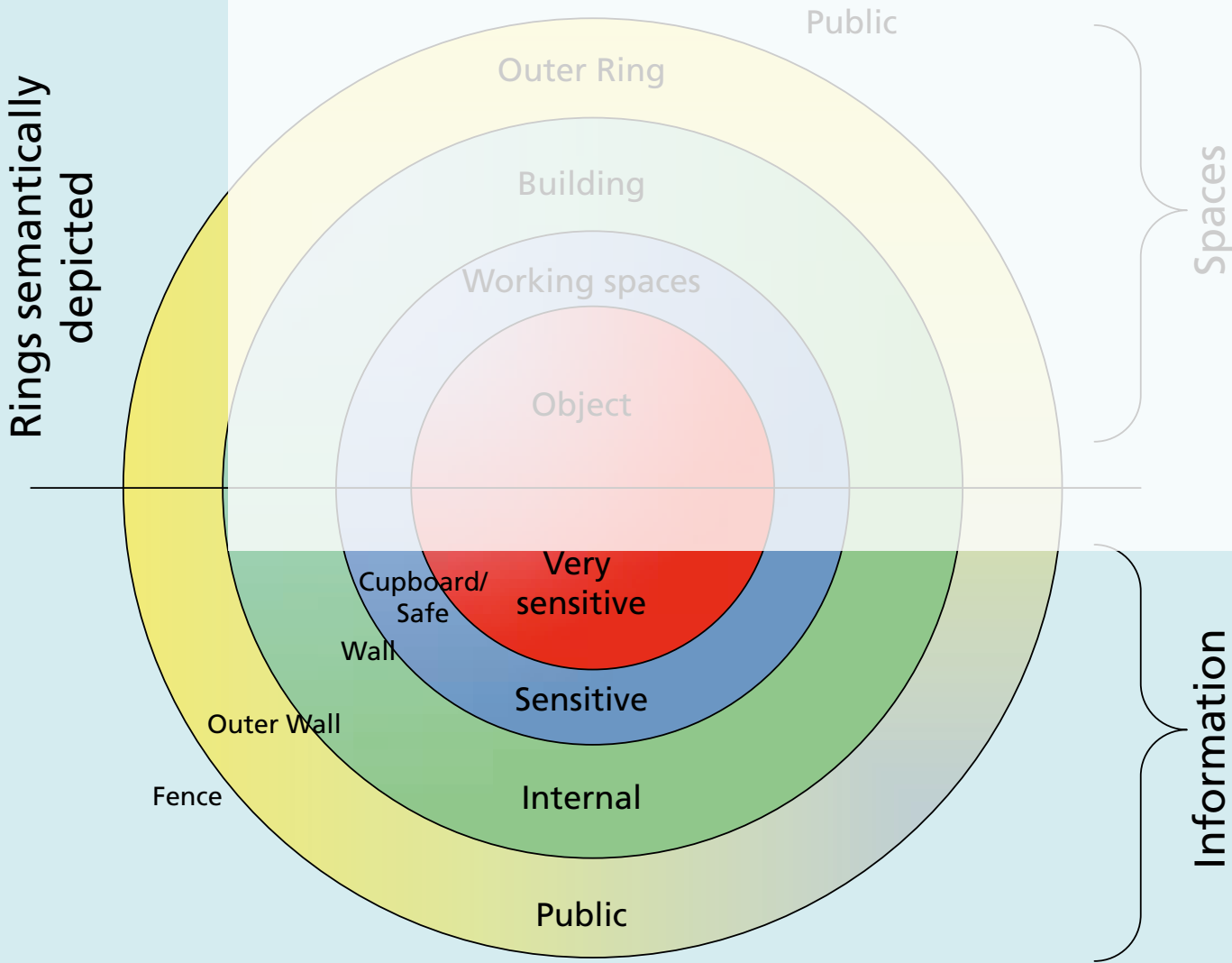


Information Security Foundation
based on ISO/IEC 27002

Courseware



Information Security Foundation (based on ISO/IEC 27002)
Courseware

Colofon

Title: Information Security Foundation (based on ISO/IEC 27002) Courseware

Authors: Hans Baars, Jule Hintzbergen, Andre Smulders en Kees Hintzbergen

Publisher: Van Haren Publishing, Zaltbommel

ISBN Hard copy: 978 94 018 0060 0

Edition: First edition, first impression, September 2016

Design & layout: Van Haren Publishing, Zaltbommel

Copyright: © Van Haren Publishing 2016

For any future enquiries about Van Haren Publishing, please send an email to: info@vanharen.net

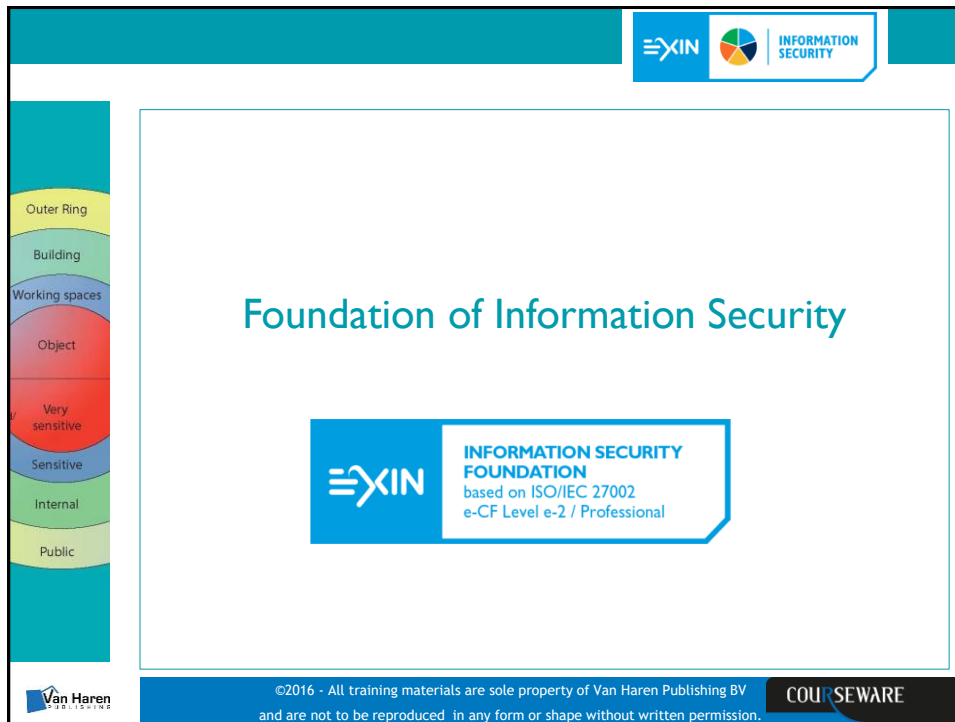
All rights reserved. No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by the publisher.

Although this publication has been composed with much care, neither author, nor editor, nor publisher can accept any liability for damage caused by possible errors and/or incompleteness in this publication.

The Certificate EXIN Information Security Foundation based on ISO/IEC 27002 is part of the qualification program Information Security. The module is followed up by the Certificates EXIN Information Security Management Advanced based on ISO/IEC 27002 and EXIN Information Security Management Expert based on ISO/IEC 27002.

Contents

Introduction	5
Module 1: About this course	7
ISFS THE START	7
About EXIN	8
About ISF	8
ISFS exam specifications	9
ISFS basic concepts list	10
ISFS literature, how to use the book	11
Module 2: Information and security, ISO 2700x	13
The concept of information	13
Value of information	15
Reliability aspects	18
Module 3: Threats and risks	23
Threats and risks	23
Relationships between threats, risks and the reliability of information	25
Module 4: Approach and organization	29
Approach and organization	29
Security policy and security organization	30
Components	31
Incident management	33
Other security processes	36
Module 5: Measures	39
Measures	39
Importance of measures	40
Physical security measures	43
Technical measures	44
Organizational measures	47
Module 6: Legislation and regulations	55
Legislation and regulations	55
Module 7: Exam Training	59
Module 8: Exam Time	101
EXIN Sample Exam	105
EXIN Preparation Guide	141



The slide features a vertical navigation bar on the left with the following categories: Outer Ring, Building, Working spaces, Object, Very sensitive, Sensitive, Internal, and Public. The central content box contains the title 'Foundation of Information Security' and the EXIN Information Security Foundation logo, which is based on ISO/IEC 27002 e-CF Level e-2 / Professional. The footer includes the Van Haren Publishing logo, a copyright notice for 2016, and the COURSEWARE logo.

Outer Ring

Building

Working spaces

Object

Very sensitive

Sensitive

Internal

Public

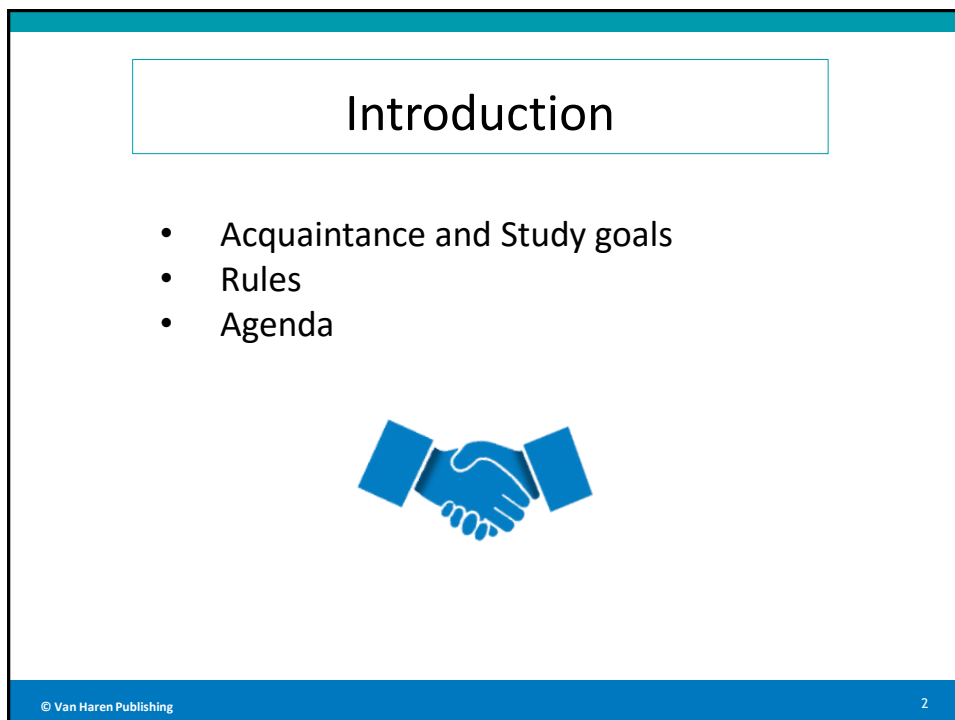
EXIN INFORMATION SECURITY

Foundation of Information Security

EXIN INFORMATION SECURITY FOUNDATION
based on ISO/IEC 27002
e-CF Level e-2 / Professional

©2016 - All training materials are sole property of Van Haren Publishing BV and are not to be reproduced in any form or shape without written permission.


Van Haren Publishing COURSEWARE



The slide is titled 'Introduction' and contains a list of three bullet points: 'Acquaintance and Study goals', 'Rules', and 'Agenda'. Below the list is a blue icon of two hands shaking. The footer includes the Van Haren Publishing logo and the page number 2.

Introduction


- Acquaintance and Study goals
- Rules
- Agenda



© Van Haren Publishing 2

This Clipboard shows per slide in which paragraph (§) of the desk book you can find additional information.

About the courseware



Study book Courseware Trainer slides

© Van Haren Publishing 3

Contents

Agenda

Day 1	Day 2
09.00 - 9.30 Introduction	09:00 – 09:20 Wrap up from day 1
09.30 - 10.15 Module 1: About Exin	09:20 – 10:05 Module 6: Legislation
10.15 – 12.00 Module 2: Information and security	10:05 – 10:20 Break
12.00 - 12.30 Lunch	10.20 – 12.20 Module 7: Exam training
13.30 - 13.15 Module 3: Threats and risks	12.20 – 13:00 Lunch
13.15 – 14.45 Module 4: Approach and organization	13:00 - 14:30 Self study
14.45 – 17.00 Module 5: Measures	14:30 – 14:50 Break
	14:50 - 15:00 Module 8: Exam overview
	15:00 - 16:00 Doing the actual exam

© Van Haren Publishing 4

Foundation of Information Security

The slide features a vertical stack of colored segments on the left side, representing a security model. From top to bottom, the segments are: Outer Ring (yellow), Building (light green), Working spaces (light blue), Object (red), Very sensitive (dark red), Sensitive (blue), Internal (green), and Public (light green). The main content area contains the text: "Foundation of Information Security" and "Module I About this course".

©2016 - All training materials are sole property of Van Haren Publishing BV and are not to be reproduced in any form or shape without written permission.

The slide displays the course logo at the top center, which includes the "EXIN" logo, a circular icon with four colored segments (green, blue, orange, red), and the text "INFORMATION SECURITY". Below the logo, the text "Module 1" is followed by a large box containing the title "ISFS THE START".

© Van Haren Publishing

Foundation of Information Security

About this course

INFORMATION SECURITY FOUNDATION
 based on ISO/IEC 27002
 e-CF Level e-2 / Professional

About EXIN

- EXIN
- Mission
- EXIN and information security

© Van Haren Publishing 7

About ISFS

- Why ISFS
- What are benefits of examination
- Target group
- e-Competence Framework (e-CF)

About EXIN

- EXIN
- Mission
- EXIN and information security

e-CF Area	e-Competence	e-1	e-2	e-3	e-4	e-5
RUN	C.2. Change Support					
	C.3. Service Delivery					
ENABLE	D.9. Personnel Development					
	D.10. Information and Knowledge Management					
MANAGE	E.3. Risk Management					
	E.8. Information Security Management					

Legend for coverage:
 General - The competence is covered at the level indicated
 Partial - The competence is covered to some extent
 Superficial - Relevant knowledge is covered to some extent
 The competence level is available in the framework
 The competence level is not available in the framework

© Van Haren Publishing 8

Exam requirements

Exam requirement	Exam specification	Weight %	
1 Information and security			10
	1.1 The concept of information	2.5	
	1.2 Value of information	2.5	
	1.3 Reliability aspects	5	
2 Threats and risks			30
	2.1 Threats and risks	15	
	2.2 Relationships between threats, risks and the reliability of information	15	
3 Approach and organization			10
	3.1 Security policy and security organization	2.5	
	3.2 Components	2.5	
	3.3 Incident management	5	
4 Measures			40
	4.1 Importance of measures	10	
	4.2 Physical security measures	10	
	4.3 Technical measures	10	
	4.4 Organizational measures	10	
5 Legislation and regulation			10
	5.1 Legislation and regulations	10	
Total 100	Total 100	Total 100	

ISFS exam specifications

- | | |
|--|---|
| <p>1. Information and security (10%)</p> <p>1.1 The concept of information (2.5%)
The candidate understands the concept information.
The candidate is able to:
1.1.1 Explain the difference between data and information;
1.1.2 Describe the storage medium that forms part of the basic infrastructure.</p> <p>1.2 Value of information (2.5%)
The candidate understands the value of information for organizations.
The candidate is able to:
1.2.1 Describe the value of data/information for organizations;
1.2.2 Describe how the value of data/information can influence organizations;
1.2.3 Explain how applied information security concepts protect the value of data/information.</p> <p>1.3 Reliability aspects (5%)
The candidate knows the reliability aspects (confidentiality, integrity, availability) of information.
The candidate is able to:
1.3.1 Name the reliability aspects of information;
1.3.2 Describe the reliability aspects of information.</p> <p>2. Threats and risks (30%)</p> <p>2.1 Threat and risk (15%)
The candidate understands the concepts of threat and risk.
The candidate is able to:
2.1.1 Explain the concepts threat, risk and risk analysis;
2.1.2 Explain the relationship between a threat and a risk;
2.1.3 Describe various types of threats;
2.1.4 Describe various types of damage;
2.1.5 Describe various risk strategies.</p> <p>2.2 Relationships between threats, risks and the reliability of information. (15%)
The candidate understands the relationship between threats, risks and the reliability of information.
The candidate is able to:
2.2.1 Recognize examples of the various types of threats;
2.2.2 Describe the effects that the various types of threats have on information and the processing of information.</p> | <p>3. Approach and organization (10%)</p> <p>3.1 Security policy and security organization (2.5%)
The candidate has knowledge of the concepts security policy and security organization.
The candidate is able to:
3.1.1 Outline the objectives and the content of a security policy;
3.1.2 Outline the objectives and the content of a security organization.</p> <p>3.2 Components (2.5%)
The candidate knows the various components of the security organization.
The candidate is able to:
3.2.1 Explain the importance of a code of conduct;
3.2.2 Explain the importance of ownership;
3.2.3 Name the most important roles in the information security organization.</p> <p>3.3 Incident Management (5%)
The candidate understands the importance of incident management and escalation.
The candidate is able to:
3.3.1 Summarize how security incidents are reported and what information is required;
3.3.2 Give examples of security incidents;
3.3.3 Explain the consequences of not reporting security incidents;
3.3.4 Explain what an escalation entails (functionally and hierarchically);
3.3.5 Describe the effects of escalation within the organization;
3.3.6 Explain the incident cycle.</p> <p>4. Measures (40%)</p> <p>4.1 Importance of measures (10%)
The candidate understands the importance of security measures.
The candidate is able to:
4.1.1 Describe various ways in which security measures may be structured or arranged;
4.1.2 Give examples for each type of security measure;
4.1.3 Explain the relationship between risks and security measures;
4.1.4 Explain the objective of the classification of information;
4.1.5 Describe the effect of classification.</p> <p>4.2 Physical security measures (10%)
The candidate has knowledge of both the set-up and execution of physical security measures.
The candidate is able to:
4.2.1 Give examples of physical security measures;
4.2.2 Describe the risks involved with insufficient physical security measures.</p> |
|--|---|

ISFS exam specifications



- 4.3 Technical measures (10%)**
The candidate has knowledge of both the set-up and execution of technical security measures.
The candidate is able to:
- 4.3.1 Give examples of technical security measures;
 - 4.3.2 Describe the risks involved with insufficient technical security measures;
 - 4.3.3 Understand the concepts cryptography, digital signature and certificate;
 - 4.3.4 Name the three steps for online banking (PC, web site, payment);
 - 4.3.5 Name various types of malicious software;
 - 4.3.6 Describe the measures that can be used against malicious software.
- 4.4 Organizational measures (10%)**
The candidate has knowledge of both the set-up and execution of organizational security measures.
The candidate is able to:
- 4.4.1 Give examples of organizational security measures;
 - 4.4.2 Describe the dangers and risks involved with insufficient organizational security measures;
 - 4.4.3 Describe access security measures such as the segregation of duties and the use of passwords;
 - 4.4.4 Describe the principles of access management;
 - 4.4.5 Describe the concepts identification, authentication and authorization;
 - 4.4.6 Explain the importance to an organization of a well set-up Business Continuity Management;
 - 4.4.7 Make clear the importance of conducting exercises.
- 5. Legislation and regulations (10%)**
- 5.1 Legislation and regulations (10%)**
The candidate understands the importance and effect of legislation and regulations.
The candidate is able to:
- 5.1.1 Explain why legislation and regulations are important for the reliability of information;
 - 5.1.2 Give examples of legislation related to information security;
 - 5.1.3 Give examples of regulations related to information security;
 - 5.1.4 Indicate possible measures that may be taken to fulfill the requirements of legislation and regulations.

Chapter 3

ISFS basic concepts list

- Access control
- Asset
- Audit
- Authentication
- Authenticity
- Authorization
- Availability
- Backup
- Biometrics
- Botnet
- Business Continuity Management (BCM)
- Business Continuity Plan (BCP)
- Business Assets
- Category
- Certificate
- Change Management
- Classification (grading)
- Clear desk policy
- Code of conduct
- Code of practice for information security (ISO/IEC 27002:2013)
- Completeness
- Compliance
- Computer criminality legislation
- Confidentiality
- Continuity
- Controls
- Corrective
- Copyright legislation
- Correctness
- Cryptography
- Cyber crime
- Damage
- Data
- Detective
- Digital signature
- Direct damage
- Disaster
- Disaster Recovery Plan (DRP)
- Encryption
- Escalation
 - o Functional escalation
 - o Hierarchical escalation
- Exclusivity
- Hacking
- Hoax
- Identification
- Impact
- Incident cycle
- Indirect damage
- Information
- Information analysis
- Information architecture
- Information management
- Information security review
- Information system
- Infrastructure
- Integrity
- Interference
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- Key
- Logical access management
- Managing business assets
- Maintenance door
- Malware
- Non-disclosure agreement
- Non-repudiation
- Patch
- Personal data protection legislation
- Personal firewall
- Phishing
- Precision
- Preventive
- Priority
- Privacy
- Production factor
- Public Key Infrastructure (PKI)
- Public records legislation
- Qualitative risk analysis
- Quantitative risk analysis
- Reductive
- Redundancy
- Reliability of information
- Repressive
- Risk
- Risk analysis
- Risk assessment (Dependency & Vulnerability analysis)
 - o Risk avoiding
 - o Risk bearing
- Risk management
 - o Risk neutral
- Risk strategy
- Robustness
- Rootkit
- Secret authentication information
- Security in development
- Security event
- Security incident
- Security measure
- Security Organization
- Security Policy
- Security regulations for the government
- Segregation of duties
- Social engineering
- Spam
- Spyware
- Stand-by arrangement
- Storage medium
- System acceptance testing
- Threat
- Timeliness
- Trojan
- Uninterruptible Power Supply (UPS)
- Urgency
- User access provisioning
- Validation
- Verification
- Virtual Private Network (VPN)
- Virus
- Vulnerability
- Worm

Contents

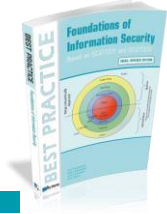
ISFS literature

Exam literature

K Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
 Van Haren Publishing, 3rd edition, 2015
 ISBN 978 94 018 0012 9
 eBook 978 94 018 0541 4

Overview of the literature

Exam specification	Literature
1.1	Chapter 3
1.2	Chapter 3 and 4
1.3	Chapter 3 and 4
2.1	Chapter 3
2.2	Chapter 3 and 11
3.1	Chapter 3, 5 and 6
3.2	Chapter 6, 7, 8 and 13
3.3	Chapter 3, 15 and 16
4.1	Chapter 3, 8 and 16
4.2	Chapter 3 and 11
4.3	Chapter 6, 10, 11 and 12
4.4	Chapter 3, 6, 9, 17 and 18
5.1	Chapter 18



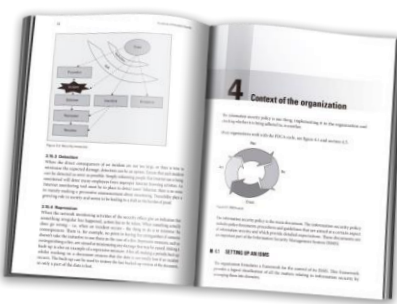
© Van Haren Publishing

13

Chapter 1

About the book

- Provides a basic understanding of information security
- Official training guide for EXIN exam Information Security Foundation
- Contains Case studies
- Contains a ISFS model exam
- Feedback to all multiple choice options



© Van Haren Publishing

14

Outer Ring

Building

Working spaces

Object

Very sensitive

Sensitive

Internal

Public

Foundation of Information Security
Module 2 Information and security, ISO 2700x

©2016 - All training materials are sole property of Van Haren Publishing BV
and are not to be reproduced in any form or shape without written permission.

Van Haren PUBLISHING

COURSEWARE

Module 2

THE CONCEPT OF INFORMATION

© Van Haren Publishing

16

Difference between data and information

- **Data:**
 - can be processed by Information technology
- **Information:**
 - Is data that has acquired a certain meaning

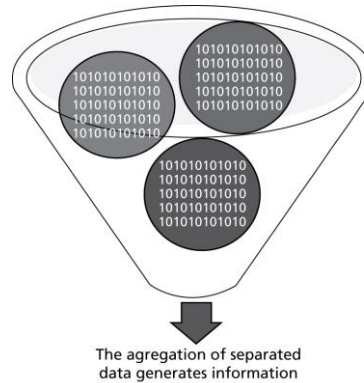


Figure 4.3 Aggregation of data generates information

Source: Foundations of IT Security Based on ISO27001/27002

© Van Haren Publishing 2010

Examples of elements that forms part of the basic infrastructure

- **Information Technology**
 - Workstations
 - Data transport via a network, cabled or wireless;
 - Servers;
 - Data storage;
 - Mobile phones;
 - Other connections
- **Information Systems**
 - File cabinets containing printed documents;
 - A printed phone directory;



Module 2

VALUE OF INFORMATION

© Van Haren Publishing

19

Par 4.10.4

Value of data for organizations

- Data can have great significance – depending on how it is used
- Value is primarily determined by the user
 - How important is that data to perform a certain task



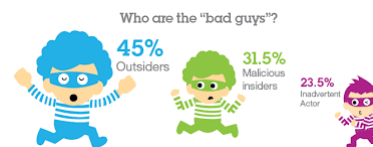
© Van Haren Publishing

20

Par 4.10.5

Value of information for organizations

- Some people may consider a particular set of data uninteresting, others may be able to extract valuable information from it



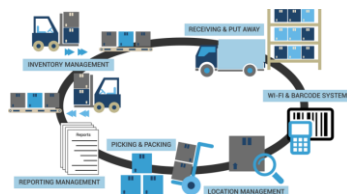
© Van Haren Publishing

21

Par 4.10.6

Why is information/data valuable?

- A warehouse that loses its customer and stock information would usually not be able to operate without it
- For an accountant's office, information is actually their only product.



© Van Haren Publishing

22

Par 3.4

how applied information security concepts protect the value of data/information

- **Confidentiality**
 - Access to information is granted on a 'need to know' basis
 - Logical access management ensures that unauthorized persons or processes do not have access to automated systems, databases and programs.
 - A separation of duties is created between organizational units;
 - Strict separations are created between development, test and production
 - Measures are taken to ensure the privacy of personnel and third parties.

© Van Haren Publishing

23

Par 3.5

how applied information security concepts protect the value of data/information

- **Integrity**
 - Changes in systems and data are authorized.
 - Where possible, mechanisms are built in that force people to use the correct term.
 - Users' actions are recorded (logged) so that it can be determined who made a change in the information;
 - Vital system actions, for example installing new software, cannot be carried out by just one person.

© Van Haren Publishing

24

Par 3.6

how applied information security concepts protect the value of data/information

- **Availability**
 - The management and storage of data is such that the risk of losing information is minimal;
 - Back-up procedures are set up.
- Statutory requirements for how long data must be stored will vary from country to country in EU, the USA, and elsewhere.

© Van Haren Publishing 25

Module 2

RELIABILITY ASPECTS

© Van Haren Publishing 26

Par 3.3

Fundamental principles of security

- All security controls, mechanisms and safeguards are implemented to provide one or more of these principles
- all risks, threats, and vulnerabilities are measured for their potential capability to compromise one or all of the CIA principles

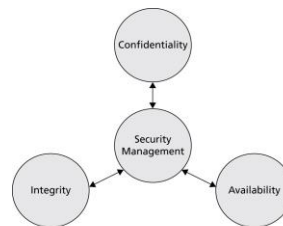


Figure 4.1 The CIA triangle
Source: Foundations of IT Security Based on ISO27001/27002

© Van Haren Publishing 2010

© Van Haren Publishing

27

Par 3.4

CONFIDENTIALITY

- the limits in terms of who can get what kind of information



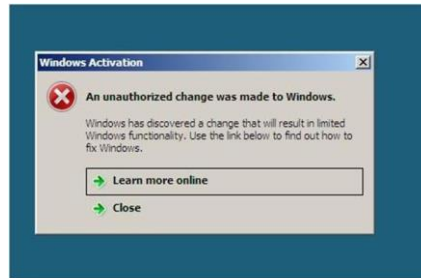
© Van Haren Publishing

28

Par 3.5

INTEGRITY

- Integrity refers to being correct or consistent with the intended state of information.
- Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity.



© Van Haren Publishing

29

Par 3.6

AVAILABILITY

- The characteristics of availability are:
 - Timeliness;
 - Continuity;
 - Robustness.



© Van Haren Publishing

30

Appendix C.1

Questions

1. What is the relationship between data and information?
 - A. Data is structured information.
 - B. Information is the meaning and value assigned to a collection of data

© Van Haren Publishing 31

Appendix C.1

Questions

2. In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages. Which factor is not important for determining the value of data for an organization?
 - A. The content of data.
 - B. The degree to which missing, incomplete or incorrect data can be recovered.
 - C. The indispensability of data for the business processes.
 - D. The importance of the business processes that make use of the data.

© Van Haren Publishing 32

Appendix C.1

Questions

3. A hacker gains access to a webserver and can view a file on the server containing credit card numbers. Which of the Confidentiality, Integrity, Availability (CIA) principles of the credit card file are violated?

- A. Availability
- B. Confidentiality
- C. Integrity

© Van Haren Publishing 33

Appendix C.1

Questions

4. There is a network printer in the hallway of the company where you work. Many employees don't pick up their printouts immediately and leave them on the printer. What are the consequences of this to the reliability of the information?

- A. The integrity of the information is no longer guaranteed.
- B. The availability of the information is no longer guaranteed.
- C. The confidentiality of the information is no longer guaranteed.

© Van Haren Publishing 34

Outer Ring

Building

Working spaces

Object

Very sensitive

Sensitive

Internal

Public

Foundation of Information Security
Module 3 Threats and risks

©2016 - All training materials are sole property of Van Haren Publishing BV
and are not to be reproduced in any form or shape without written permission.

Van Haren PUBLISHING

COURSEWARE

Module 3

THREATS AND RISKS

© Van Haren Publishing

36

Par 3.9

Threat and threat agent

- A threat is a potential cause of an unwanted incident
- A threat agent is an entity that takes advantage of a vulnerability
- For example, a threat agent could be an intruder accessing the network through a port on the firewall,
- Or a process accessing data in a way that violates the security policy

© Van Haren Publishing

37

Par 3.8

Risk

- A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact.
- For example a fire can break out at your company;
- or an employee who does not work in the HR department gains access to private or sensitive information.

© Van Haren Publishing

38

Par 3.13.3

Risk analysis

- Risk analysis is the process of:
 - Identifying assets and their value
 - Establishing a balance between the costs of an incident and the costs of a security measure
 - Determining relevant vulnerabilities and threats
- A risk analysis ensures:
 - security measures are deployed in a cost-effective and timely manner, and
 - provide an effective answer to the threats

© Van Haren Publishing

39

Par 3.1

Relationship between a threat and a risk

- A threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.
- Risk relates to the potential that threats cause harm to an organization.

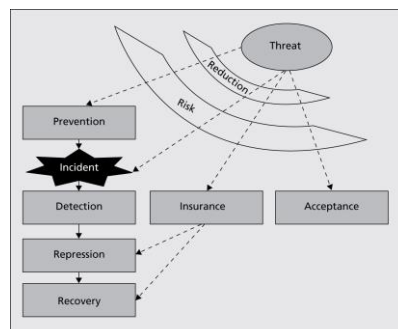


Figure 5.1 Security measures
Source: Foundations of IT Security Based on ISO27001:2002

© Van Haren Publishing

40