  - How risk management works and what the components of the overall risk are

- Thus: YOU will be able to assess, evaluate and decide

L7 – Information Security

Topics

- Introduction
- **The three targets of Information Security**
- Data Protection
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - ISO 27001/2
  - PCI SSC / PCI DSS
- Summary

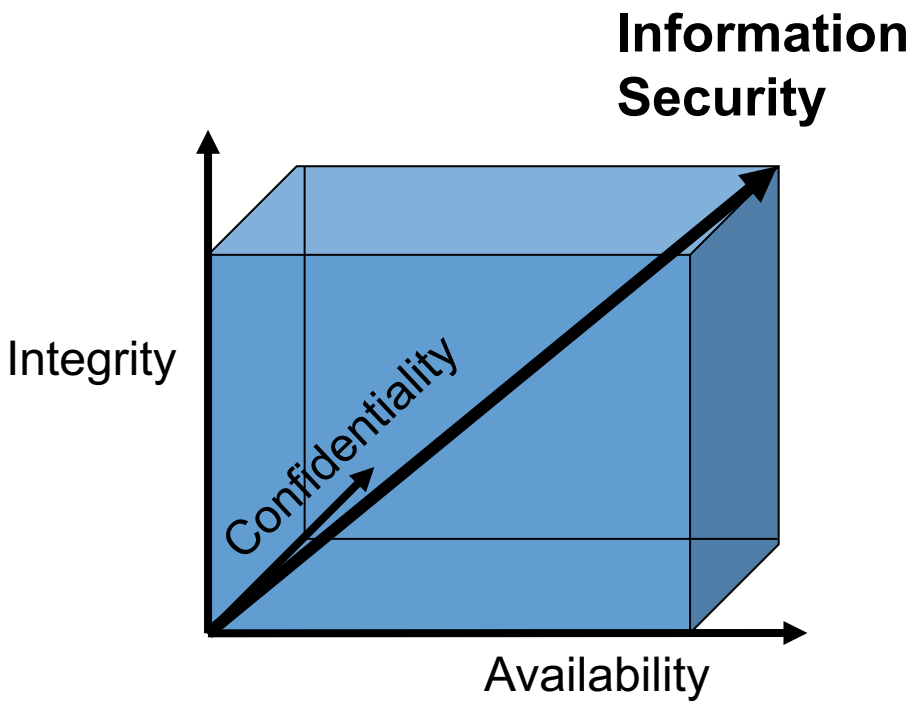
L7 - Information Security

Information Security - CIA

Information Security targets the protection of

- **C** onfidentiality
- **I** ntegrity
- **A** vailability

of data and systems



L7 - Information Security

Information Security - CIA

Three Key Terms:

- Confidentiality
  - Accessibility to data and information is granted only for authorized people/entities with the need and the right to access
- Integrity
  - Data is correct, complete, and comprehensible/reproducible
- Availability
  - Accessibility of data, information and applications is given whenever there is a demand to do so

L7 - Information Security

Information Security - CIA

Other concepts are

- Reliability
  - of applications, systems
- Stability
  - of hardware, infrastructure
- Nonrepudiability
  - of eMails, orders, …
- Accountability….

But the required ideas are already contained in the three components of Information security

L7 - Information Security

Information Security - CIA

Examples:

- Identity theft
- Lost data (is it really lost??)
- Web site alterations
- outages
- ….other examples?

L7 – Information Security

Topics

- Introduction
- The three targets of Information Security
- **Data Protection**
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - ISO 27001/2
  - PCI SSC / PCI DSS
- Summary

L7 - Information Security

Data Protection, Privacy

Data Protection and Privacy

- The target of Data Protection / Data Privacy is not the security of data
- Target is, to protect the right of self-determination of an individual
- Data Privacy law in many countries demand companies establish specific privacy controls to protect the rights of users, customers, employees

L7 - Information Security

Data Protection, Privacy

8 common privacy controls:

- Physical Access control
  - Restricts the physical access to Hardware / Systems on which personal data is processed to those who have the granted right to do so
- Application Access control
  - Restricts the access to computer applications with which personal data is processed to those who have the granted right to do so
- Data Access Control
  - Ensures that users can only access personal data for which they are granted the right within a system or application
- Data transfer control, to ensure that
  - (i) it can be monitored and determined, to which entities/systems personal data can be transferred and
  - (ii) the unauthorized read/copy/change or delete access to personal data during transfer is prevented
- Input Control
  - Ensures that it can ex-post be verified and determined which personal data has been entered when into the systems and by whom.

L7 - Information Security

Data Protection, Privacy

8 common privacy controls, cont'd:

- Outsourcing control
  - Ensures that personal data which is processed on contractual basis can only be processed according to the instructions of the Outsourcer
- Availability Control
  - Ensures that personal data is protected against accidental deletion or destruction
- Purpose Segregation Control
  - Ensures that personal data gathered for different purposes can be processed separately

L7 - Information Security

Data Protection, Privacy

HK: Personal Data Ordinance - Six Data Protection Principles:

- **DPP1:** personal data shall be collected for a purpose directly related to a function and activity of the data user; lawful and fair collection of adequate data; data subjects shall be informed of the purpose for which the data are collected and to be used.
- **DPP2:** all practicable steps shall be taken to ensure the accuracy of personal data; data shall be deleted upon fulfillment of the purpose for which the data are used.
- **DPP3:** unless the data subject has given prior consent, personal data shall be used for the purpose for which they were originally collected or a directly related purpose.
- **DPP4**: all practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure.
- **DPP5**: formulates and provides policies and practices in relation to personal data
- **DPP6:** individuals have rights of access to and correction of their personal data. Data users should comply with data access or data correction request within the time limit, unless reasons for rejection prescribed in the Ordinance are applicable.

L7 – Information Security

Topics

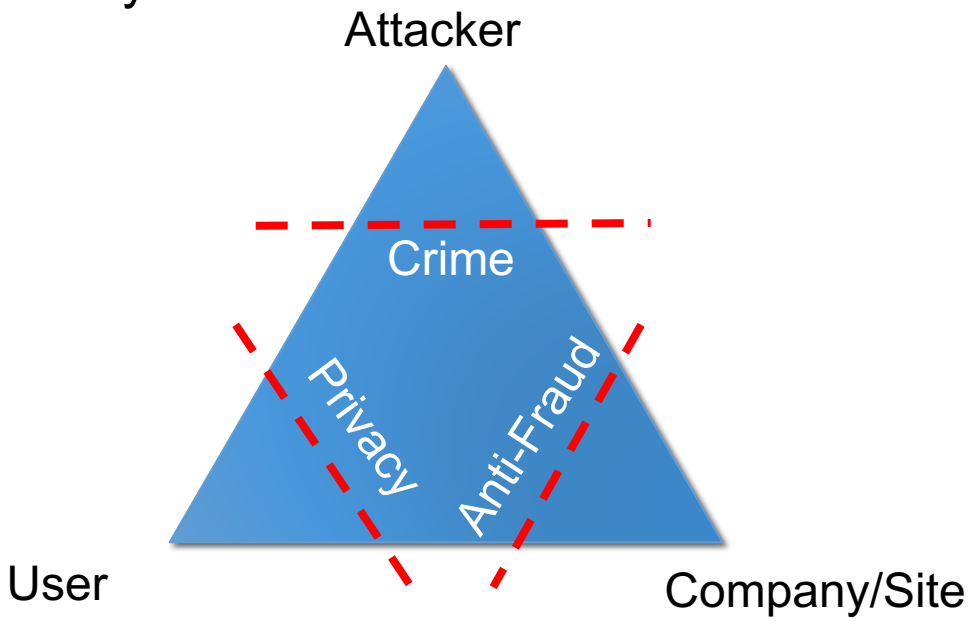
- Introduction
- The three targets of Information Security
- Data Protection
- **Psychonomics of Security**
  - **Psychology of security**
  - **Economics of security**
- Information Security Management
  - ISO 27001/2
  - PCI SSC / PCI DSS
- Summary

L7 - Information Security

Psychology of Security

What drives our perception and inclination towards security and security mechanisms?

the triangle of Security:



L7 - Information Security

Psychology of Security

Authority - Some historic experiments:

The Milgram Experiment:

- People are asked to execute electrical shocks in an experimental setting, with a strong person playing the ‘teacher’/’professor’
- the person subjected to the shock is demonstrating severe pain
- the persons executing the shocks showed strong obedience to the ‘authority’ of the leading person in the professor-role

The Stanford prison experiment

- Students were divided into ‘guards’ and ‘prisoners’ for a role play
- the experiment had to be stopped due to the extreme brutality exhibited by the ‘guards’

L7 - Information Security

Psychology of Security

Authority - Some historic experiments:

The experiments show the strong role that ‘authority’ plays in many contexts.

Social engineering is a security attack that tries to exploit this fact:

- the attacker is investigating the circumstances and will assume a position of authority, i.e impersonate an officer, an administrator, a bank clerk etc.
- many common people fall into the trap and do not question this authority or this position

L7 - Information Security

Economics of Security

What drives Security?

- Who is interested in Security?
- Who is benefitting from Security?

What inhibits Security?

- Who has the cost of Security?
- Who has the knowledge?
- Who represents the risk?

Much of this chapter follows ideas and papers by Ross Anderson and Tyler Moore.

L7 - Information Security

Economics of Security

A shift in perspective:

- The first Security concern were the malicious outsiders
  - Cryptography is used to keep them out
- The second Security concern are the selfish insiders
  - approaches like game theory and microeconomics are used to model their behaviour

L7 - Information Security

Economics of Security

Security as a (side) effect

consider a medieval city:

- if every family secures a part of the city wall, the defense depends on the laziest family
- if disputes with attackers are fought out by the best skilled fighters, the safety depends on the best knight in town
- if a war is a matter of attrition, then the outcome depends on all citizens efforts together

L7 - Information Security

Economics of Security

Security as a (side) effect

consider a Software company:

- a security vulnerability might be introduced by the most careless programmer
- the chance of finding it before deployment depends on the sum of all testers efforts
- the overall resilience of the system depends on the individual skill of the security architect

L7 - Information Security

Economics of Security

Security as a mass distribution factor

- The more people use a service, the more valuable it becomes
- The more programmers write software for a platform, the higher the distribution ratio for this platform will be.

Consequences:

- there is a tendency to ‘the winner takes all’ results, i.e. dominant platforms arise after a period of market battle
- companies who want to win this battle need to attract programmers and users
- this leads to inherently insecure systems, as security is perceived as inconvenience and therefore is an inhibitor for mass distribution of new platforms

L7 - Information Security

Economics of Security

Security as a mass distribution factor

The paradox consequences:

- established platform tend to have more and higher security restrictions, less flexibility and tighter user control

- Reason is, that once the market dominance is established, tighter security helps supporting the lock-in effect
- Security and controls are ‘abused’ to maintain the dominant position

L7 - Information Security

Economics of Security

Security problems – disclose or cover up ?

Does publication of security vulnerabilities help …

- the crooks, as they can go on to exploit unpatched systems
- vendors, as they have the public to help finding issues in their Software
- the users, as the products become safer, since vendors fear the transparency of the market?

Or should vulnerabilities be kept secret to avoid large debate and the multitude of potential attackers?

what is your opinion?

L7 - Information Security

Economics of Security

Security efforts – effectiveness proven by certificates?

What do certificates prove?

- that a company has spent considerable effort and money to get all processes right and secure?
- that a company has spent considerable effort and money to have an independent party assert the security level
- or even …. both?

Research in 2006 showed that overall about 3% of the websites were malicious, but from those with certificates, about 8% were malicious.

L7 - Information Security

Economics of Security

Security – Economics of privacy

The effectiveness of privacy laws is unclear for many countries

- which country's law is to apply – the website operator's, the user's, the website host's?

Technology has made collection of personal data easier and more beneficial for companies.

However, there also exists a 'privacy gap', i.e. a difference between stated and revealed privacy

L7 - Information Security

Economics of Security

Security – Economics of privacy

An experiment:

- a questionnaire to measure students' privacy preferences was designed, asking embarrassing questions.
- the questionnaire was presented in three different settings to three different groups:
  - one group answered under neutral university conditions
  - a second group answered the same questions after having read a detailed privacy policy, ensuring strongly their data being treated with utmost care
  - a third group answered on a nonuniversity website, with a 'how BAD are you?' theme and no privacy at all.
- paradoxically, group 2 answered fewer questions than group 1, group 3 answered more questions than group 1

L7 – Information Security

Topics

- Introduction
- The three targets of Information Security
- Data Protection
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - **ISO 27001/2**
  - PCI SSC / PCI DSS
- Summary

L7 - Information Security

Information Security Management

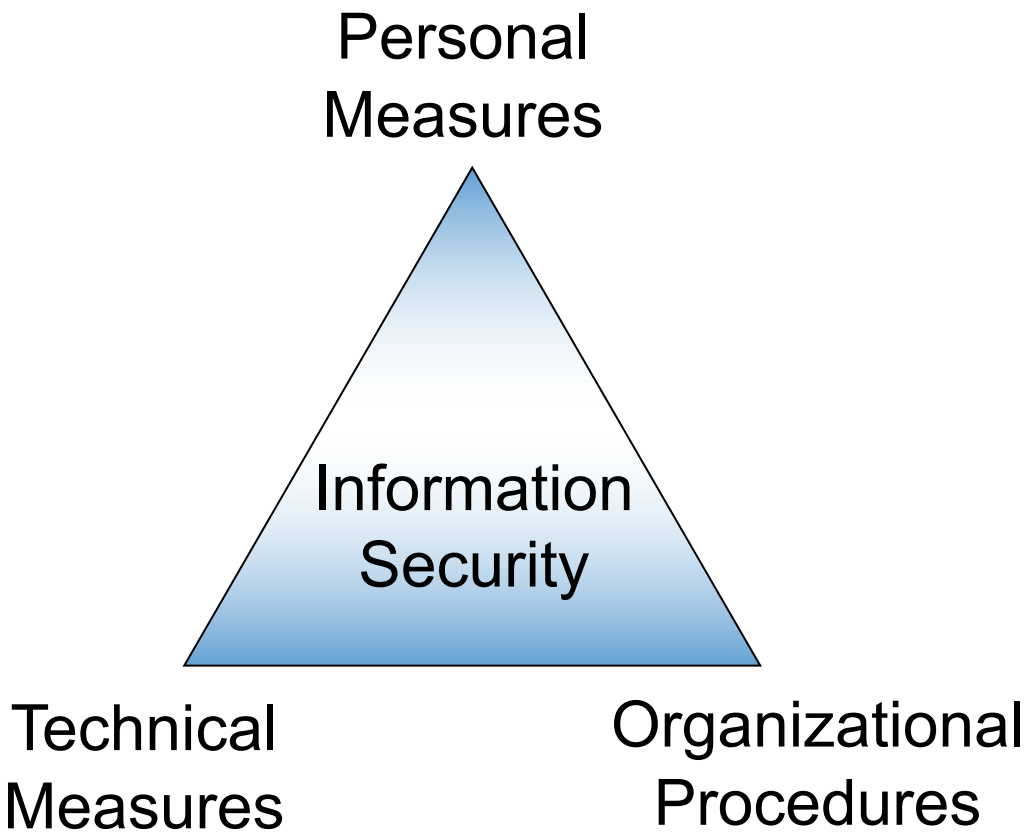
Questions:

- What objectives do you think Security Management needs to achieve?
  - find categories to differentiate types of objectives
- What is needed in an organisation to make Security management effective?
  - find the roles and responsibilities that are required to be set up
  - find other organisational measures are needed to achieve the objectives

L7 - Information Security

Information Security Management

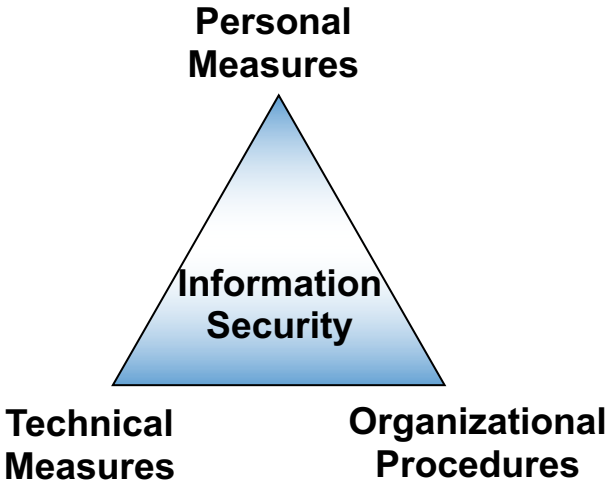
Information Security as an internal function covers three major areas



L7 - Information Security

Information Security Management

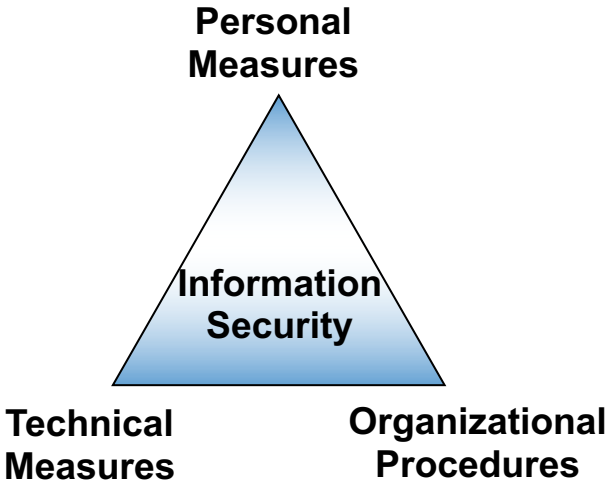
- Technical Measures, e.g.
  - Securing Data transfers
  - Securing company networks
  - Detecting attacks from outside the network
  - Virus scanners (PC, Server, eMail, Web)
  - Encryption techniques
  - Digital signatures
  - Monitoring data traffic outbound



L7 - Information Security

Information Security Management

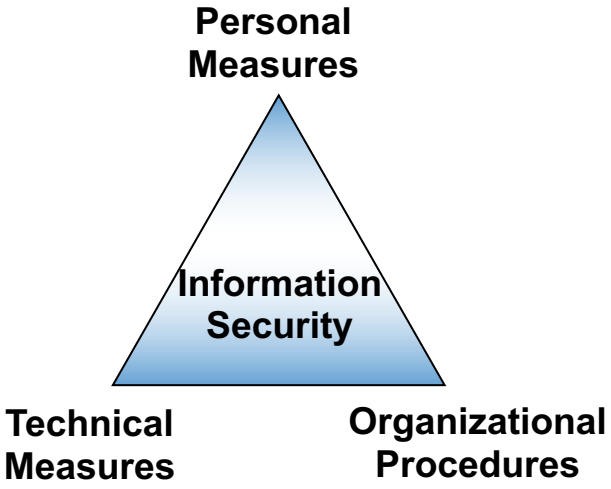
- Organizational Procedures, e.g.
  - Definition of access controls
  - Administration of User Accounts
  - Monitoring of system logs
  - Documentation of Guidelines
  - Software development methods
  - Maintenance of development and test environments
  - Requirements towards customers and Providers
  - Auditing of controls and procedures



L7 - Information Security

Information Security Management

- Personal Measures, e.g.
  - Ensure Confidentiality of data
    - On the phone, printer, fax
    - When sending eMails
    - When leaving the work place
  - Ensure Availability of systems
    - Lock up laptops
    - Delete suspicious eMails
    - Report incidents immediately
  - Ensure Integrity
    - Keep own password secret
    - Follow the rules, procedures, guidelines



L7 - Information Security

Information Security Management

Especially in banking and financial context, Information Security needs to be a process that is

- Supported by management
- Divided into clear roles and responsibilities
- Oriented on industry best practices
- Based on company specific requirements
- Supported by sufficient resources (heads, $)
- Audited to be effective
- Adapted, when correction is needed

A process oriented approach to managing Information Security can be certified.

L7 - Information Security

Information Security Management – ISO Norms

- Information Security Management Systems (ISMS) have a certain history of standardization attempts
- Origins mostly in UK (BS=British Standard)
- Others: “Code of Practice”

- Later: merge national Standards into ISO Norms
- For ISMS: the ISO 2700x family of standards

L7 - Information Security

Information Security Management – ISO Norms

The 2700x Family of Norms

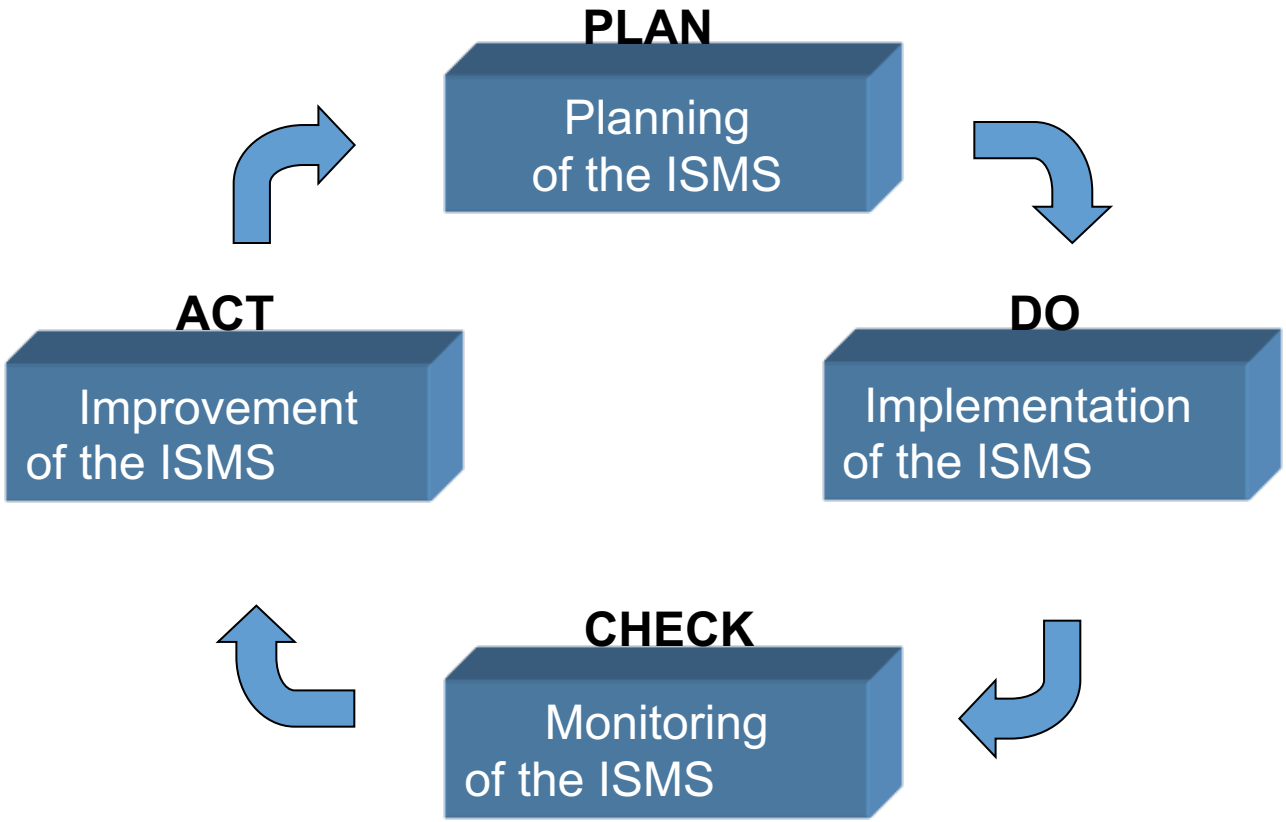
- ISO 27000:2013 Overview and Vocabulary of ISMS
- ISO 27001:2005 Requirements for ISMS (based on BS7799-2)
- ISO 27002:2005 Code of Practice for ISM (based on ISO 17799)
- ISO 27003:2010 ISMS Implementation Guide
- ISO 27004:2009 ISM Measurement
- ISO 27005:2011 IS Risk Mgmt (based on ISO 13335/BS 7799-3)
- ISO 27006:2011 Requirements for ISMS Auditing Bodies
- ISO 27007:2011 Guidelines for ISMS Auditing
- ISO 27008:2011 Guidelines for Auditors on IS controls

- ISO 27031 IT Readiness for Business Continuity

L7 - Information Security

Information Security Management – ISO 27001

ISO 27001: Process orientation of ISMS



L7 - Information Security

Information Security Management – ISO 27001

Target of the norm

- Provide a frame work for an effective ISMS
- make ISMS a strategic decision within an organisation
- Provide a way to define an ISMS, depending on
  - profile, targets and processes of a business
  - the resulting security requirements
  - size and structure of an organisation
- Determine the capability of an organisation to
  - gather its own security requirements
  - fulfill demands of customers and business partners
  - fulfill other regulatory or contractual requirements

L7 - Information Security

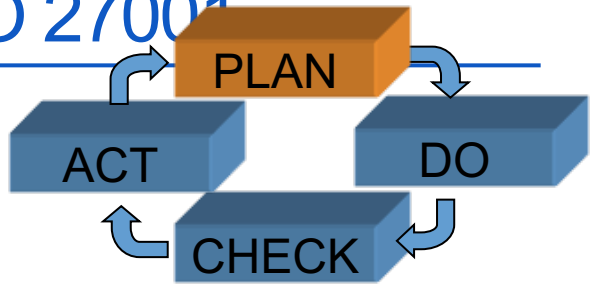
Information Security Management – ISO 27001

Depth of Requirements in the norm

- Requirements are formulated in generic terms, in order to be applicable for any company, independent of type, size, processes etc.
- Mandatory requirements are the ones in Chapters 4-8
- Recommended controls – as referred to in Annex A and detailed in ISO 27002 – can be tailored according to the specific demands of the company

L7 - Information Security

Information Security Management – ISO 27001

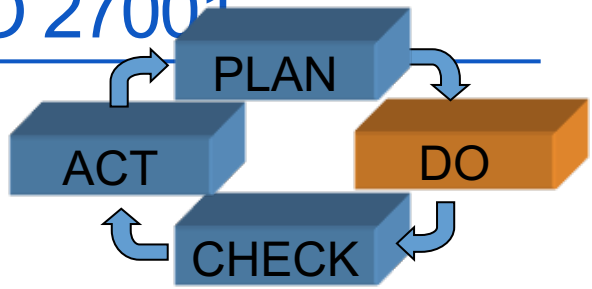


Ch 4 - Establish the ISMS (PDCA: Plan)

- Define scope and boundaries of the ISMS
- Define an ISMS policy
- Define the risk assessment approach of the organization
- Identify the risks, Analyse and evaluate the risks
- Identify and evaluate options for the treatment of risks.
- Select control objectives and controls for the treatment of risks, Prepare a “Statement of Applicability”
- Obtain management approval of the proposed residual risks
- Obtain management authorization to implement and operate the ISMS

L7 - Information Security

Information Security Management – ISO 27001

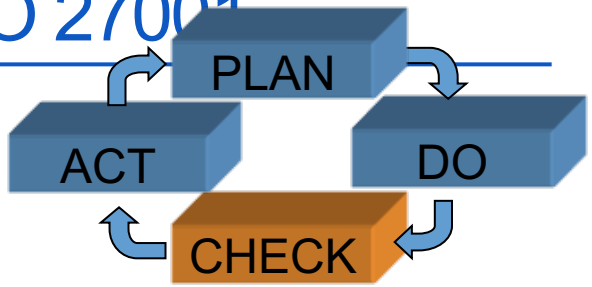


Ch 4 - Implement and operate the ISMS

- Formulate a risk treatment plan
- Implement the risk treatment plan in order to achieve the identified control objectives, Implement controls
- Define how to measure the effectiveness of the controls
- specify how to assess control effectiveness
- Implement training and awareness programmes
- Manage operation and resources of the ISMS.
- Implement procedures and other controls that enable prompt detection of security events and response to security incidents

L7 - Information Security

Information Security Management – ISO 27001

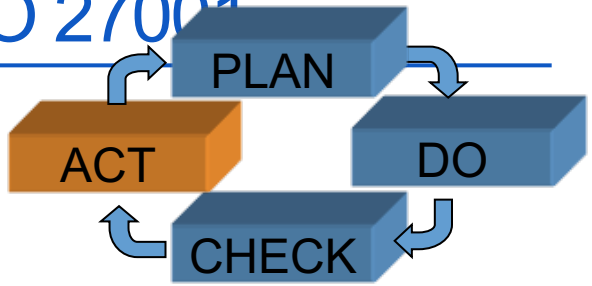


Ch 4 - Monitor and review the ISMS

- Execute monitoring and reviewing procedures
- Undertake regular reviews of the effectiveness of the ISMS
- Measure the effectiveness of controls
- Review risk assessments and residual/acceptable risks
- Conduct internal ISMS audits at planned intervals
- Undertake a management review of the ISMS
- Update security plans to take into account the findings of monitoring and reviewing activities
- Record actions and events that could have an impact on the effectiveness of the ISMS

L7 - Information Security

Information Security Management – ISO 27001



Ch 4 - Maintain and improve the ISMS

- Implement the identified improvements
- Take appropriate corrective and preventive action
- Apply the lessons learnt from the security experiences of other organizations and those of the organization itself
- Communicate the actions and improvements to all interested parties, agree on how to proceed
- Ensure that the improvements achieve their intended objectives

L7 - Information Security

Information Security Management – ISO 27001

Ch 5 - Management responsibility

- Management commitment
  - establishing an ISMS policy; establishing roles and responsibilities
  - ensuring that ISMS objectives and plans are established
  - communicating to the organization
  - providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS
  - deciding the criteria for accepting risks and the acceptable levels of risk
  - ensuring internal ISMS audits and management reviews are conducted
- Resource management
  - Provision of resources for all aspects of maintaining and improving
  - Training, awareness and competence

L7 - Information Security

Information Security Management – ISO 27001

Ch 6 - Internal ISMS audits

- The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:
  - conform to the requirements of this International Standard and relevant legislation or regulations
  - conform to the identified information security requirements
  - are effectively implemented and maintained and
  - perform as expected

L7 - Information Security

Information Security Management – ISO 27001

Ch 7 - Management review of the ISMS

- Management shall regularly review the organization's ISMS
  - ensure its continuing suitability, adequacy and effectiveness
  - assessing opportunities for improvement
  - results of the reviews shall be documented and records maintained
- Inputs include
  - results of ISMS audits / reviews; status of preventive/corrective actions
  - feedback from interested parties;
  - techniques, products or procedures to improve the ISMS
  - performance and effectiveness;
- Outputs include
  - Any decision that is required for resources and improvement

L7 - Information Security

Information Security Management – ISO 27001

Ch 8 - ISMS improvement

- Continual improvement
  - information security policy, information security objectives,
  - audit results, analysis of monitored events,
  - corrective and preventive actions and
  - management review
- Corrective action
  - eliminate the cause of nonconformities with the ISMS requirements
- Preventive action
  - determine action to eliminate the cause of potential nonconformities
  - implementing preventive action needed;
  - recording results of action taken

L7 - Information Security

Information Security Management – ISO 27001

a simplified perspective:

- Say what you do
  - Write down the procedures and guidelines
- Do what you say
  - Follow the rules
- Record what you do
  - Keep documentation (as specified by your procedures);
- Prove (to yourself and others) that you did it
  - Verify results by comparing documentation of target and results
- Improve it
  - Act on the differences

?

L7 - Information Security

Information Security Management – ISO 27001

Chapter 4 is the anchor for Audits and Certifications

- Documentation required for
  - The IS Policy and ISMS itself
    - plus the scope, i.e. for which company parts, business processes
  - the statement of applicability, i.e. the security controls chosen
    - plus the way and results of measuring and monitoring them
  - a method of keeping records for the control measurements
    - plus the required set of records proving the execution
  - the risk assessment methodology
    - plus the results in applying it
  - a document classification system
    - plus procedures to consistently apply according to the classification

L7 - Information Security

Information Security Management – ISO 27002

Aim of the Norm ISO 27002 is to provide

- practical guidelines to achieve a comprehensive and complete framework for IS Security in a company
- a security objective for each area of concern
- detailed security controls and guidance on implementation

- a basis for cross-company development of security guidelines, standards and efficient security practices

ISO 27002 by itself is not applicable for certification

but it delivers much of the content that is required

L7 - Information Security

Information Security Management – ISO 27002

Main chapters of ISO 27002:

5	SECURITY POLICY
6	ORGANIZATION OF INFORMATION SECURITY
7	ASSET MANAGEMENT
8	HUMAN RESOURCES SECURITY
9	PHYSICAL AND ENVIRONMENTAL SECURITY
10	COMMUNICATIONS AND OPERATIONS MGMT
11	ACCESS CONTROL
12	INF. SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
13	INFORMATION SECURITY INCIDENT MANAGEMENT
14	BUSINESS CONTINUITY MANAGEMENT
15	COMPLIANCE

L7 - Information Security

Information Security Management – ISO 27002

The chapter structure of ISO 27002:

8 Human resources security

8.1 Prior to employment[3]

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.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

8.1.1 Roles and responsibilities

Control

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

Implementation guidance

Security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization's information security policies (see 5.1);

b) protect assets from unauthorized access, disclosure, modification, destruction or interference;

c) execute particular security processes or activities;

d) ensure responsibility is assigned to the individual for actions taken;

L7 - Information Security

Information Security Management – ISO 27002

The norms ISO 2700x can not be freely distributed, they are licensed material.

But: Bryant University is referring to the norms ISO 27001/2 on their Standards page:

http://infosec.bryant.edu/standards.html

take a look ! (and grab it while it's there…you might need it ...)

L7 – Information Security

Topics

- Introduction
- The three targets of Information Security
- Data Protection
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - ISO 27001/2
  - **PCI SSC / PCI DSS**
- Summary

L7 - Information Security

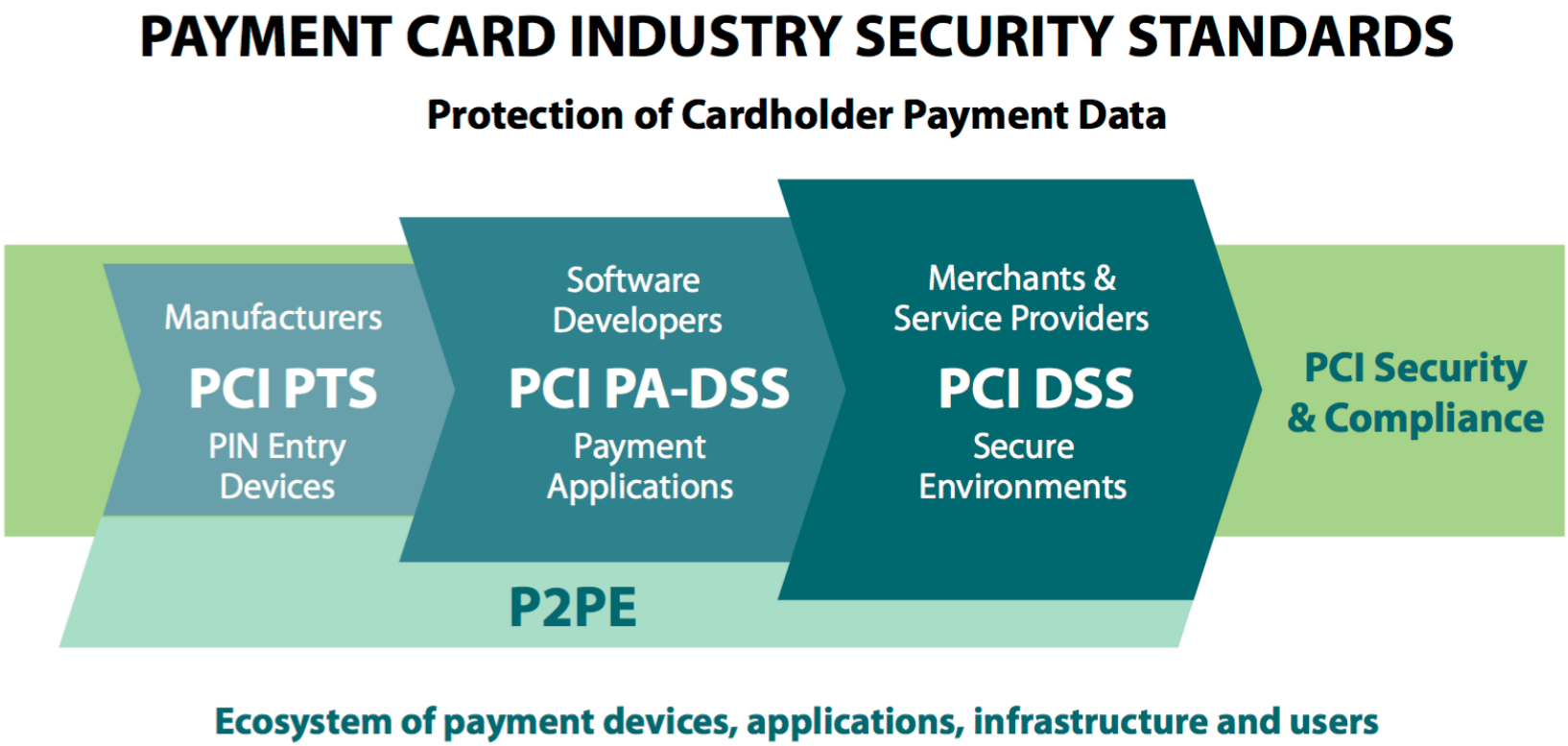
Information Security – PCI Security Standards

- The Payment Card Industry (PCI) Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data.
- The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions.
- The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.

L7 - Information Security

Information Security – PCI Security Standards

- from the Quick Reference Guide:



L7 - Information Security

Information Security – PCI Security Standards

- PCI Security Standards Include:
  - PCI Data Security Standard (PCI DSS)
  - PIN Transaction Security (PTS) Requirements
  - Payment Application Data Security Standard (PA-DSS)
  - PCI Point-to-Point Encryption Standard (P2PE)

- PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

L7 - Information Security

Information Security – PCI Security Standards

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

L7 - Information Security

Information Security – PCI Security Standards

- The PCI SSC sets the PCI Security Standards, but each payment card brand has its own program for compliance, validation levels and enforcement.
- Compliance Assessment can be done by:
  - Qualified Assessors
    - The Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualfied Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are approved by the Council to assess compliance with the PCI DSS. ASVs are approved by the Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers.
  - Self-Assessment Questionnaire
    - The Self-Assessment Questionnaire (SAQ) is a validation tool for eligible organizations who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC).

L7 – Information Security

Topics

- Introduction
- The three targets of Information Security
- Data Protection
- Psychonomics of Security
  - Psychology of security
  - Economics of security
- Information Security Management
  - ISO 27001/2
  - PCI SSC / PCI DSS
- **Summary**

L7 - Information Security

Information Security – Summary

Information Security is much more than ‘Viruses and Worms’, much more than just firewall-protection of user devices.

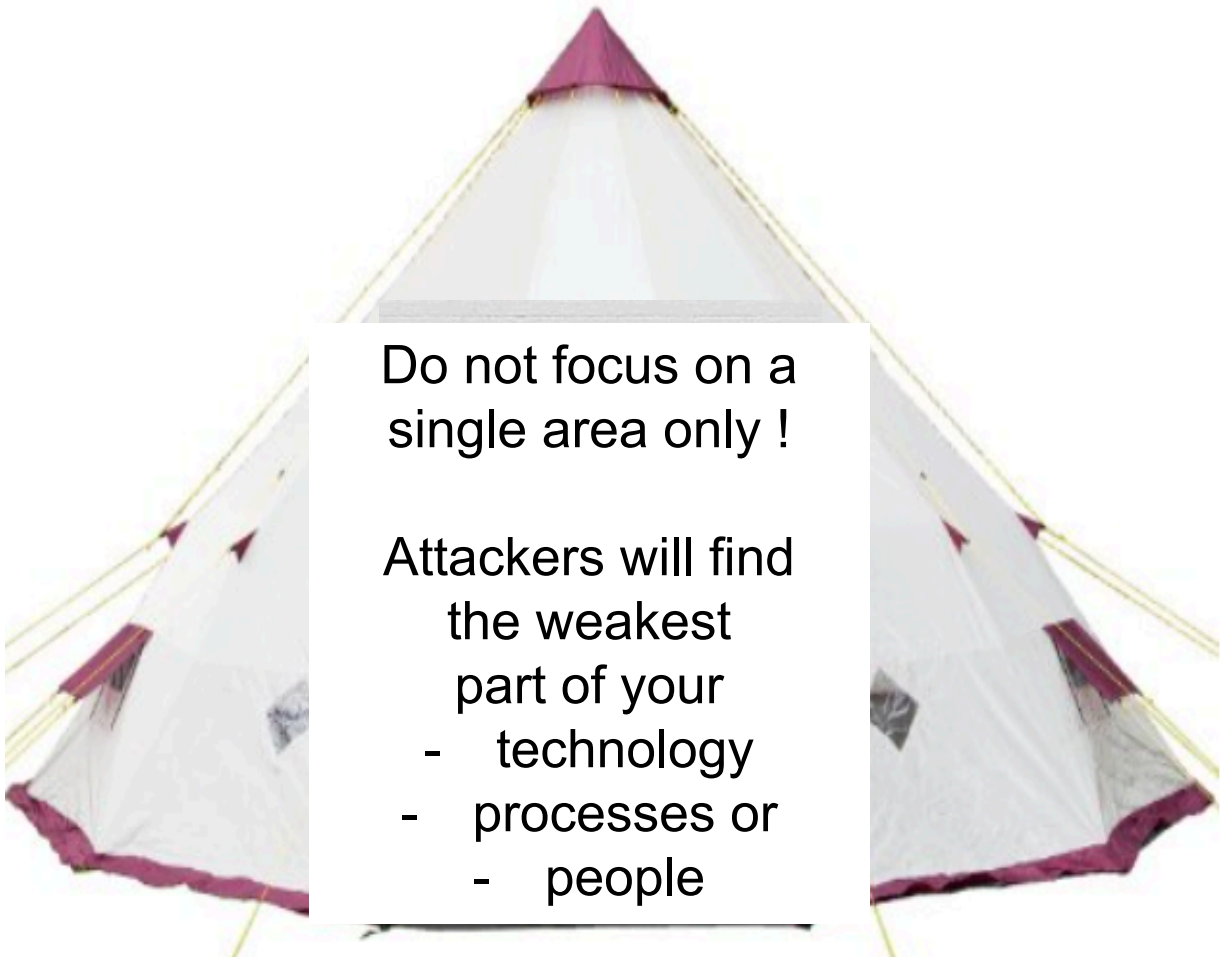
- Information Security encompasses:
  - Technology
    - attempting to set new/higher hurdles until the attackers can overcome them
  - Processes
    - attempting to instill the right guidelines and best practices into a company / organization
  - Behaviour
    - attempting to create knowledge and adoption of the personal behaviour required
- Information Security is influenced by
  - expectations and perceptions (of users and providers)
  - economical considerations and incentives

L7 - Information Security

Information Security – Summary

Information Security requires all protection areas to be considered and properly covered

otherwise:



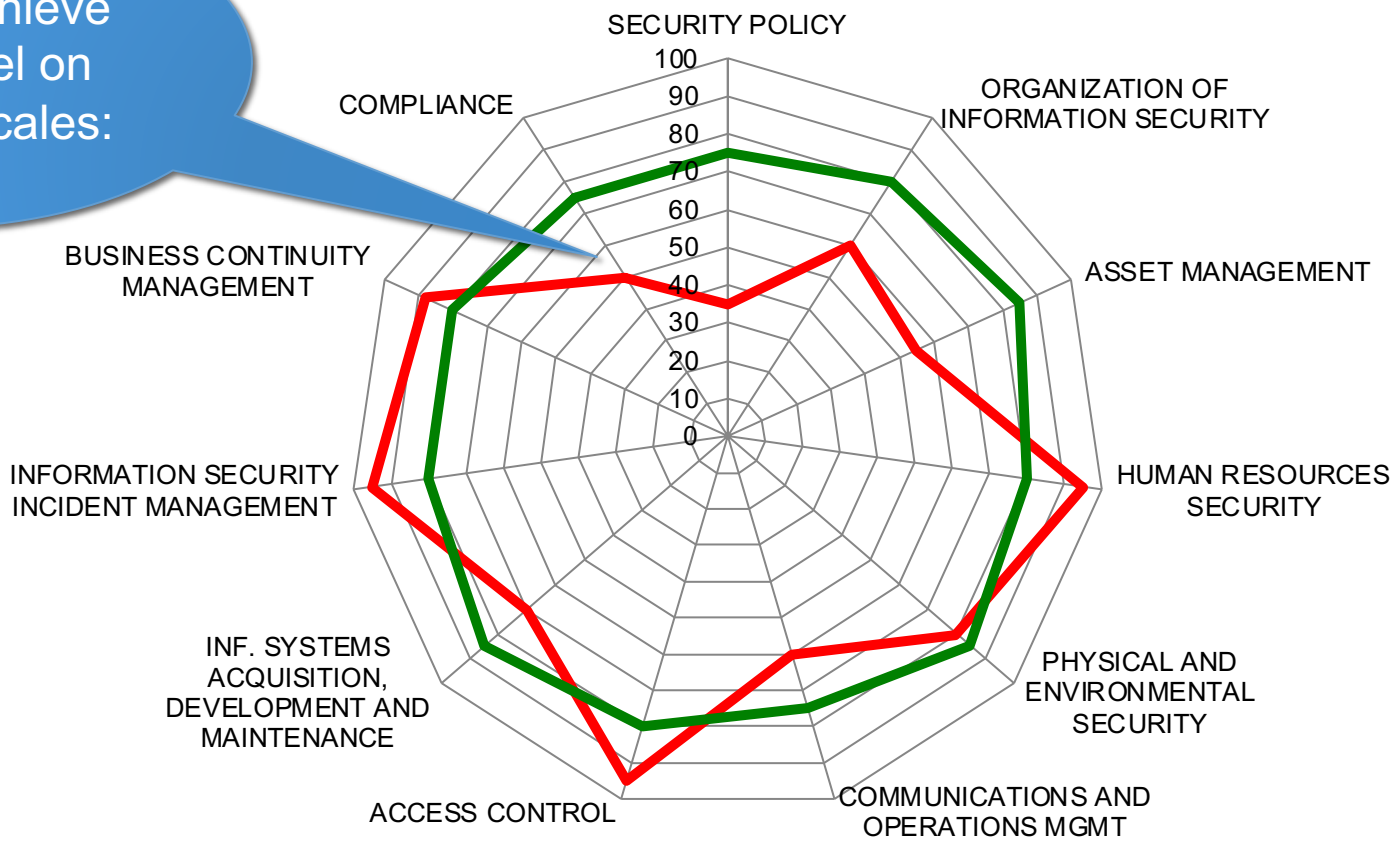
Do not focus on a single area only !

Attackers will find the weakest part of your
- technology
- processes or
- people

L7 - Information Security

Information Security – Summary

Attempt to achieve a uniform level on each of the scales:



L7 - Information Security

Information Security – Summary

Bruce Schneier:

If you think technology can solve your security problems,
then you don't understand the problems
and you don't understand the technology.

If you only memorize one thing from this whole lecture, make sure it is this sentence !
This is valid for EVERY industry, not only banking.