COURSEWARE

INFORMATION SECURITY FOUNDATION

BASED ON ISOIEC 27001 ’22 COURSEWARE

Van Haren
PUBLISHING

Information Security Foundation
based on ISO/IEC 27001 ’22
Courseware

Colophon

Title:	Information Security Foundation based on ISO/IEC 27001 ’22 Courseware
Authors:	Hans Baars, Jule Hintzbergen, Kees Hintzbergen
Publisher:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN Hard Copy:	978 94 018 0943 6
Edition:	First edition, first print, January 2024
Design:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2024

For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

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.

Publisher about the Courseware

The Courseware was created by experts from the industry who served as the author(s) for this publication. The input for the material is based on existing publications and the experience and expertise of the author(s). The material has been revised by trainers who also have experience working with the material. Close attention was also paid to the key learning points to ensure what needs to be mastered.

The objective of the courseware is to provide maximum support to the trainer and to the student, during his or her training. The material has a modular structure and according to the author(s) has the highest success rate should the student opt for examination. The Courseware is also accredited for this reason, wherever applicable.

In order to satisfy the requirements for accreditation the material must meet certain quality standards. The structure, the use of certain terms, diagrams and references are all part of this accreditation. Additionally, the material must be made available to each student in order to obtain full accreditation. To optimally support the trainer and the participant of the training assignments, practice exams and results are provided with the material.

Direct reference to advised literature is also regularly covered in the sheets so that students can find additional information concerning a particular topic. The decision to leave out notes pages from the Courseware was to encourage students to take notes throughout the material.

Although the courseware is complete, the possibility that the trainer deviates from the structure of the sheets or chooses to not refer to all the sheets or commands does exist. The student always has the possibility to cover these topics and go through them on their own time. It is recommended to follow the structure of the courseware and publications for maximum exam preparation. This courseware includes the official manual. The pages following the manual contain the courseware and syllabus.

The courseware and the recommended literature are the perfect combination to learn and understand the theory.

-- Van Haren Publishing

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management

BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

Project Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

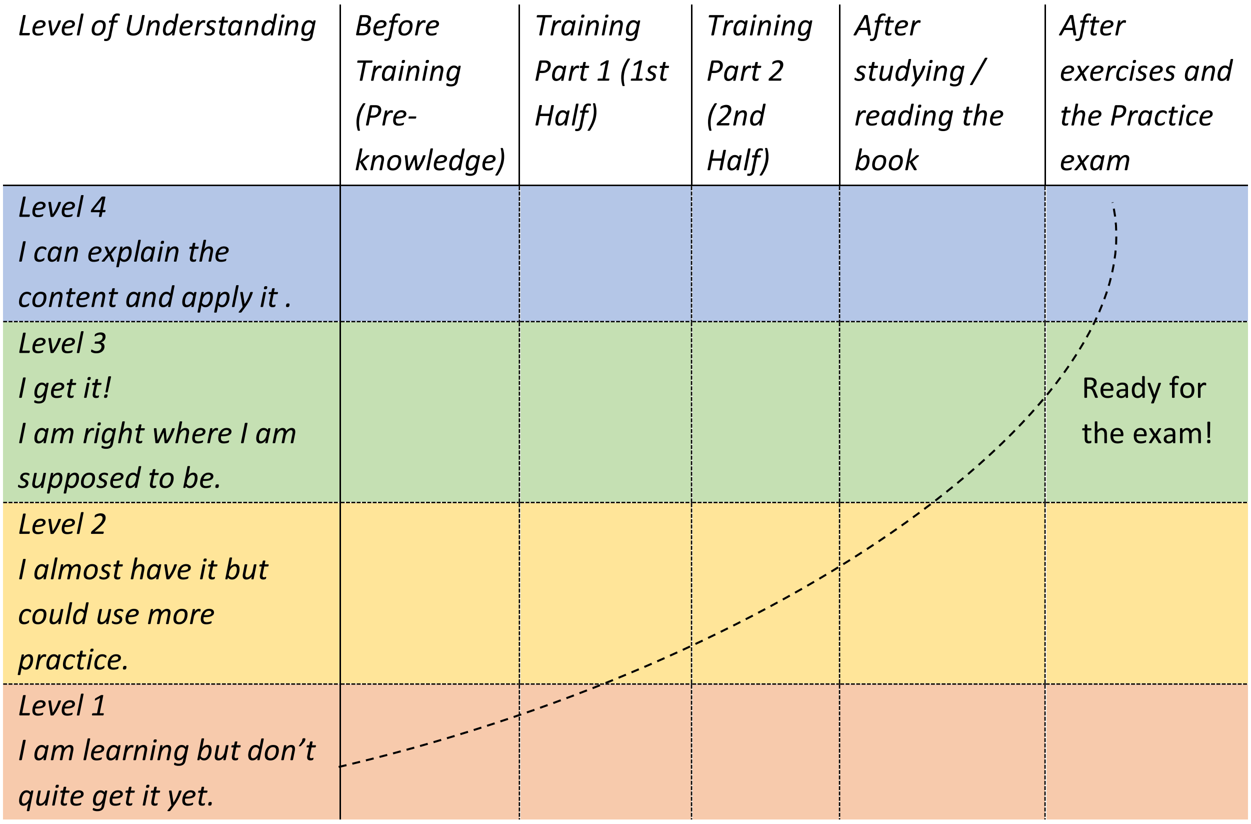
Table of content

Self-Reflection of understanding Diagram

‘*What you do not measure, you cannot control*.’’ – Tom Peters

Fill in this diagram to self-evaluate your understanding of the material. This is an evaluation of how well you know the material and how well you understand it. In order to pass the exam successfully you should be aiming to reach the higher end of Level 3. If you really want to become a pro, then you should be aiming for Level 4. Your overall level of understanding will naturally follow the learning curve. So, it’s important to keep track of where you are at each point of the training and address any areas of difficulty.

Based on where you are within the Self-Reflection of Understanding diagram you can evaluate the progress of your own training.



Level of Understanding	*Before Training (Pre-knowledge)*	*Training Part 1 (1st Half)*	*Training Part 2 (2nd Half)*	*After studying / reading the book*	*After exercises and the Practice exam*
Level 4 *I can explain the content and apply it .*					
Level 3 *I get it!* *I am right where I am supposed to be.*					Ready for the exam!
Level 2 *I almost have it but could use more practice.*					
Level 1 *I am learning but don’t quite get it yet.*					

(Self-Reflection of Understanding Diagram)

Write down the problem areas that you are still having difficulty with so that you can consolidate them yourself, or with your trainer. After you have had a look at these, then you should evaluate to see if you now have a better understanding of where you actually are on the learning curve.

Troubleshooting

Problem areas: *Topic:*

Part 1

Part 2

You have gone through the book and studied.

You have answered the questions and done the practice exam.

Timetable

Agenda with Exam

Day 1

- Introduction
- Module 1: About Exin
- Module 2: Information and security
- Lunch
- Module 3: Threats & risks
- Module 4: Approach and Organization
- Module 5:
  - 5.1: Organizational
  - 5.2: Human
  - 5.3: Physical
  - 5.4: Technical

Day 2

- Wrap up day 1
- Module 5: Measures continued
- Break
- Self study
- Lunch
- Module 6: Exam training
- Module 7: Exam explanation
- Wrap up / evaluation

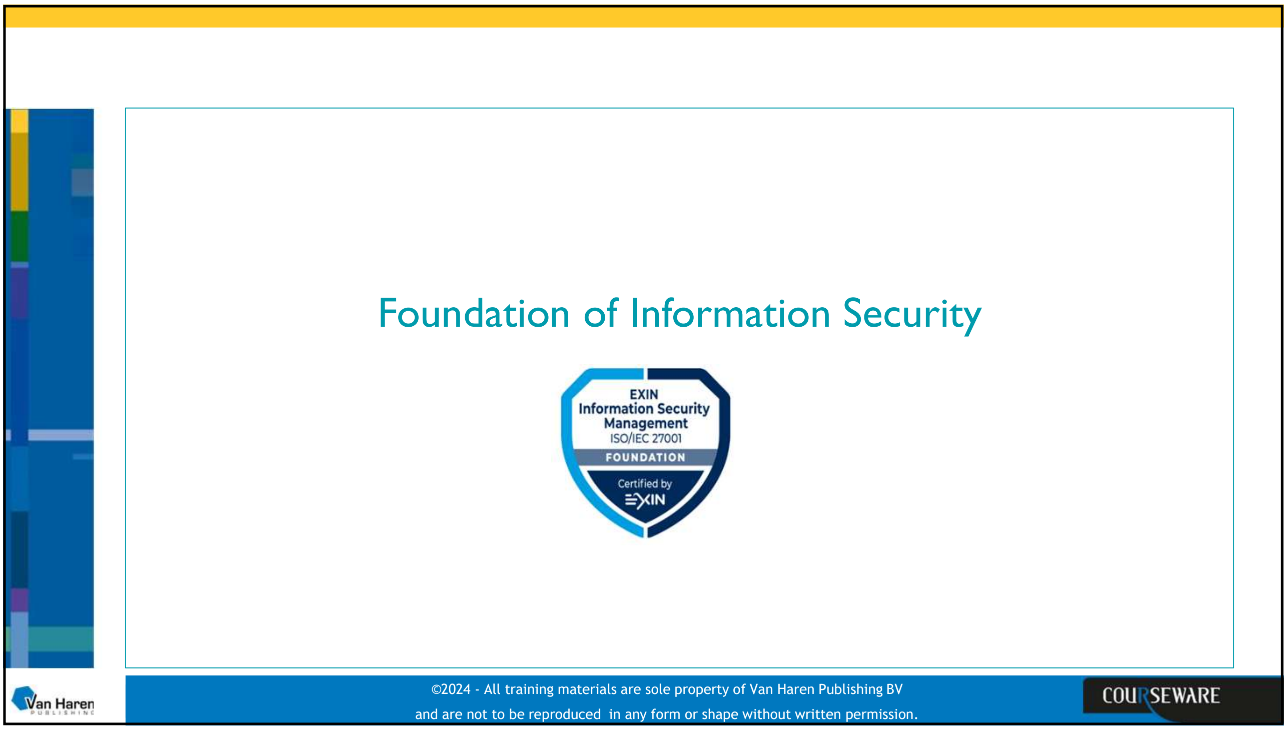
Agenda without Exam

Day 1

- Introduction
- Module 1: About Exin
- Module 2: Information and security
- Lunch
- Module 3: Threats & risks
- Module 4: Approach and Organization
- Module 5:
  - 5.1: Organizational
  - 5.2: Human
  - 5.3: Physical
  - 5.4: Technical

Day 2

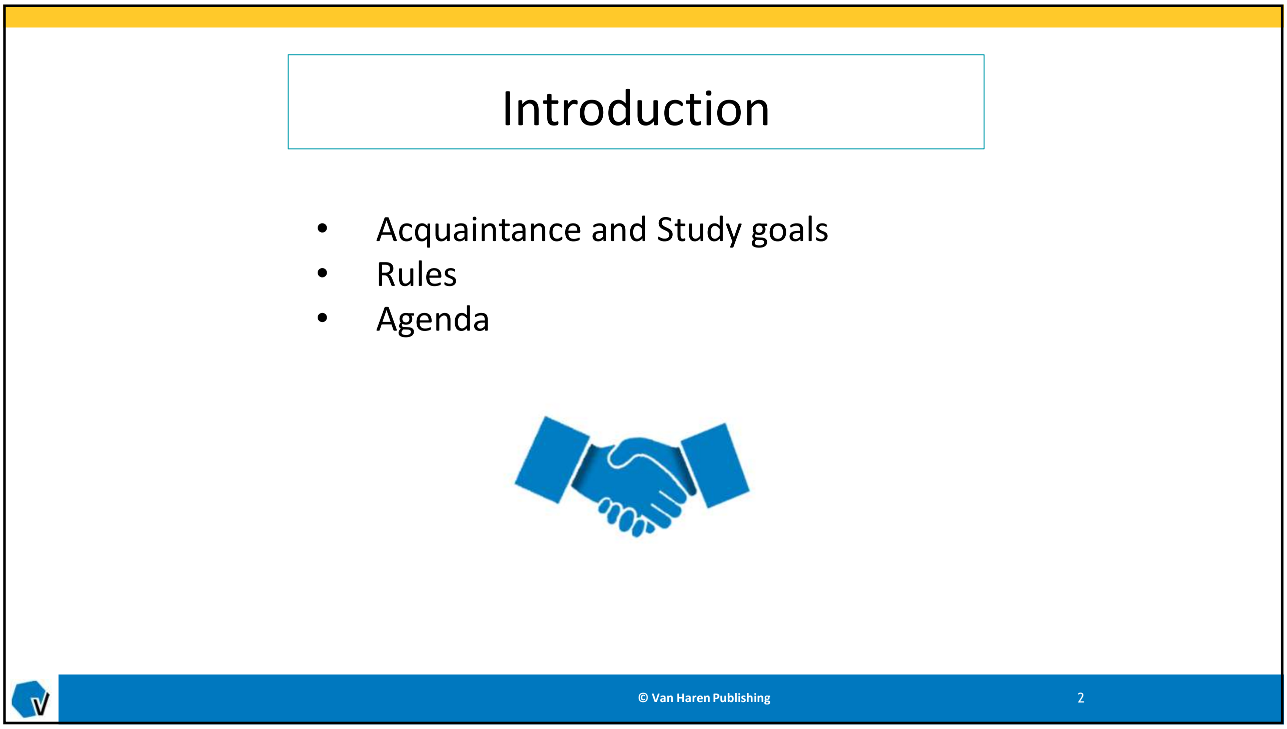
- Wrap up day 1
- Module 5: Measures continued
- Break
- Self study
- Module 6: Exam training
- Module 7: Exam explanation
- Wrap up / evaluation



Foundation of Information Security

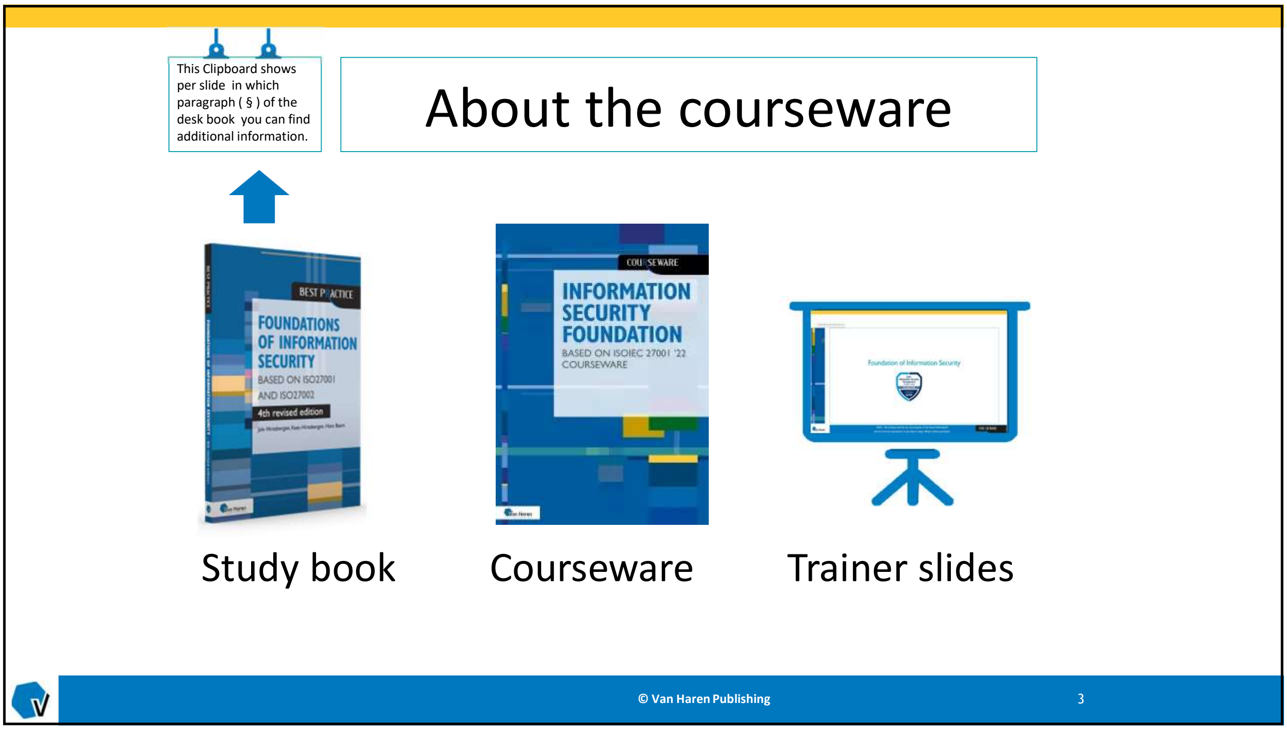
EXIN
Information Security Management
ISO/IEC 27001
FOUNDATION
Certified by EXIN

COURSEWARE



Introduction

- Acquaintance and Study goals
- Rules
- Agenda



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

About the courseware

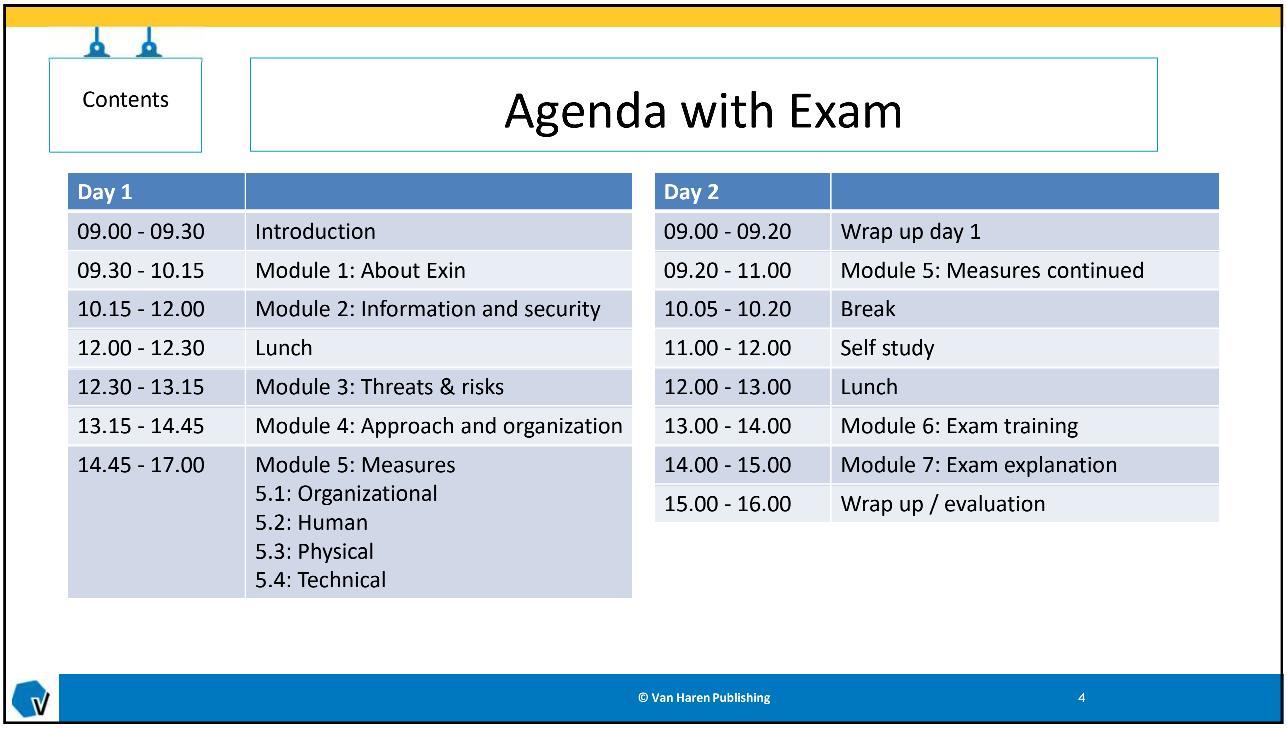
BEST PRACTICE
FOUNDATIONS OF INFORMATION SECURITY
BASED ON ISO27001 AND ISO27002
4th revised edition
COURSEWARE
INFORMATION SECURITY FOUNDATION
BASED ON ISO/IEC 27001 '22
COURSEWARE
Foundation of Information Security

Study book

Courseware

Trainer slides

© Van Haren Publishing 3



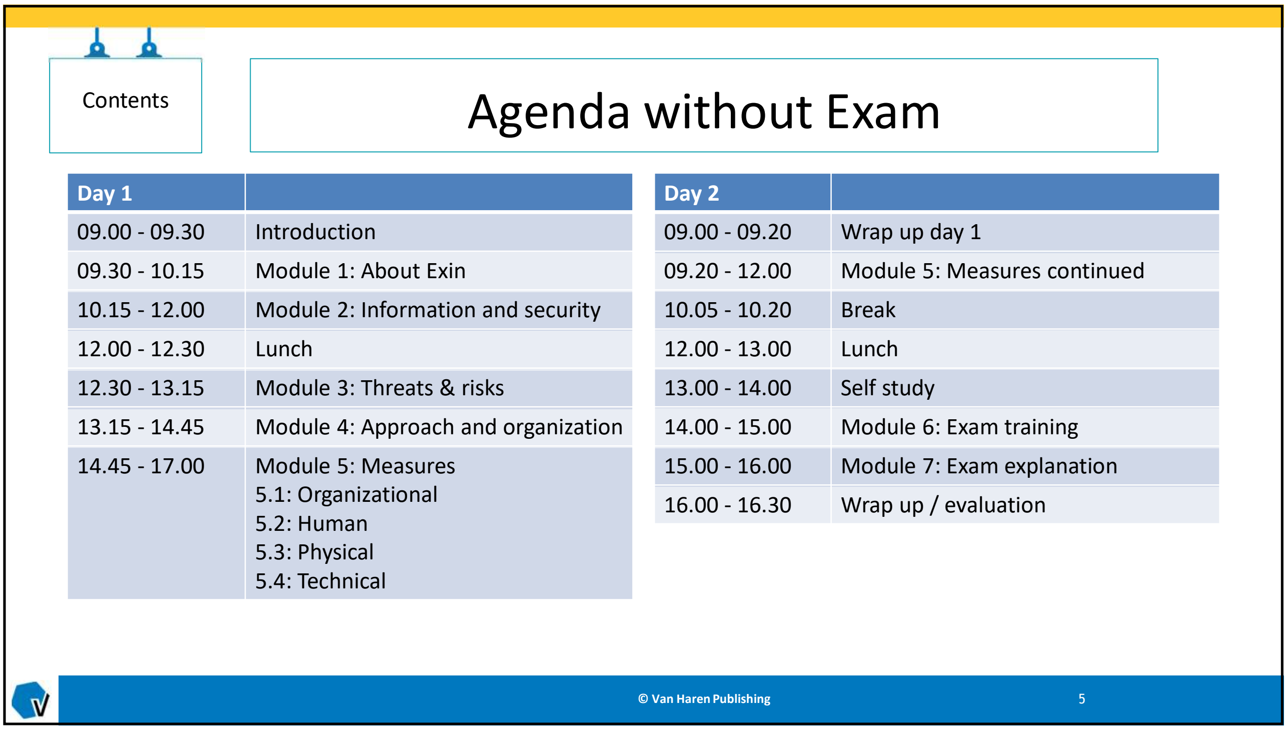
Contents

Agenda with Exam

Day 1	
09.00 - 09.30	Introduction
09.30 - 10.15	Module 1: About Exin
10.15 - 12.00	Module 2: Information and security
12.00 - 12.30	Lunch
12.30 - 13.15	Module 3: Threats & risks
13.15 - 14.45	Module 4: Approach and organization
14.45 - 17.00	Module 5: Measures 5.1: Organizational 5.2: Human 5.3: Physical 5.4: Technical

Day 2	
09.00 - 09.20	Wrap up day 1
09.20 - 11.00	Module 5: Measures continued
10.05 - 10.20	Break
11.00 - 12.00	Self study
12.00 - 13.00	Lunch
13.00 - 14.00	Module 6: Exam training
14.00 - 15.00	Module 7: Exam explanation
15.00 - 16.00	Wrap up / evaluation

© Van Haren Publishing 4



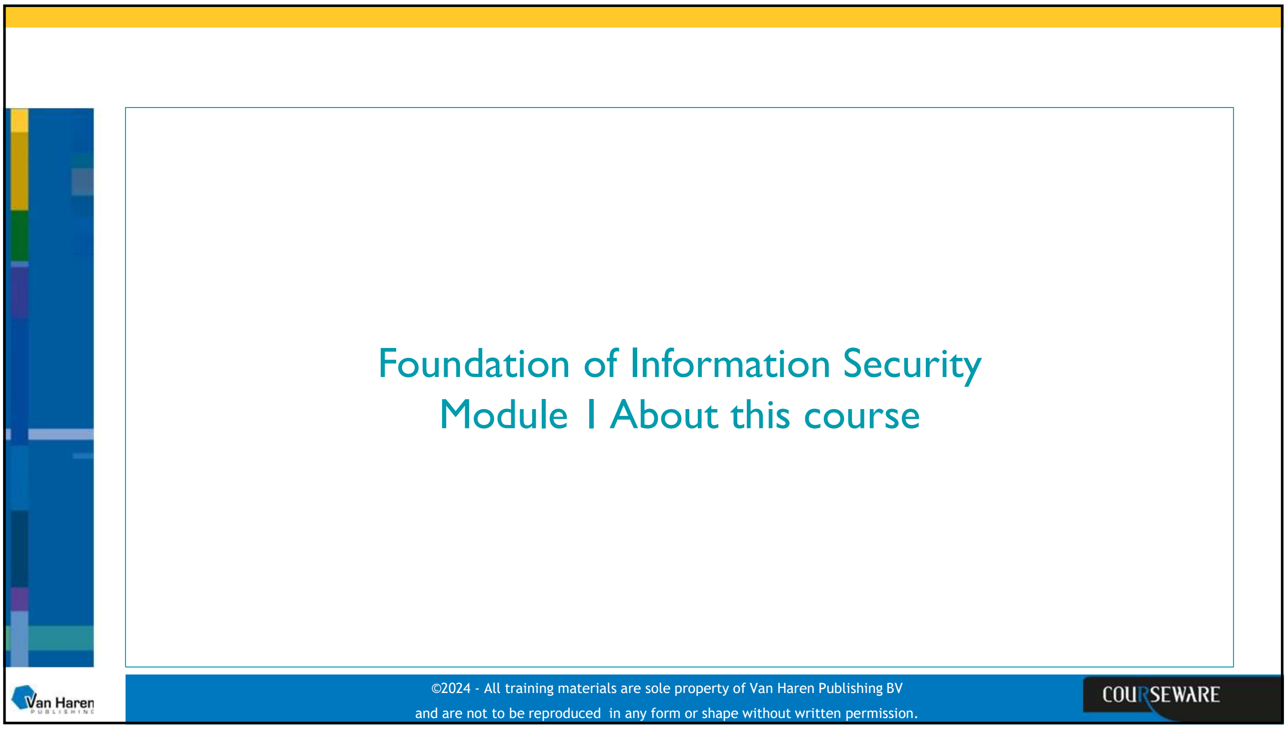
Contents

Agenda without Exam

Day 1	
09.00 - 09.30	Introduction
09.30 - 10.15	Module 1: About Exin
10.15 - 12.00	Module 2: Information and security
12.00 - 12.30	Lunch
12.30 - 13.15	Module 3: Threats & risks
13.15 - 14.45	Module 4: Approach and organization
14.45 - 17.00	Module 5: Measures 5.1: Organizational 5.2: Human 5.3: Physical 5.4: Technical

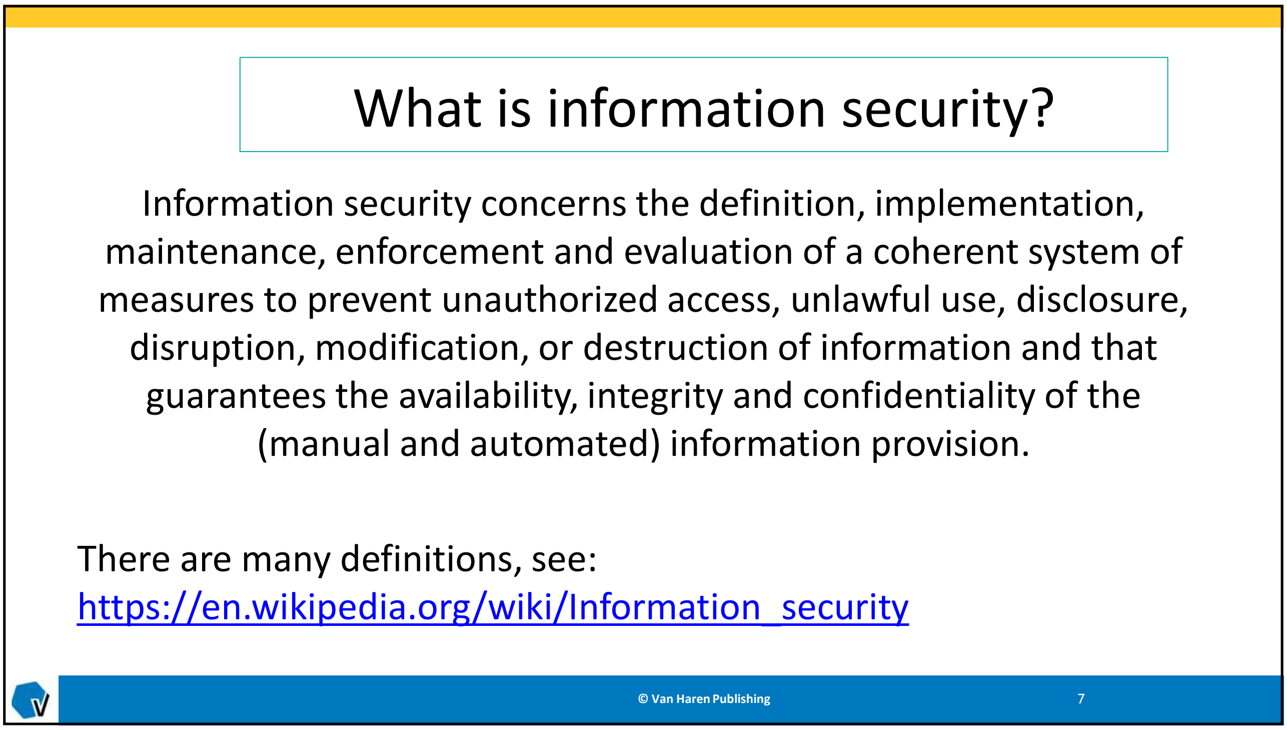
Day 2	
09.00 - 09.20	Wrap up day 1
09.20 - 12.00	Module 5: Measures continued
10.05 - 10.20	Break
12.00 - 13.00	Lunch
13.00 - 14.00	Self study
14.00 - 15.00	Module 6: Exam training
15.00 - 16.00	Module 7: Exam explanation
16.00 - 16.30	Wrap up / evaluation

© Van Haren Publishing 5



Foundation of Information Security
Module I About this course

©2024 - 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.

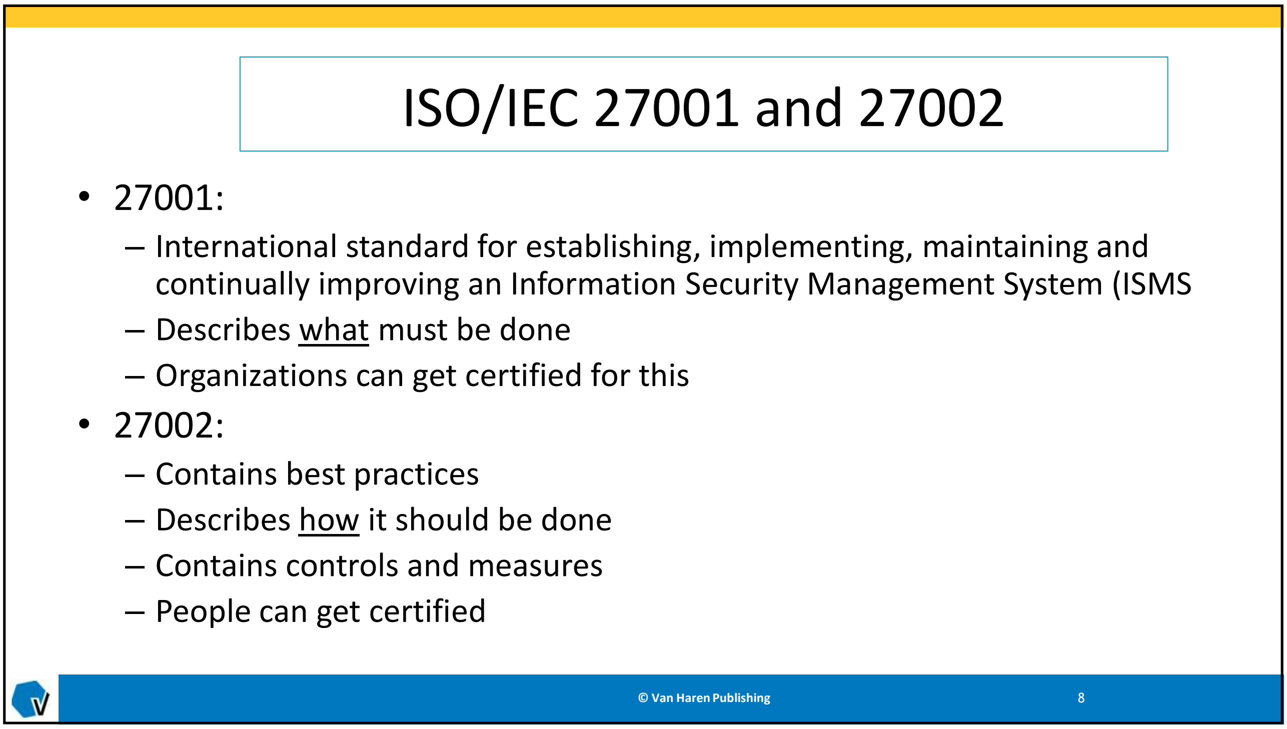


What is information security?

Information security concerns the definition, implementation, maintenance, enforcement and evaluation of a coherent system of measures to prevent unauthorized access, unlawful use, disclosure, disruption, modification, or destruction of information and that guarantees the availability, integrity and confidentiality of the (manual and automated) information provision.

There are many definitions, see:
https://en.wikipedia.org/wiki/Information_security

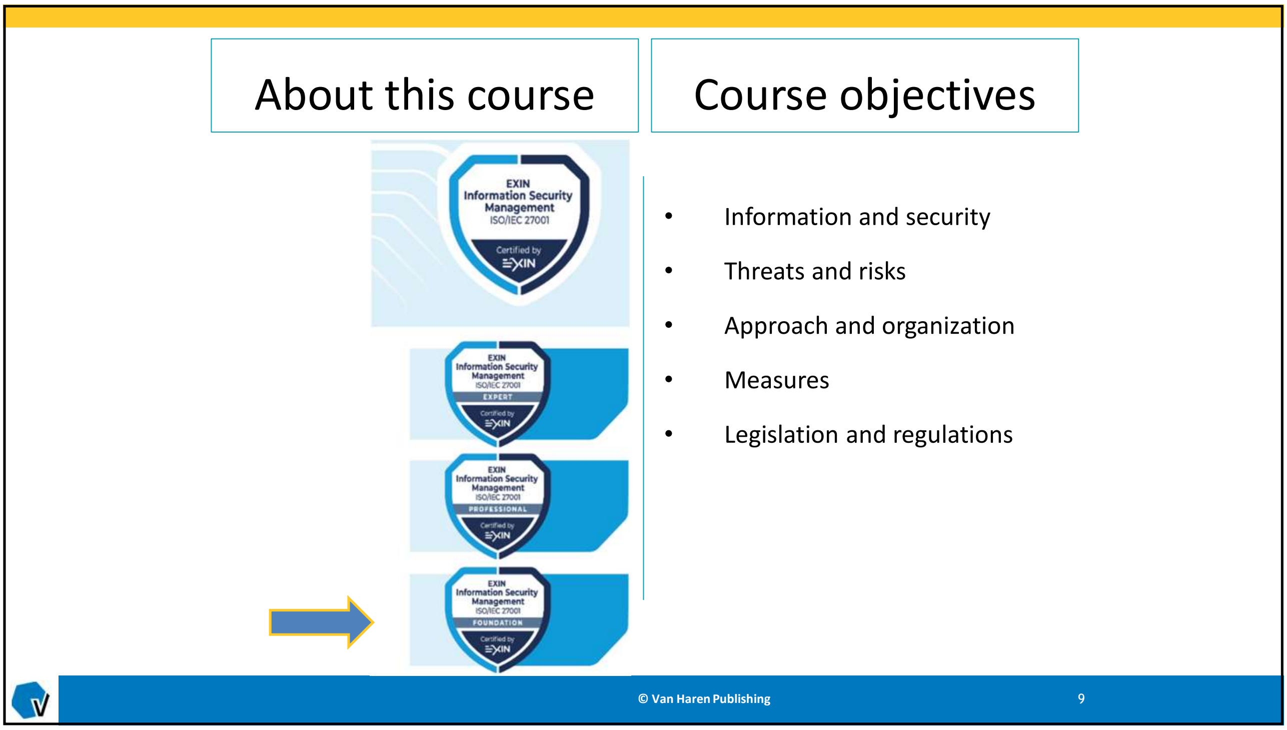
© Van Haren Publishing 7



ISO/IEC 27001 and 27002

- 27001:
  - International standard for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS
  - Describes what must be done
  - Organizations can get certified for this
- 27002:
  - Contains best practices
  - Describes how it should be done
  - Contains controls and measures
  - People can get certified

© Van Haren Publishing 8



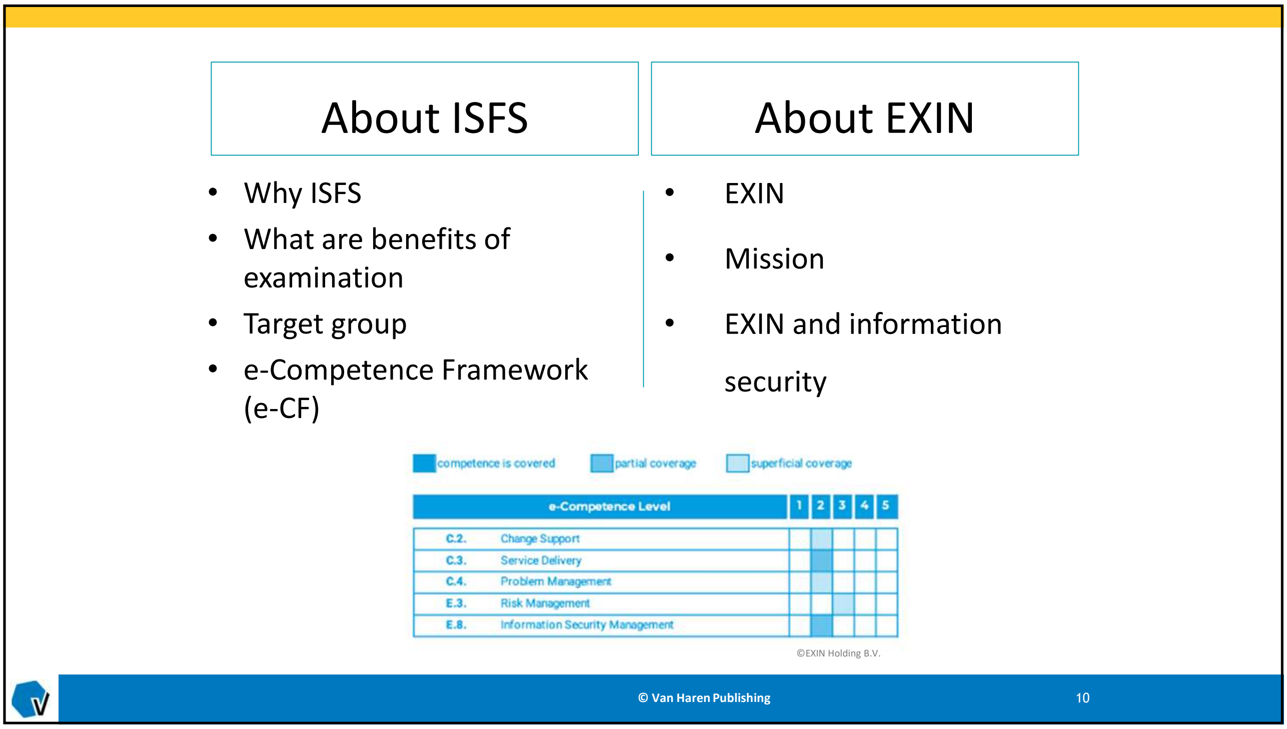
About this course

Course objectives

- Information and security
- Threats and risks
- Approach and organization
- Measures
- Legislation and regulations

EXIN
Information Security Management
ISO/IEC 27001
Certified by EXIN
EXPERT
PROFESSIONAL
FOUNDATION

© Van Haren Publishing 9



About ISFS

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

About EXIN

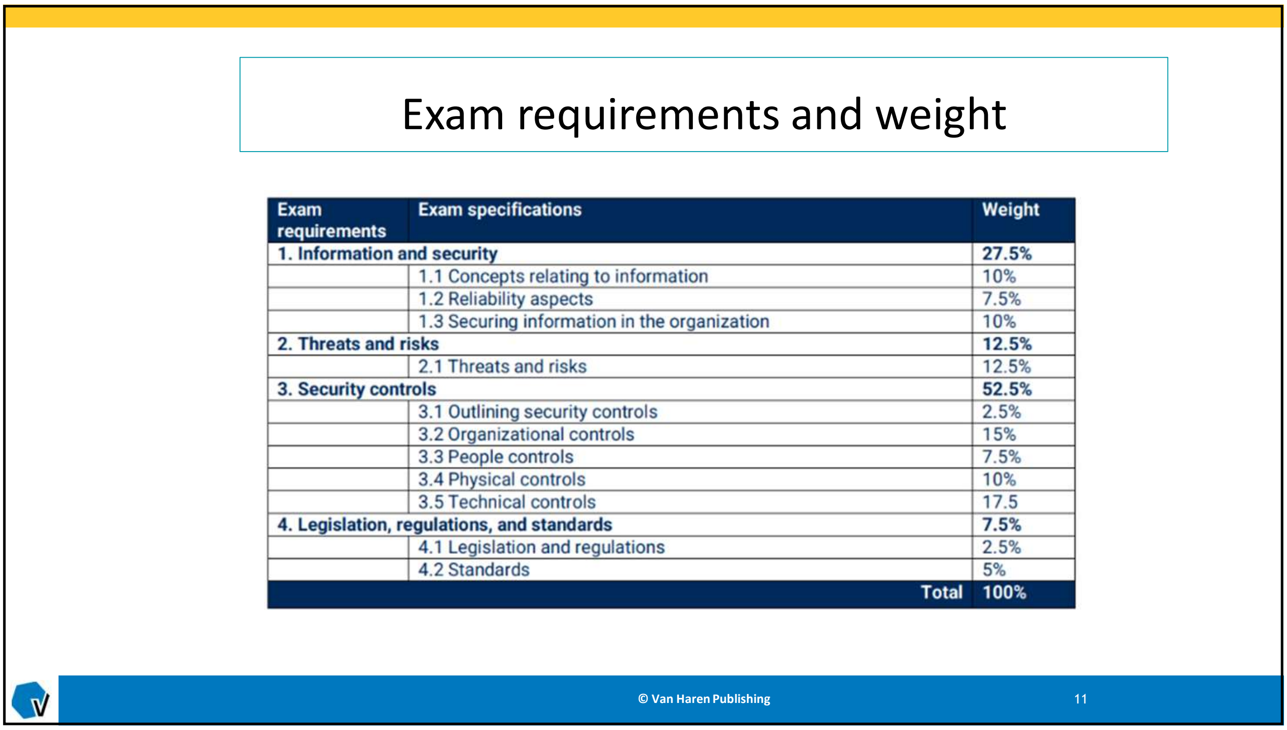
- EXIN
- Mission
- EXIN and information security

■ competence is covered ▨ partial coverage ░ superficial coverage

e-Competence Level		1	2	3	4	5
C.2.	Change Support		░			
C.3.	Service Delivery		▨			
C.4.	Problem Management		░			
E.3.	Risk Management			░		
E.8.	Information Security Management		▨			

©EXIN Holding B.V.

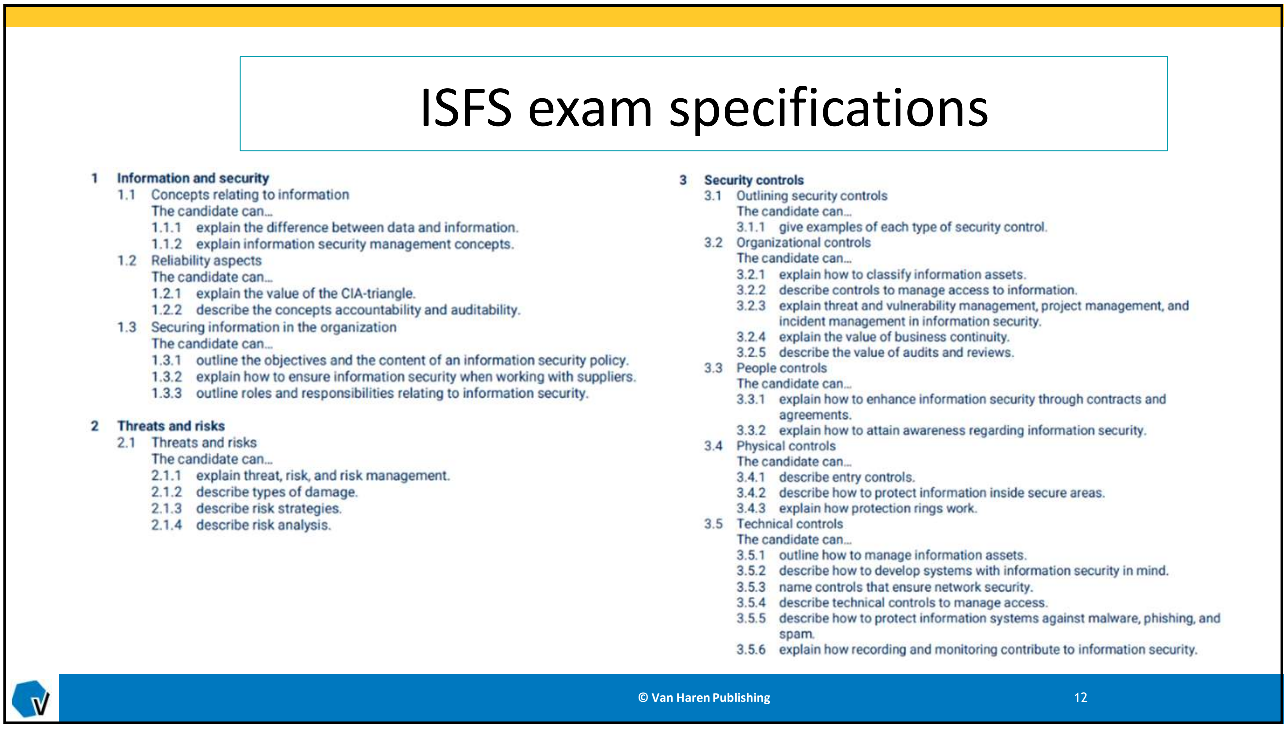
© Van Haren Publishing 10



Exam requirements and weight

Exam requirements	Exam specifications	Weight
1. Information and security		**27.5%**
	1.1 Concepts relating to information	10%
	1.2 Reliability aspects	7.5%
	1.3 Securing information in the organization	10%
2. Threats and risks		**12.5%**
	2.1 Threats and risks	12.5%
3. Security controls		**52.5%**
	3.1 Outlining security controls	2.5%
	3.2 Organizational controls	15%
	3.3 People controls	7.5%
	3.4 Physical controls	10%
	3.5 Technical controls	17.5
4. Legislation, regulations, and standards		**7.5%**
	4.1 Legislation and regulations	2.5%
	4.2 Standards	5%
	Total	**100%**

© Van Haren Publishing 11



ISFS exam specifications

1 Information and security

1.1 Concepts relating to information
The candidate can…
1.1.1 explain the difference between data and information.
1.1.2 explain information security management concepts.

1.2 Reliability aspects
The candidate can…
1.2.1 explain the value of the CIA-triangle.
1.2.2 describe the concepts accountability and auditability.

1.3 Securing information in the organization
The candidate can…
1.3.1 outline the objectives and the content of an information security policy.
1.3.2 explain how to ensure information security when working with suppliers.
1.3.3 outline roles and responsibilities relating to information security.

2 Threats and risks

2.1 Threats and risks
The candidate can…
2.1.1 explain threat, risk, and risk management.
2.1.2 describe types of damage.
2.1.3 describe risk strategies.
2.1.4 describe risk analysis.

3 Security controls

3.1 Outlining security controls
The candidate can…
3.1.1 give examples of each type of security control.

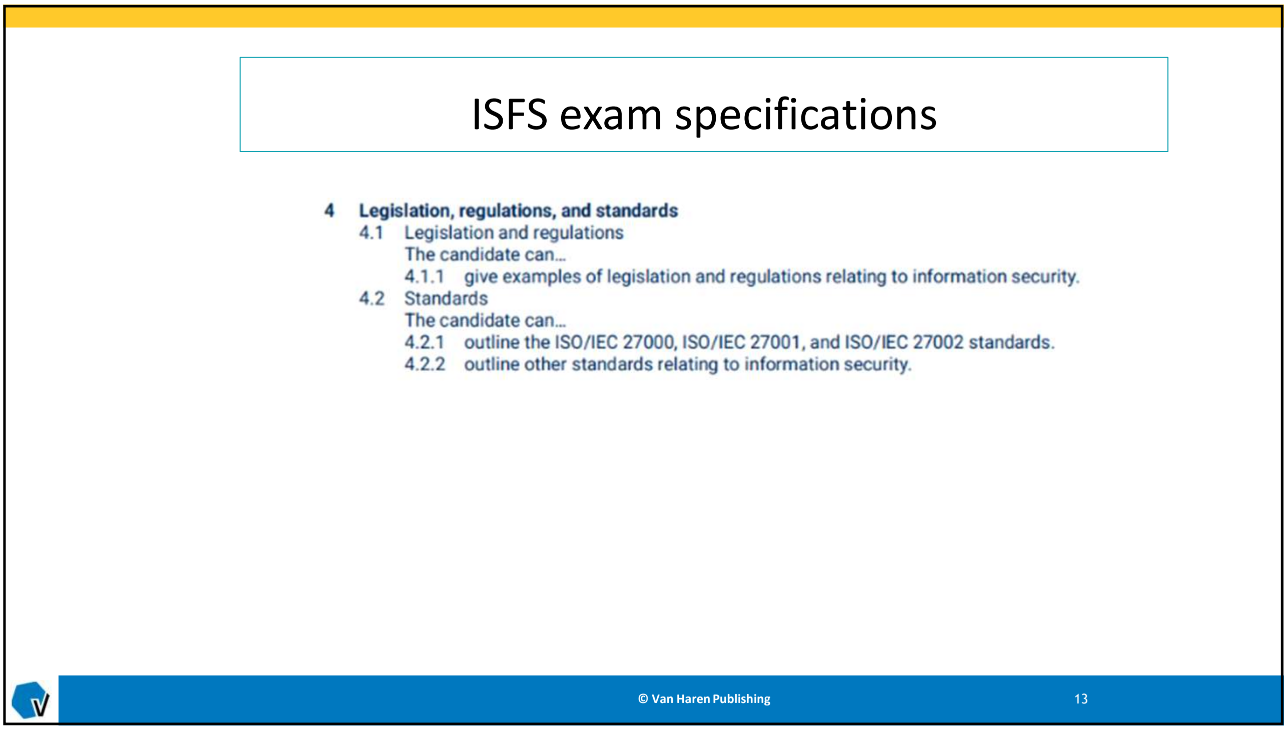
3.2 Organizational controls
The candidate can…
3.2.1 explain how to classify information assets.
3.2.2 describe controls to manage access to information.
3.2.3 explain threat and vulnerability management, project management, and incident management in information security.
3.2.4 explain the value of business continuity.
3.2.5 describe the value of audits and reviews.

3.3 People controls
The candidate can…
3.3.1 explain how to enhance information security through contracts and agreements.
3.3.2 explain how to attain awareness regarding information security.

3.4 Physical controls
The candidate can…
3.4.1 describe entry controls.
3.4.2 describe how to protect information inside secure areas.
3.4.3 explain how protection rings work.

3.5 Technical controls
The candidate can…
3.5.1 outline how to manage information assets.
3.5.2 describe how to develop systems with information security in mind.
3.5.3 name controls that ensure network security.
3.5.4 describe technical controls to manage access.
3.5.5 describe how to protect information systems against malware, phishing, and spam.
3.5.6 explain how recording and monitoring contribute to information security.

© Van Haren Publishing 12



ISFS exam specifications

4 Legislation, regulations, and standards

4.1 Legislation and regulations

The candidate can…

4.1.1 give examples of legislation and regulations relating to information security.

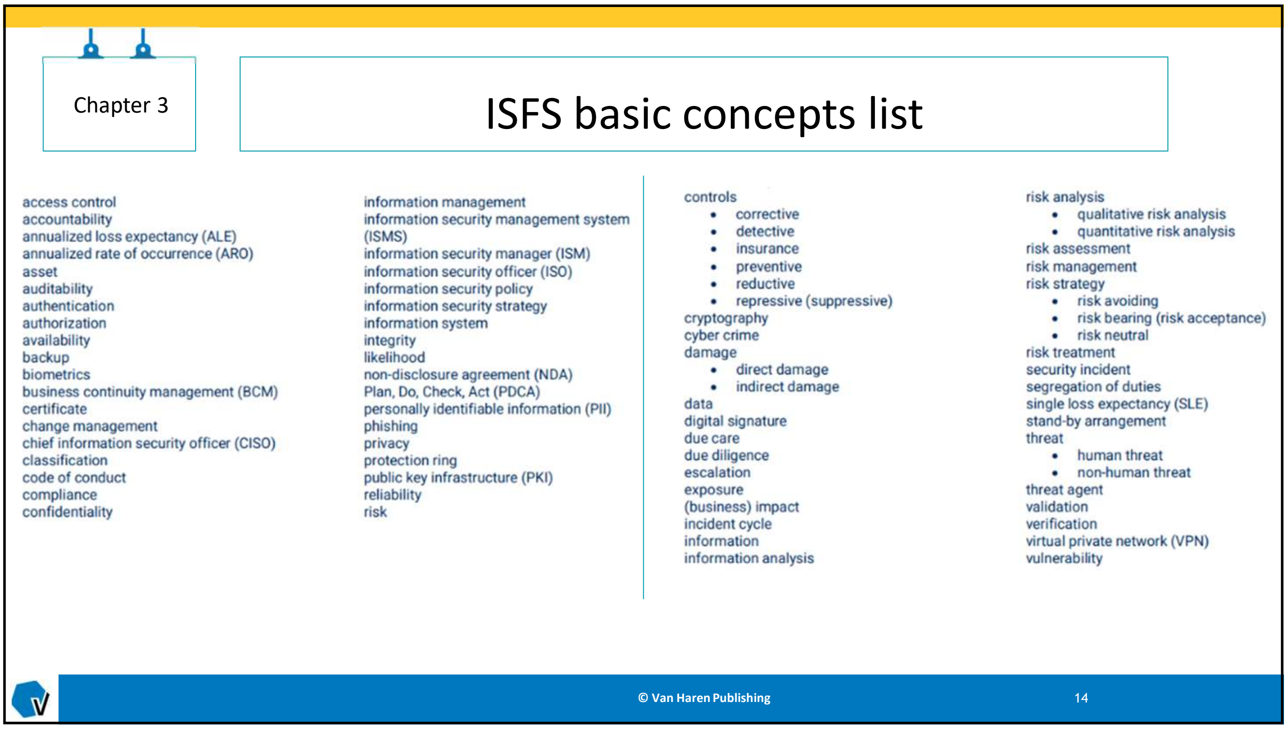
4.2 Standards

The candidate can…

4.2.1 outline the ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002 standards.

4.2.2 outline other standards relating to information security.

© Van Haren Publishing 13



Chapter 3

ISFS basic concepts list

access control
accountability
annualized loss expectancy (ALE)
annualized rate of occurrence (ARO)
asset
auditability
authentication
authorization
availability
backup
biometrics
business continuity management (BCM)
certificate
change management
chief information security officer (CISO)
classification
code of conduct
compliance
confidentiality

information management
information security management system (ISMS)
information security manager (ISM)
information security officer (ISO)
information security policy
information security strategy
information system
integrity
likelihood
non-disclosure agreement (NDA)
Plan, Do, Check, Act (PDCA)
personally identifiable information (PII)
phishing
privacy
protection ring
public key infrastructure (PKI)
reliability
risk

controls
- corrective
- detective
- insurance
- preventive
- reductive
- repressive (suppressive)

cryptography
cyber crime
damage
- direct damage
- indirect damage

data
digital signature
due care
due diligence
escalation
exposure
(business) impact
incident cycle
information
information analysis

risk analysis
- qualitative risk analysis
- quantitative risk analysis

risk assessment
risk management
risk strategy
- risk avoiding
- risk bearing (risk acceptance)
- risk neutral

risk treatment
security incident
segregation of duties
single loss expectancy (SLE)
stand-by arrangement
threat
- human threat
- non-human threat

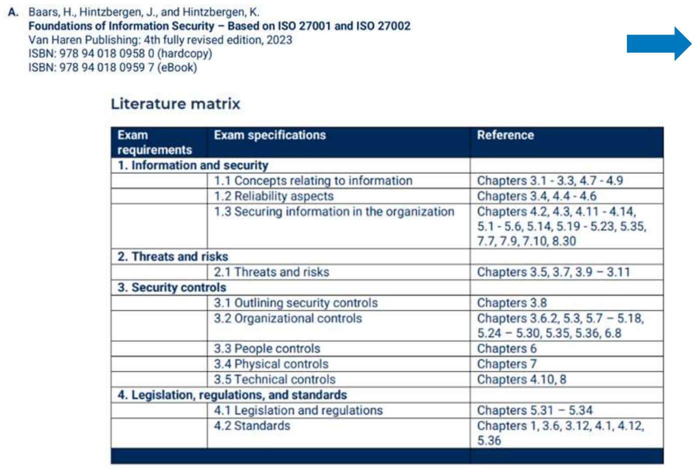
threat agent
validation
verification
virtual private network (VPN)
vulnerability

© Van Haren Publishing 14

Contents

ISFS literature

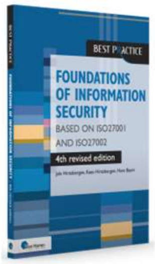
Exam literature



A. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing: 4th fully revised edition, 2023
ISBN: 978 94 018 0958 0 (hardcopy)
ISBN: 978 94 018 0959 7 (eBook)

Literature matrix

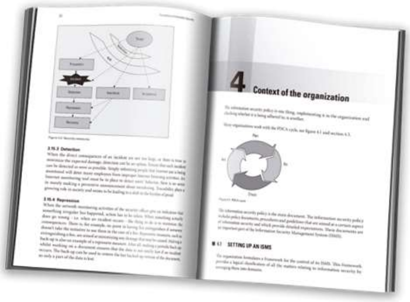
Exam requirements	Exam specifications	Reference
1. Information and security		
	1.1 Concepts relating to information	Chapters 3.1 - 3.3, 4.7 - 4.9
	1.2 Reliability aspects	Chapters 3.4, 4.4 - 4.6
	1.3 Securing information in the organization	Chapters 4.2, 4.3, 4.11 - 4.14, 5.1 - 5.6, 5.14, 5.19 - 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. Threats and risks		
	2.1 Threats and risks	Chapters 3.5, 3.7, 3.9 – 3.11
3. Security controls		
	3.1 Outlining security controls	Chapters 3.8
	3.2 Organizational controls	Chapters 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.3 People controls	Chapters 6
	3.4 Physical controls	Chapters 7
	3.5 Technical controls	Chapters 4.10, 8
4. Legislation, regulations, and standards		
	4.1 Legislation and regulations	Chapters 5.31 – 5.34
	4.2 Standards	Chapters 1, 3.6, 3.12, 4.1, 4.12, 5.36

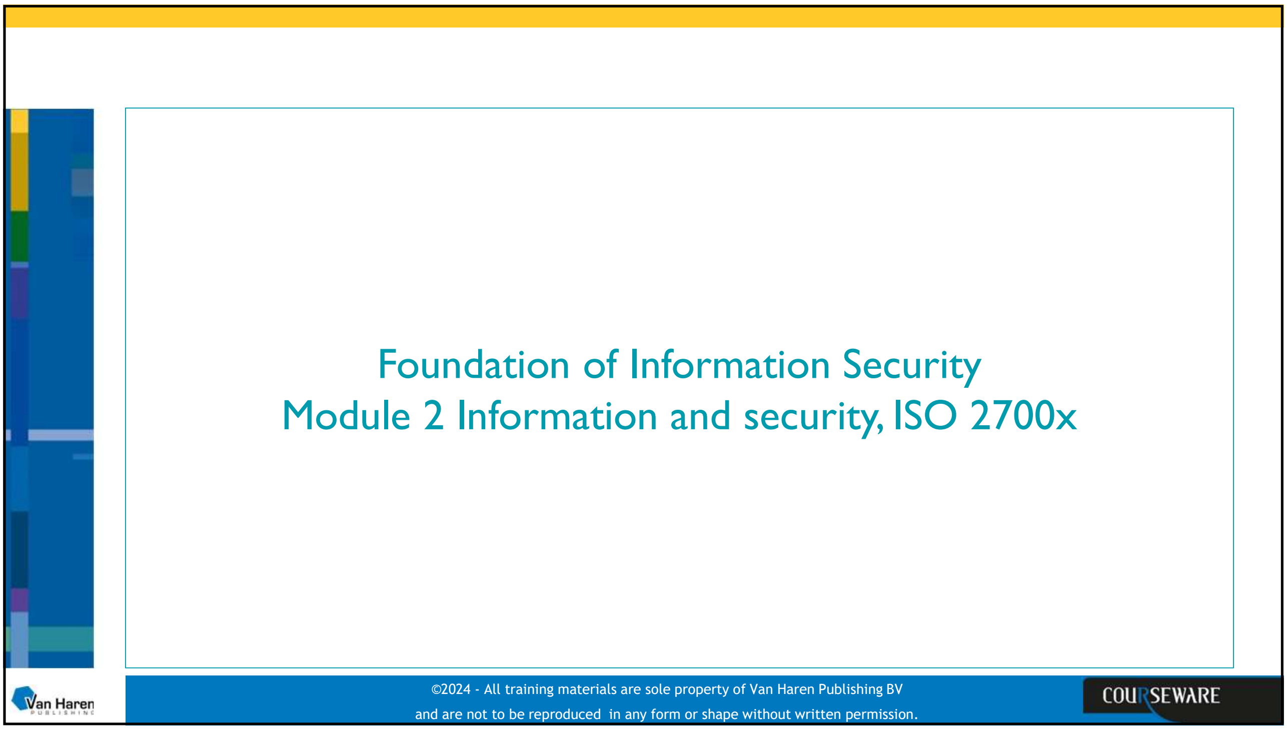


Chapter 1

About the book

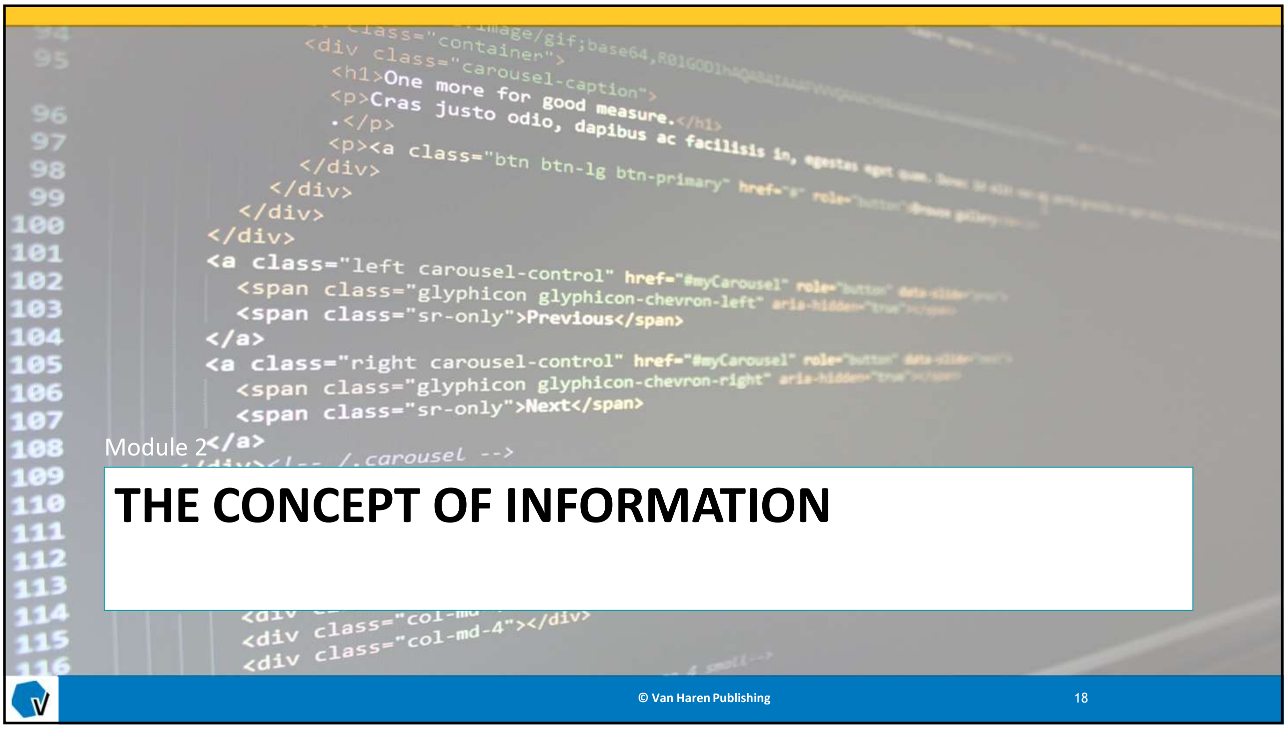
- Provides a basic understanding of information security
- Official training guide for EXIN exam Information Security Foundation
- Contains Case studies
- Contains a ISFS model exam
- Feedback to all multiple choice options





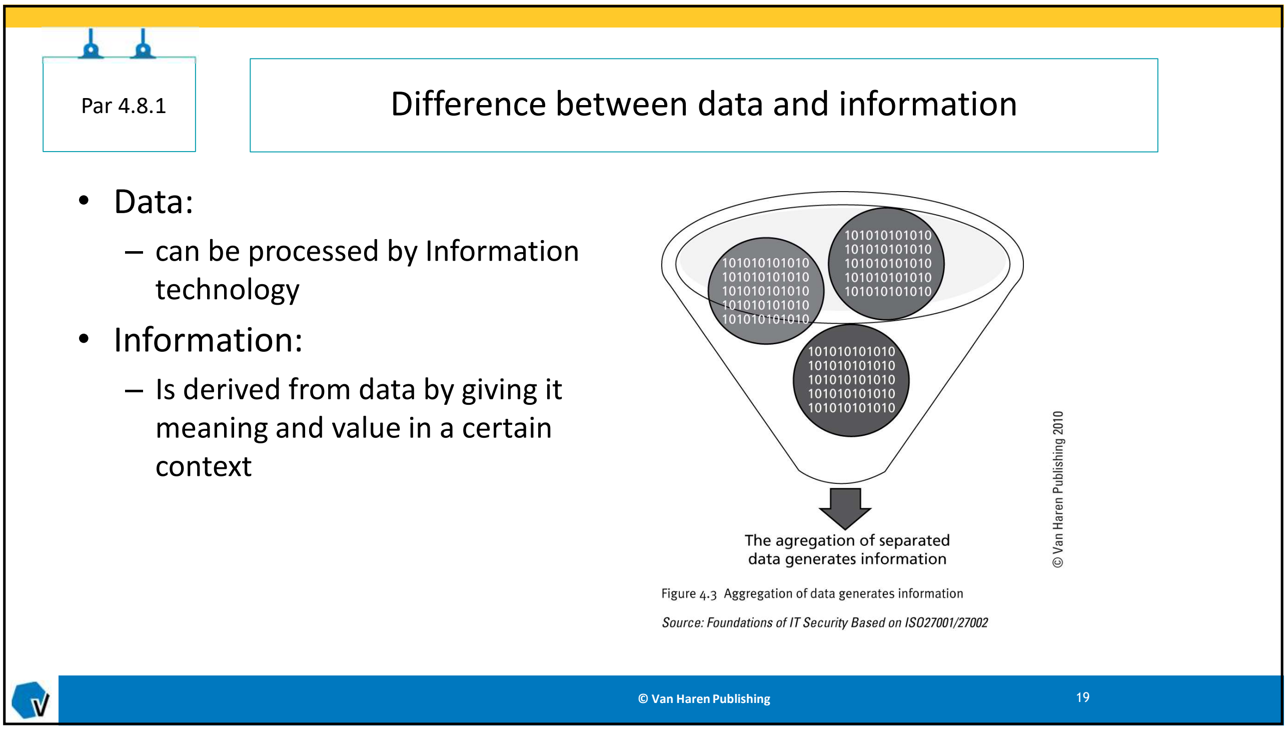
Foundation of Information Security
Module 2 Information and security, ISO 2700x

Van Haren
COURSEWARE



Module 2

THE CONCEPT OF INFORMATION



Par 4.8.1

Difference between data and information

- Data:
  - can be processed by Information technology
- Information:
  - Is derived from data by giving it meaning and value in a certain context

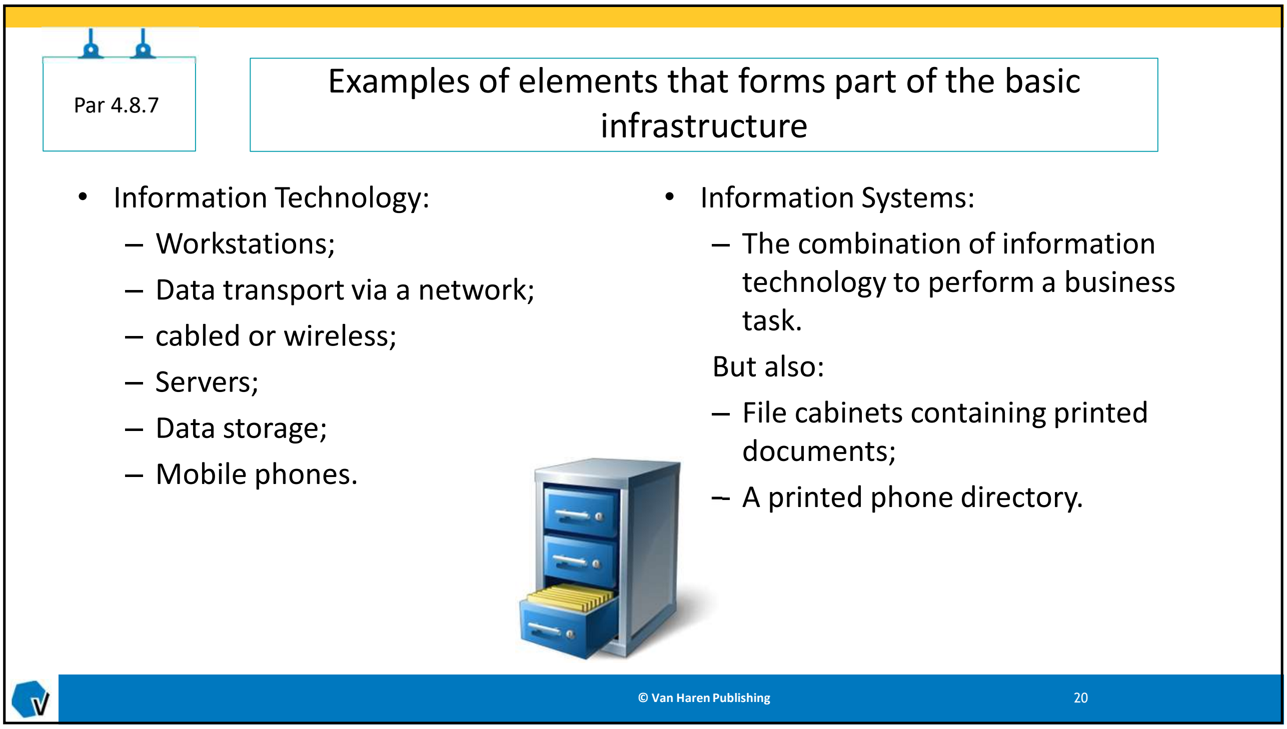
101010101010
101010101010
101010101010
101010101010
101010101010

The agregation of separated data generates information

© Van Haren Publishing 2010

Figure 4.3 Aggregation of data generates information

Source: Foundations of IT Security Based on ISO27001/27002

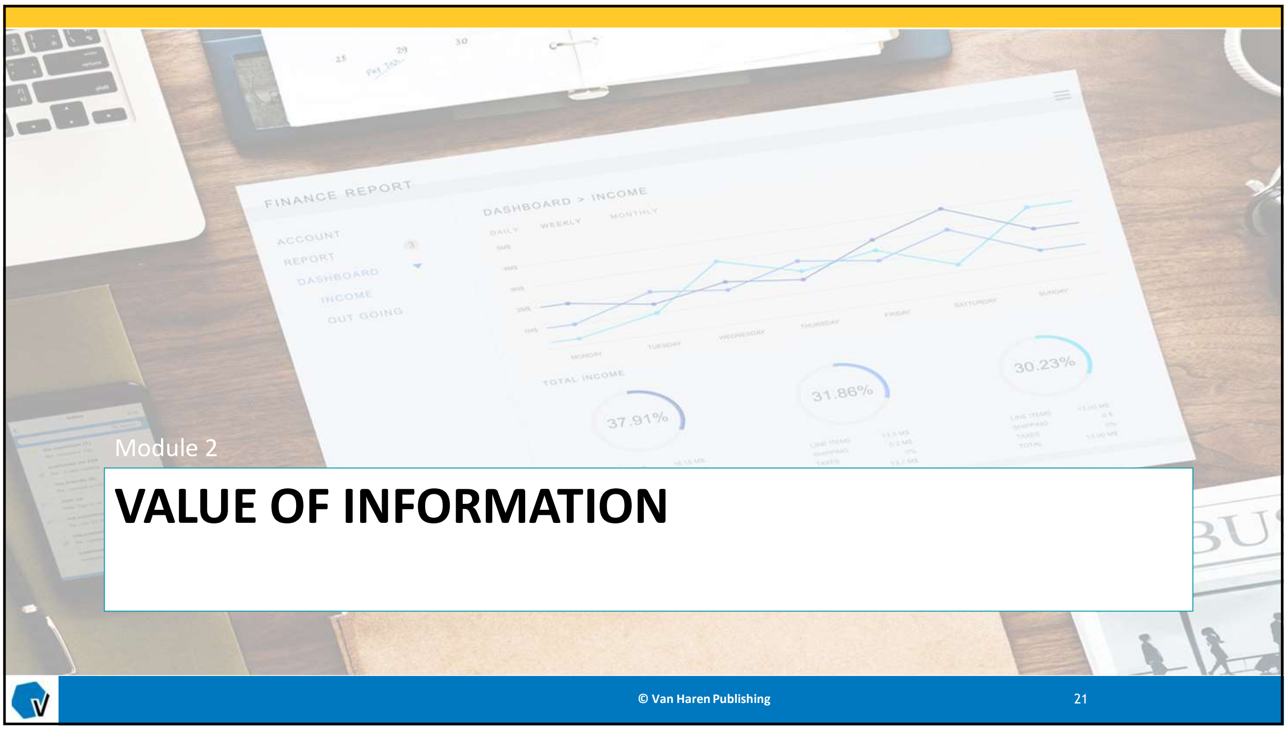


Par 4.8.7

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.
- Information Systems:
  - The combination of information technology to perform a business task.

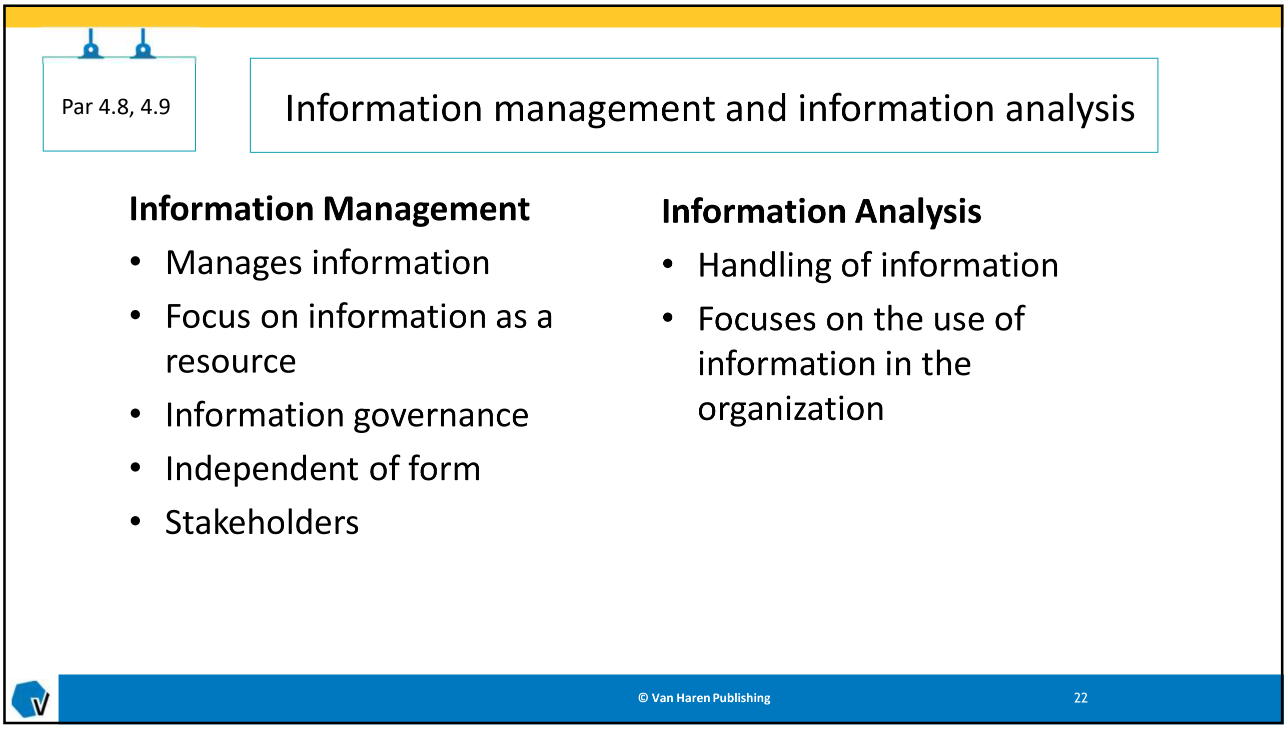
  But also:
  - File cabinets containing printed documents;
  - A printed phone directory.



Module 2

VALUE OF INFORMATION

© Van Haren Publishing 21



Par 4.8, 4.9

Information management and information analysis

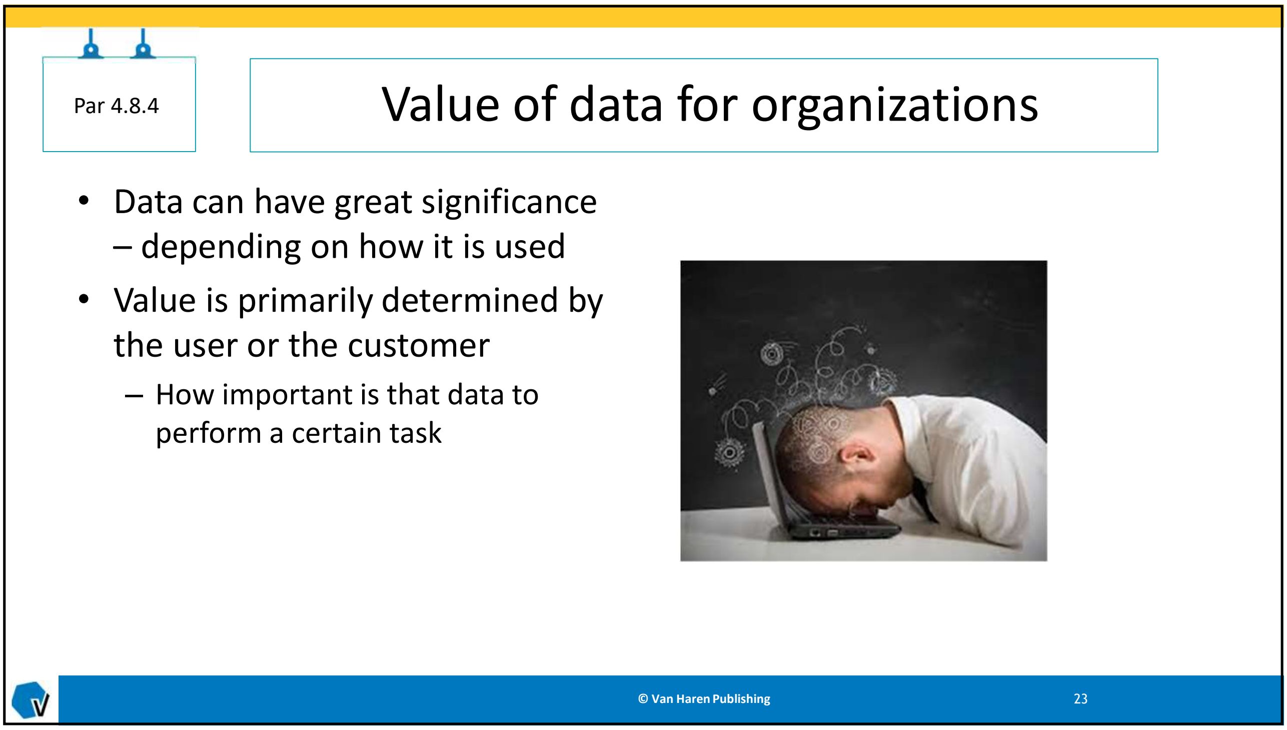
Information Management

- Manages information
- Focus on information as a resource
- Information governance
- Independent of form
- Stakeholders

Information Analysis

- Handling of information
- Focuses on the use of information in the organization

© Van Haren Publishing 22



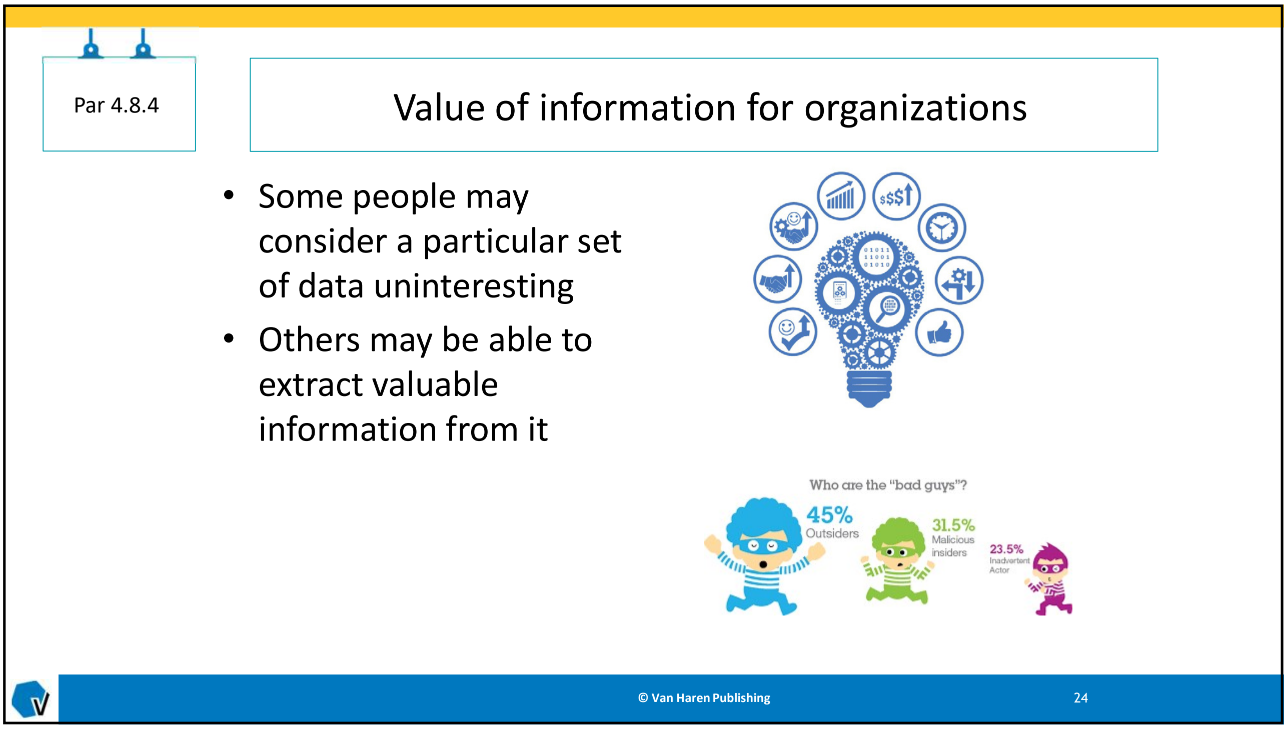
Par 4.8.4

Value of data for organizations

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

© Van Haren Publishing

23



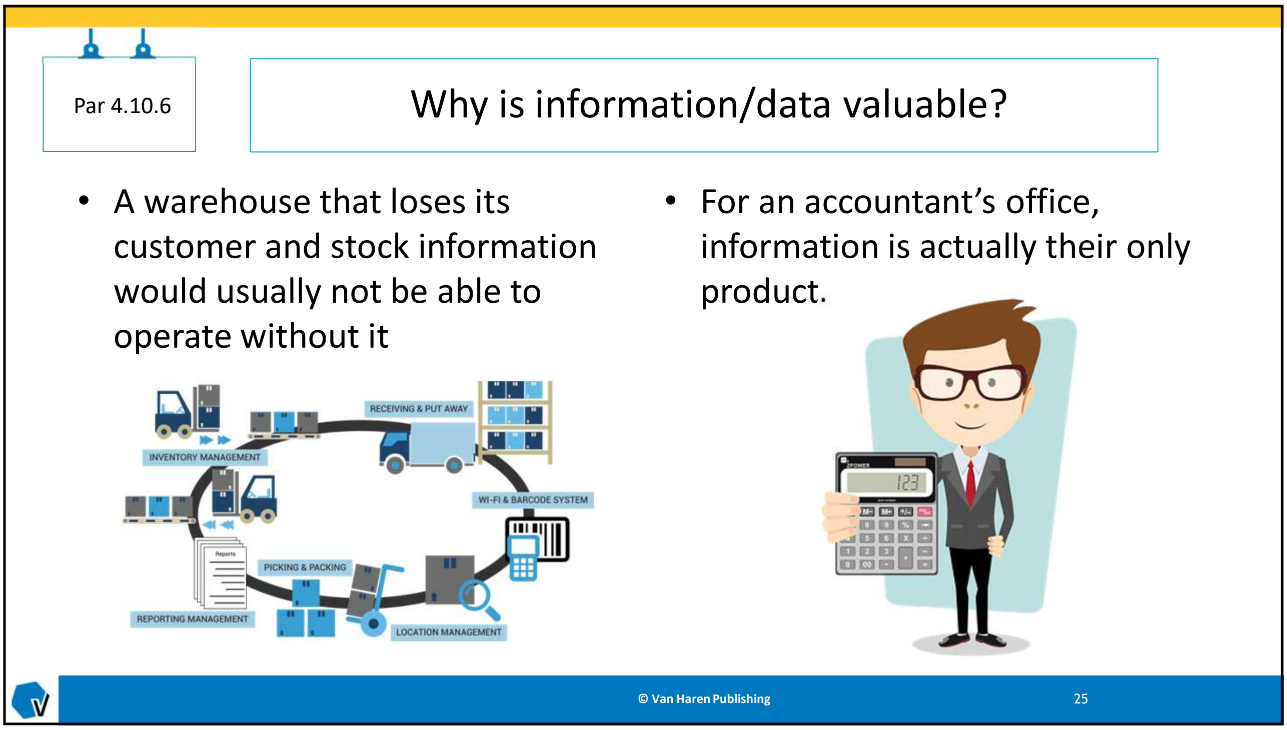
Par 4.8.4

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

24



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.

Par 3.6

New in ISO 27002:2022;
Think for yourself: the introduction of attributes

Control types
#Preventive
#Detective
#Corrective

Information security properties
#Confidentiality
#Integrity
#Availability

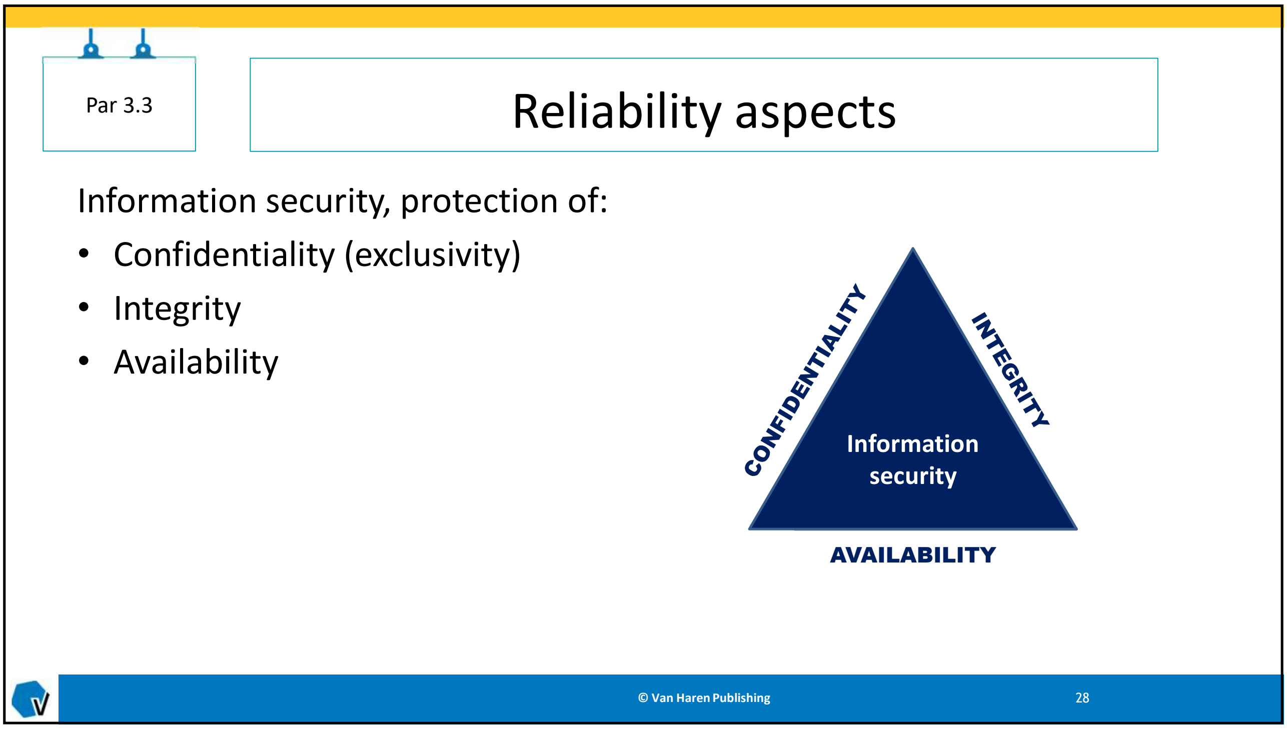
Cybersecurity concepts
#Identify
#Protect
#Detect
#Respond
#Recover

Operational capabilities
#Governance
#Asset management
#Information protection
#Human resource security
#Physical security
#System and network security
#Application security
#Secure configuration
#Identity and access management
#Threat and vulnerability management
#Continuity
#Supplier relationships security
#Legal and compliance
#Information security event management
#Security assurance

This means that the organization first thinks about how it wants to set up its ISMS, only then do you delve into the controls.

Module 2

RELIABILITY ASPECTS



Par 3.3

Reliability aspects

Information security, protection of:

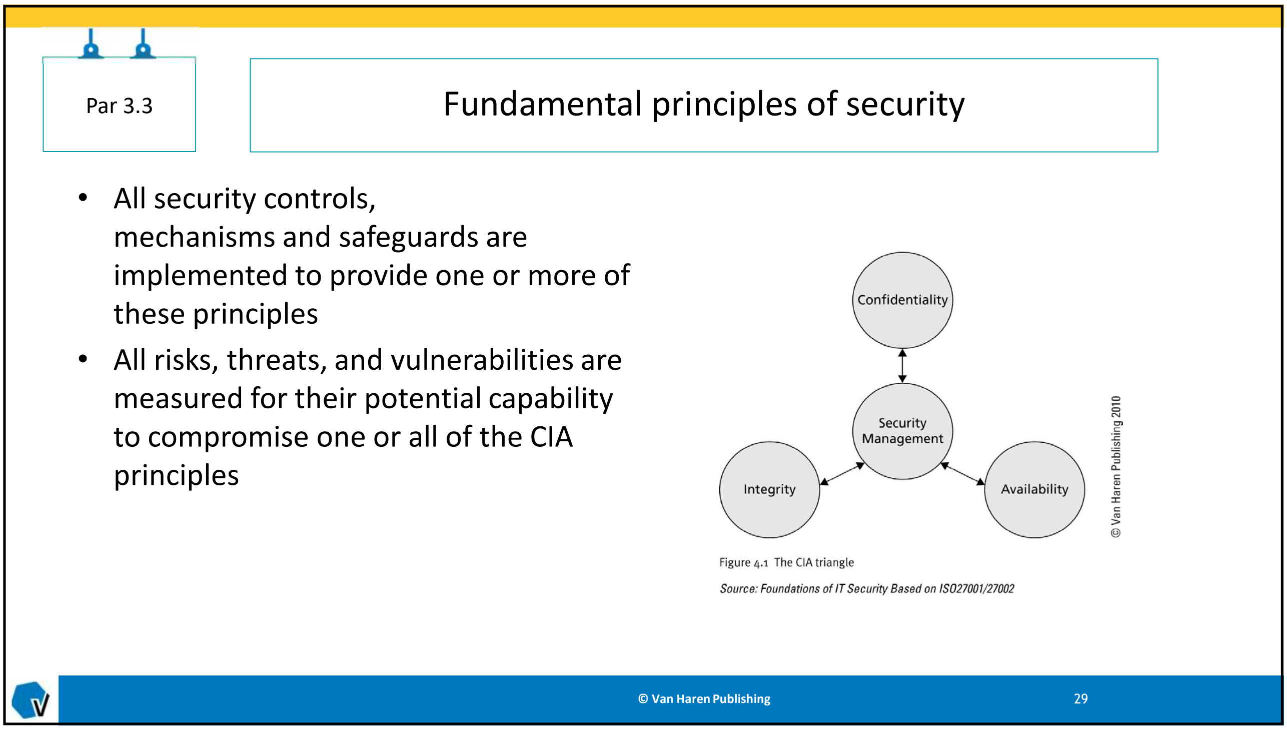
- Confidentiality (exclusivity)
- Integrity
- Availability

CONFIDENTIALITY

INTEGRITY

Information security

AVAILABILITY



Par 3.3

Fundamental principles of security

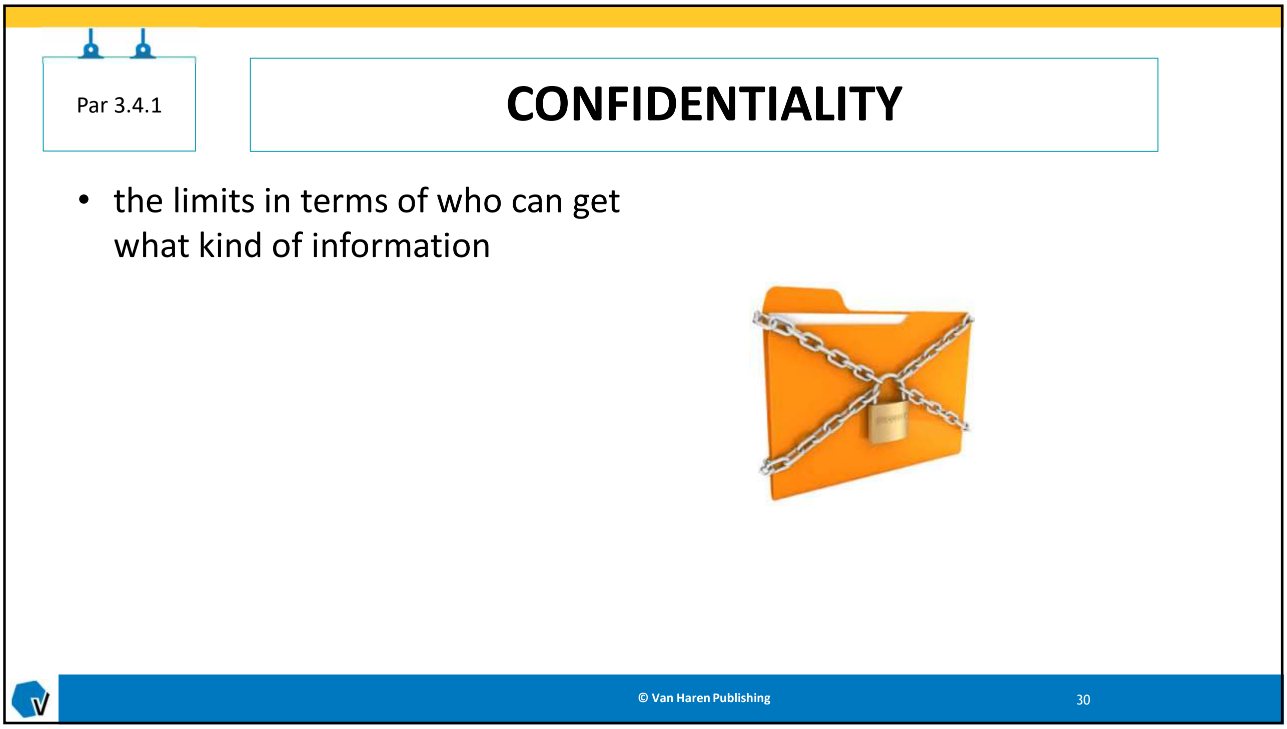
- All security controls, mechanisms and safeguards are implemented to provide one or more of these principles
- All risks, threats, and vulnerabilities are measured for their potential capability to compromise one or all of the CIA principles

© Van Haren Publishing 2010

Figure 4.1 The CIA triangle

Source: Foundations of IT Security Based on ISO27001/27002

© Van Haren Publishing 29



Par 3.4.1

CONFIDENTIALITY

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

© Van Haren Publishing 30

Par 3.2 / 3.4.1

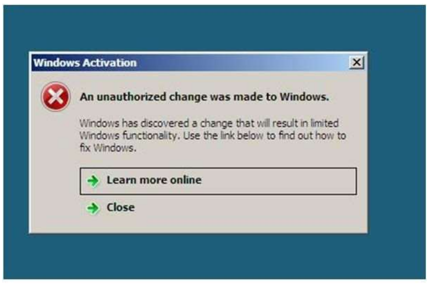
How applied information security concepts protect the value of data/information

- 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.

Par 3.4.2

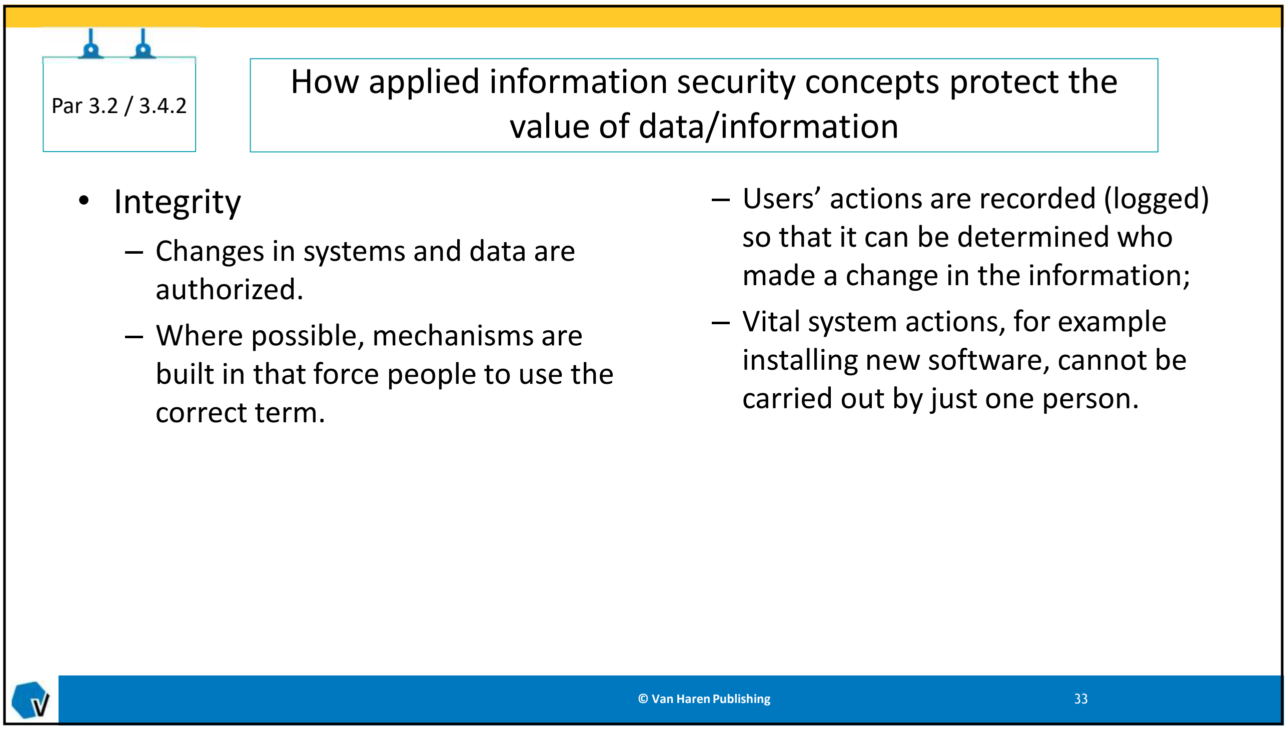
INTEGRITY

- 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.



An unauthorized change was made to Windows.

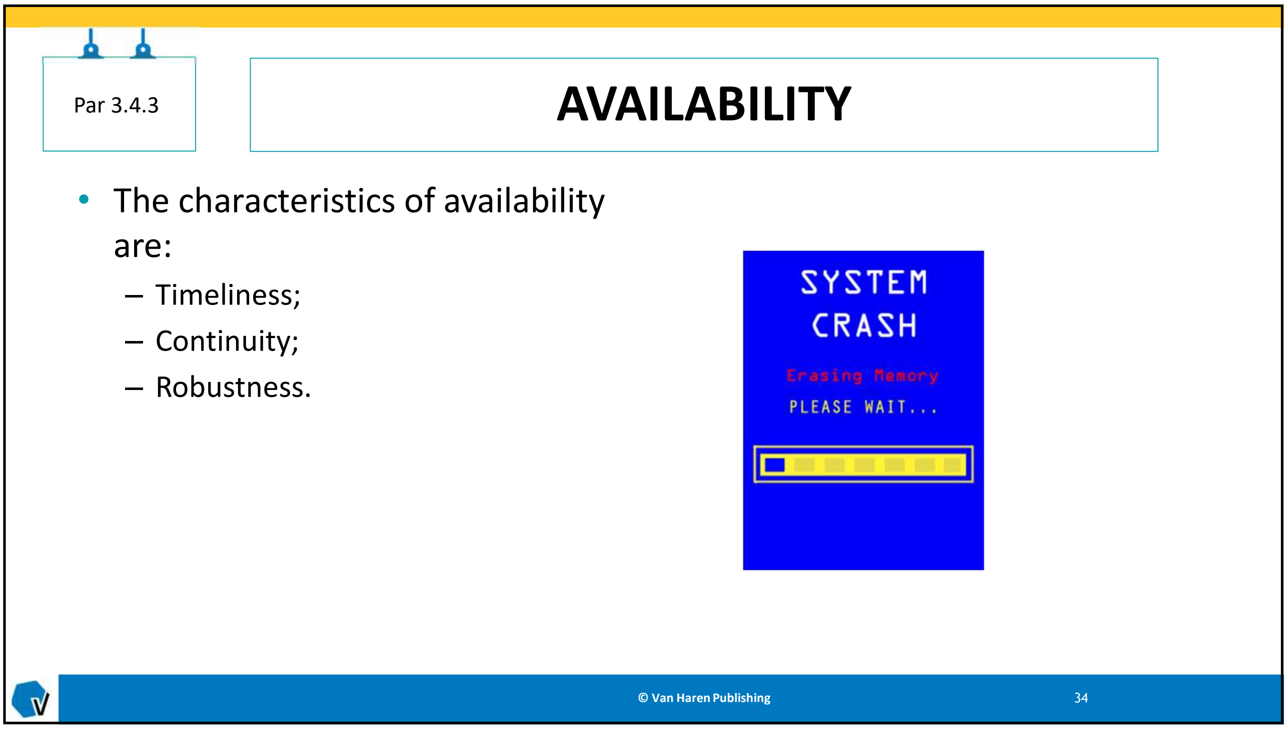
Windows has discovered a change that will result in limited Windows functionality. Use the link below to find out how to fix Windows.



Par 3.2 / 3.4.2

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.

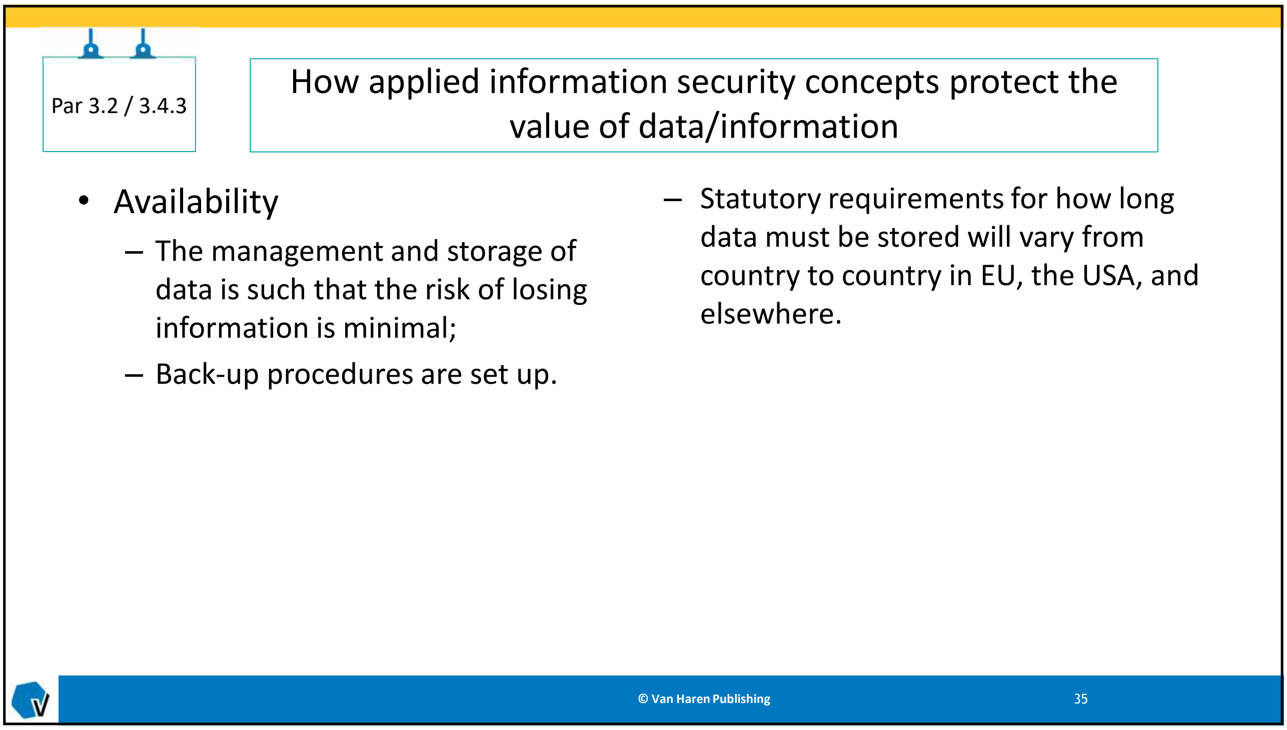


Par 3.4.3

AVAILABILITY

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

SYSTEM
CRASH
Erasing Memory
PLEASE WAIT...

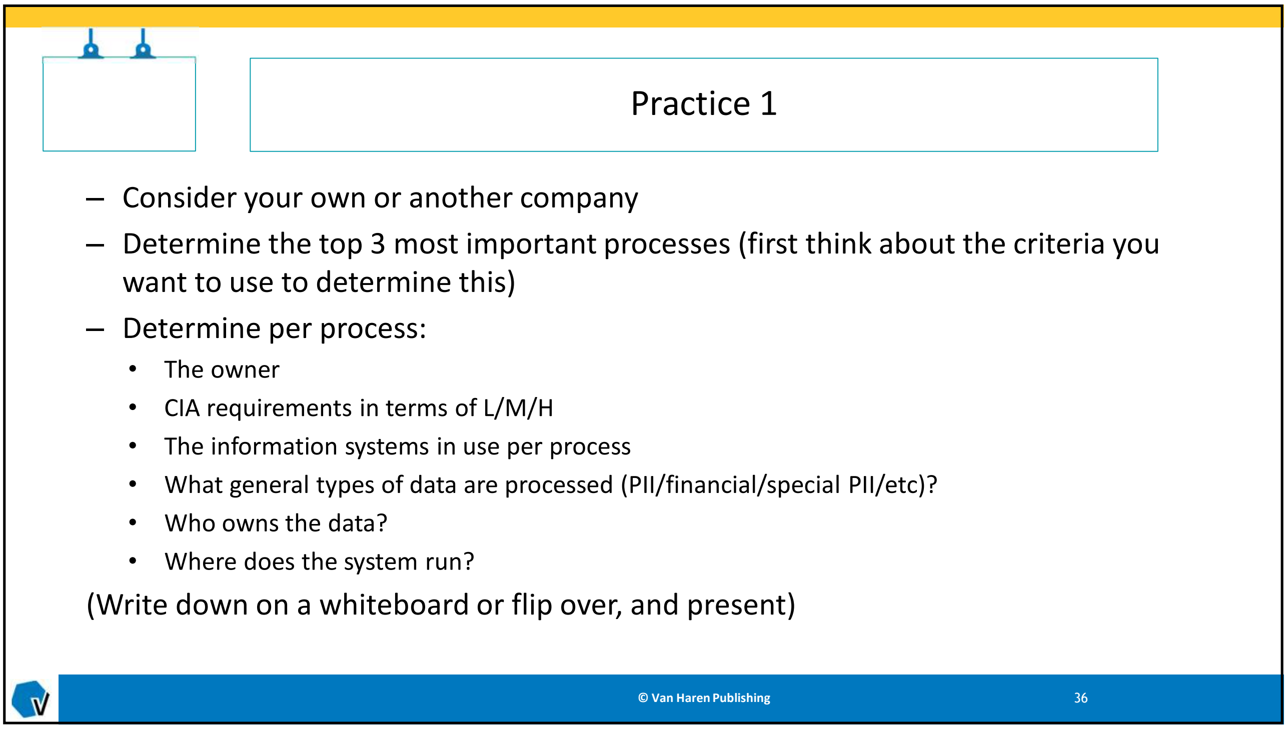


Par 3.2 / 3.4.3

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 35

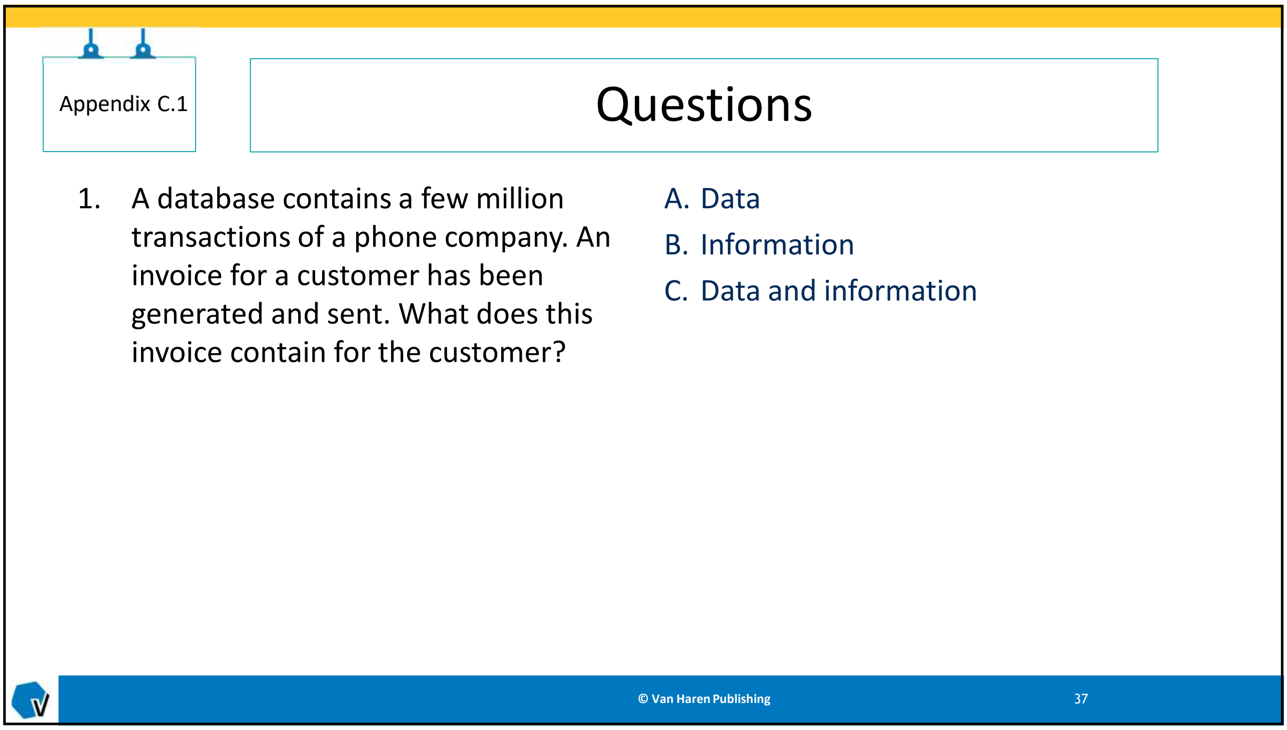


Practice 1

- Consider your own or another company
- Determine the top 3 most important processes (first think about the criteria you want to use to determine this)
- Determine per process:
  - The owner
  - CIA requirements in terms of L/M/H
  - The information systems in use per process
  - What general types of data are processed (PII/financial/special PII/etc)?
  - Who owns the data?
  - Where does the system run?

(Write down on a whiteboard or flip over, and present)

© Van Haren Publishing 36



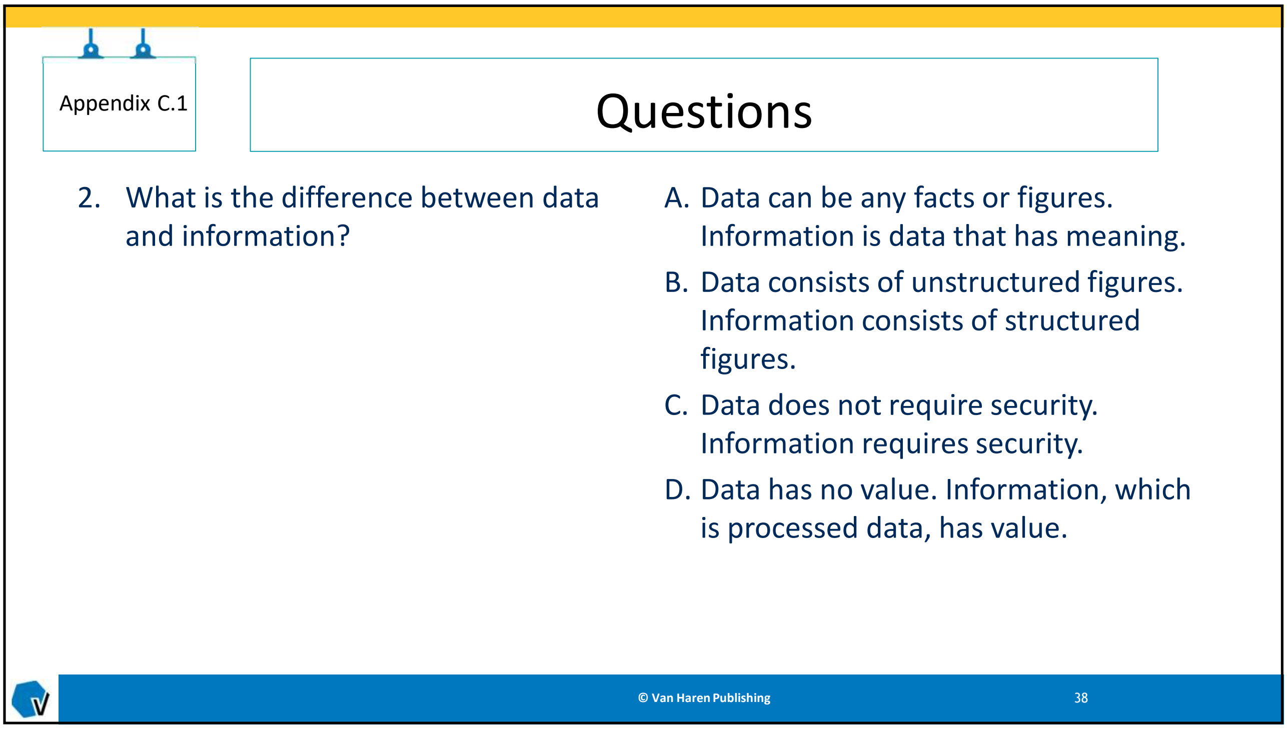
Appendix C.1

Questions

1. A database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent. What does this invoice contain for the customer?

A. Data
B. Information
C. Data and information

© Van Haren Publishing 37



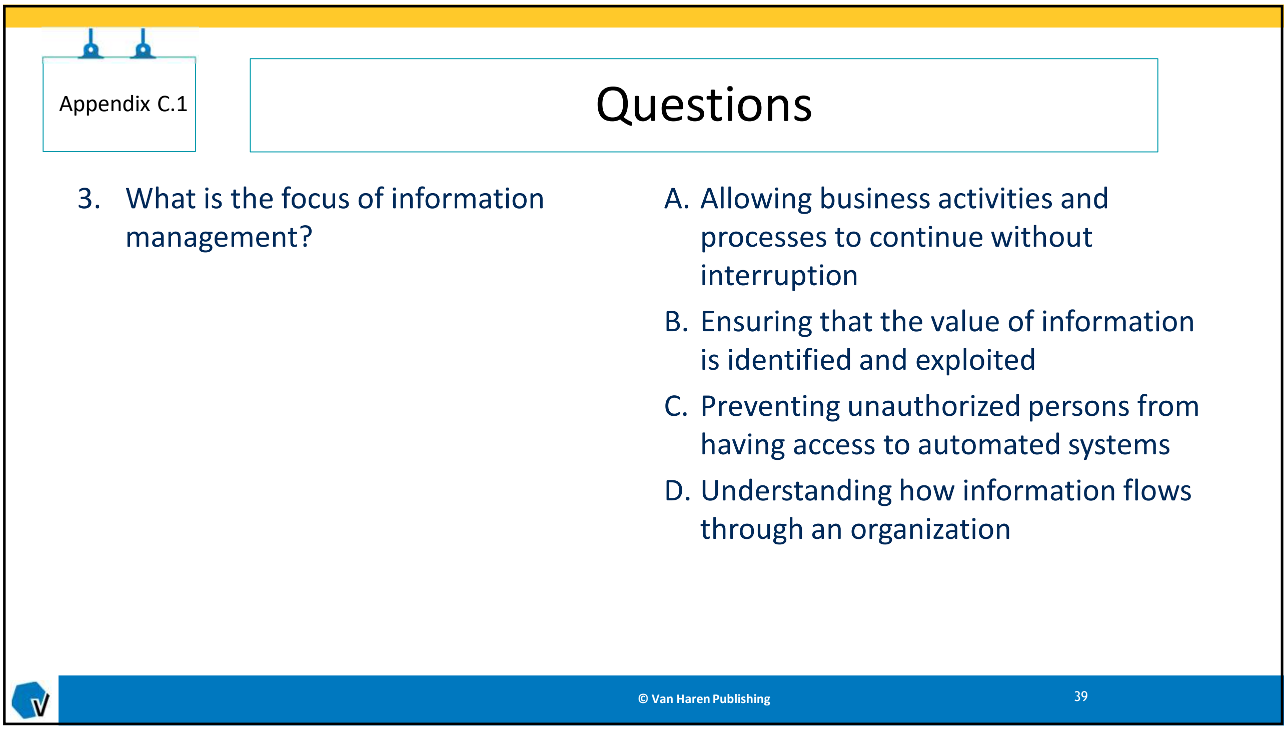
Appendix C.1

Questions

2. What is the difference between data and information?

A. Data can be any facts or figures. Information is data that has meaning.
B. Data consists of unstructured figures. Information consists of structured figures.
C. Data does not require security. Information requires security.
D. Data has no value. Information, which is processed data, has value.

© Van Haren Publishing 38



Appendix C.1

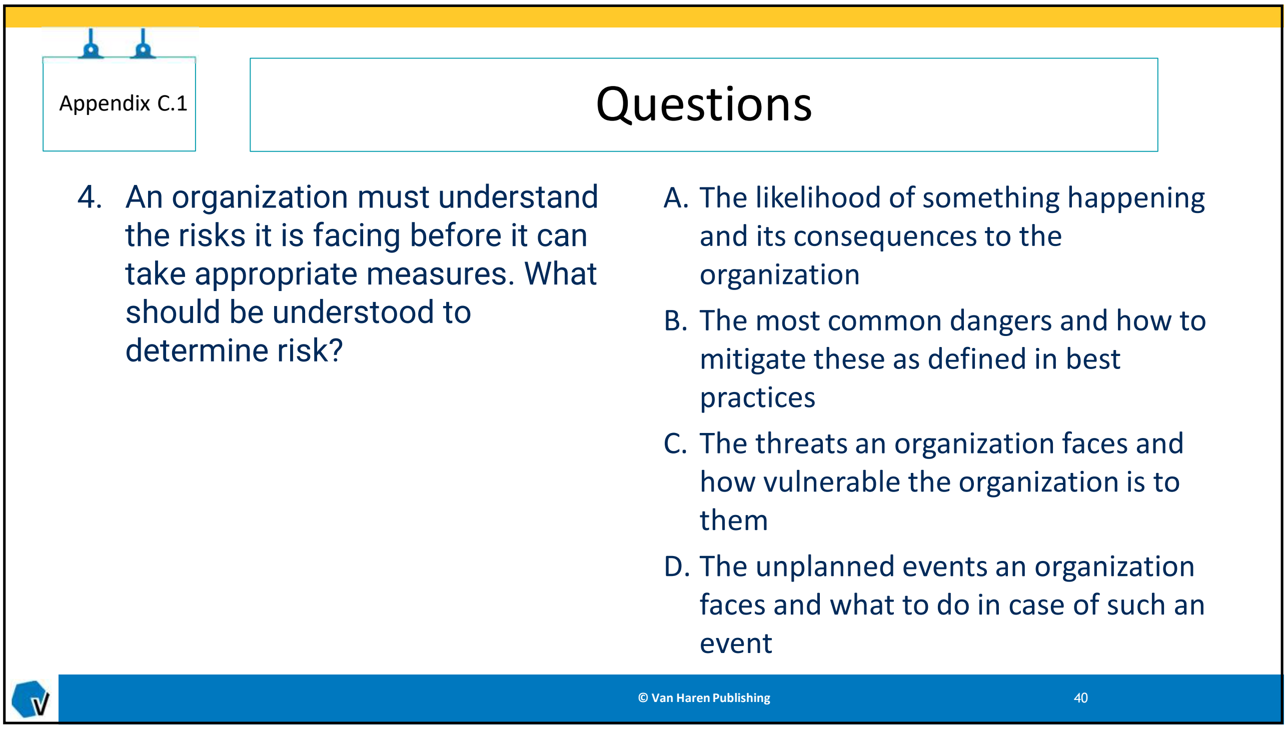
Questions

3. What is the focus of information management?

A. Allowing business activities and processes to continue without interruption
B. Ensuring that the value of information is identified and exploited
C. Preventing unauthorized persons from having access to automated systems
D. Understanding how information flows through an organization

© Van Haren Publishing

39



Appendix C.1

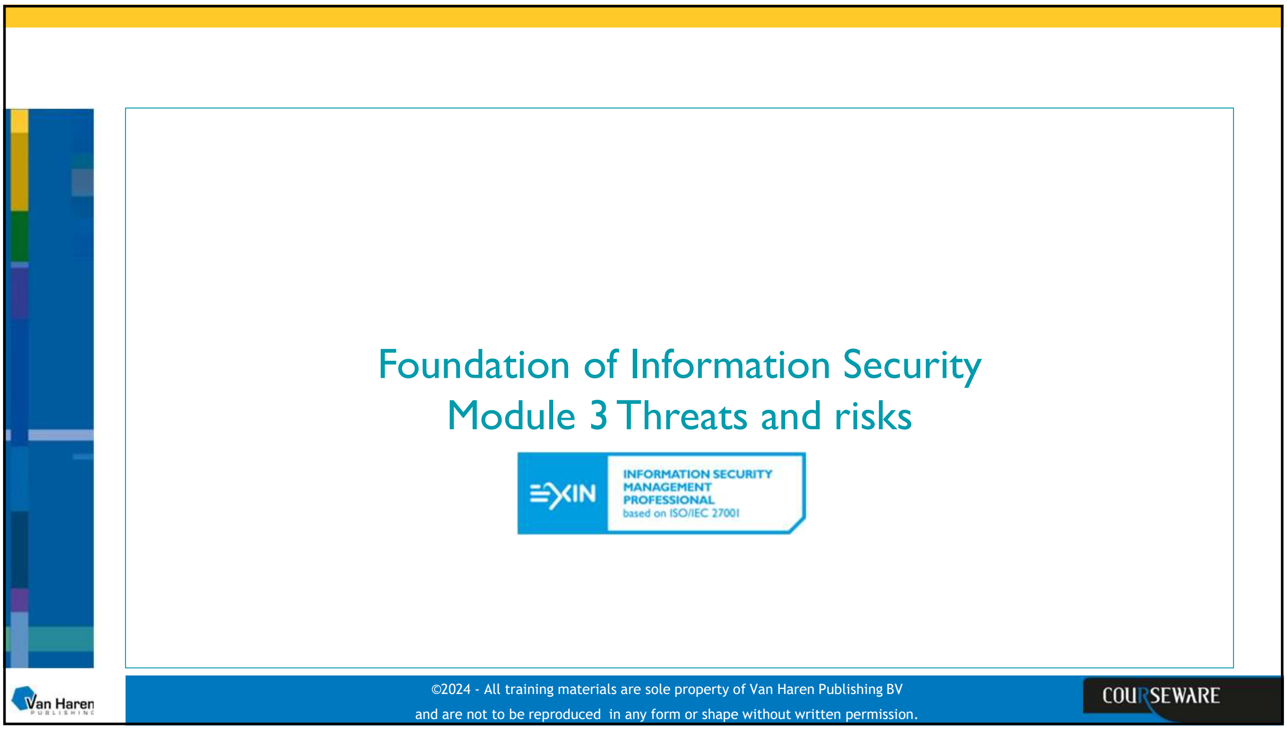
Questions

4. An organization must understand the risks it is facing before it can take appropriate measures. What should be understood to determine risk?

A. The likelihood of something happening and its consequences to the organization
B. The most common dangers and how to mitigate these as defined in best practices
C. The threats an organization faces and how vulnerable the organization is to them
D. The unplanned events an organization faces and what to do in case of such an event

© Van Haren Publishing

40

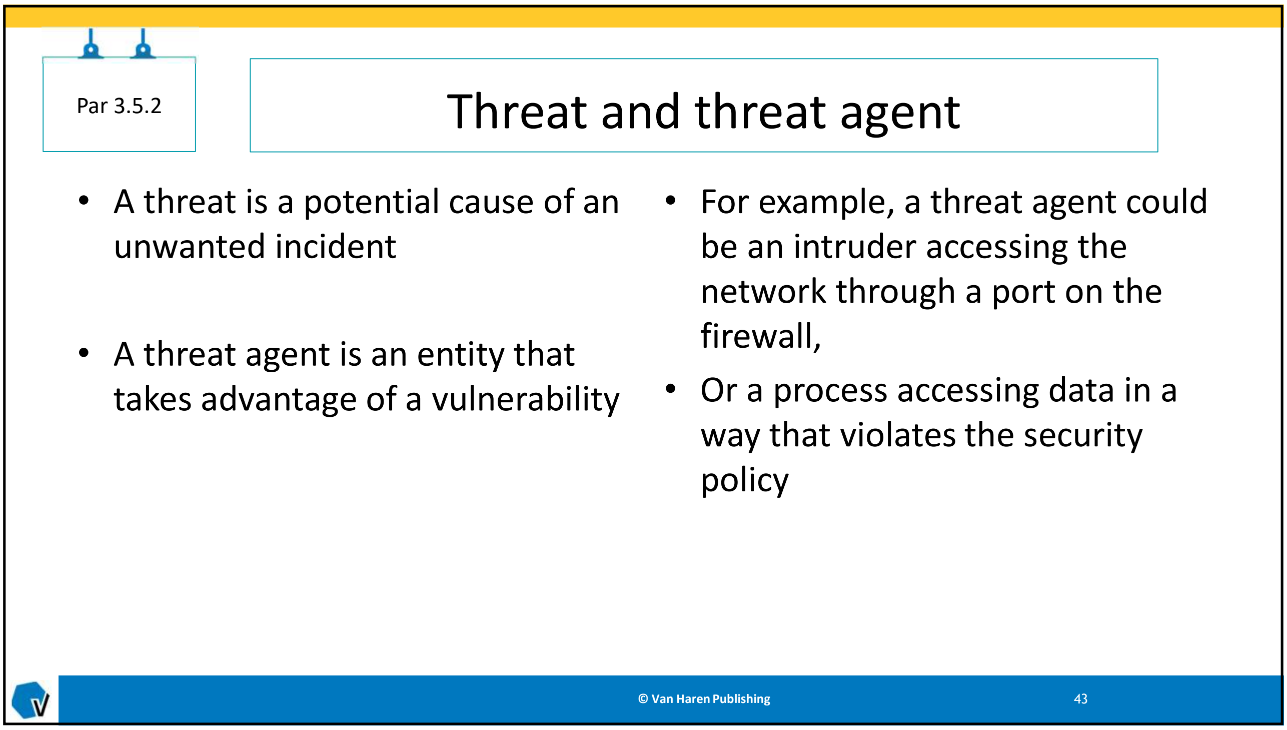


Foundation of Information Security
Module 3 Threats and risks

EXIN
INFORMATION SECURITY MANAGEMENT PROFESSIONAL
based on ISO/IEC 27001
Van Haren
COURSEWARE

Module 3

THREATS AND RISKS



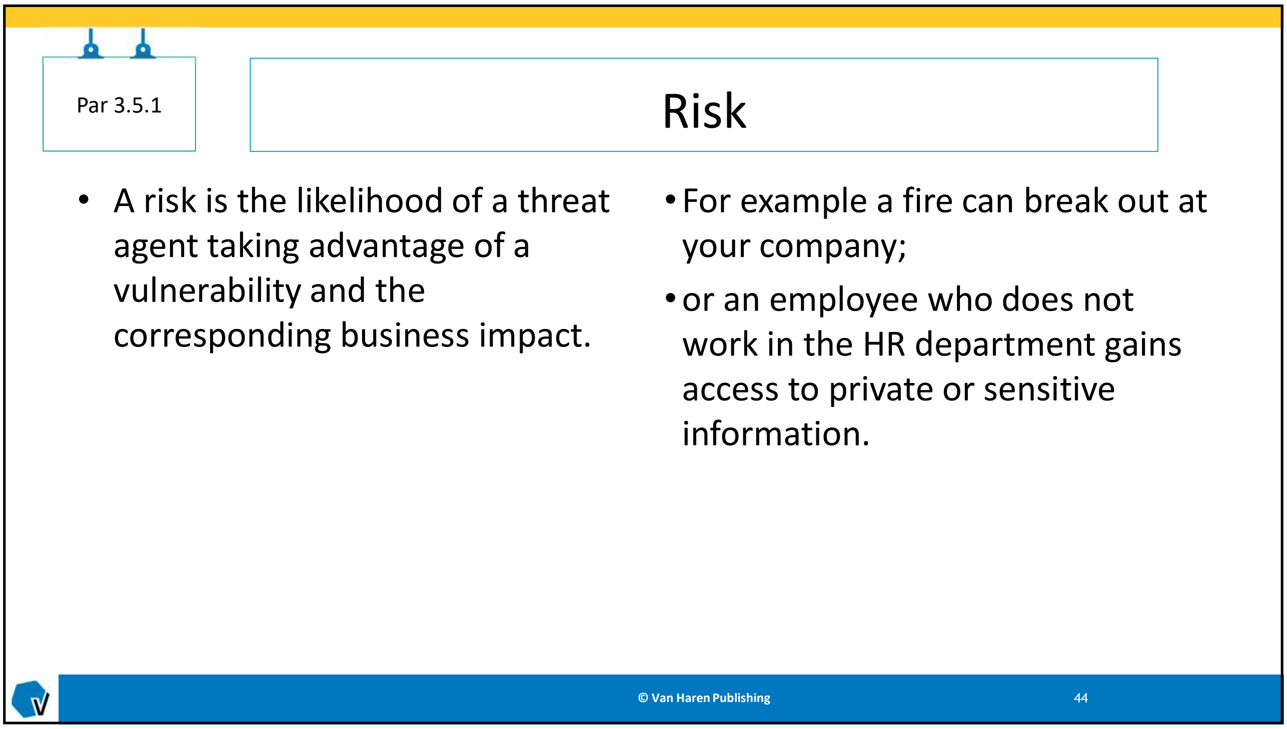
Par 3.5.2

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 43



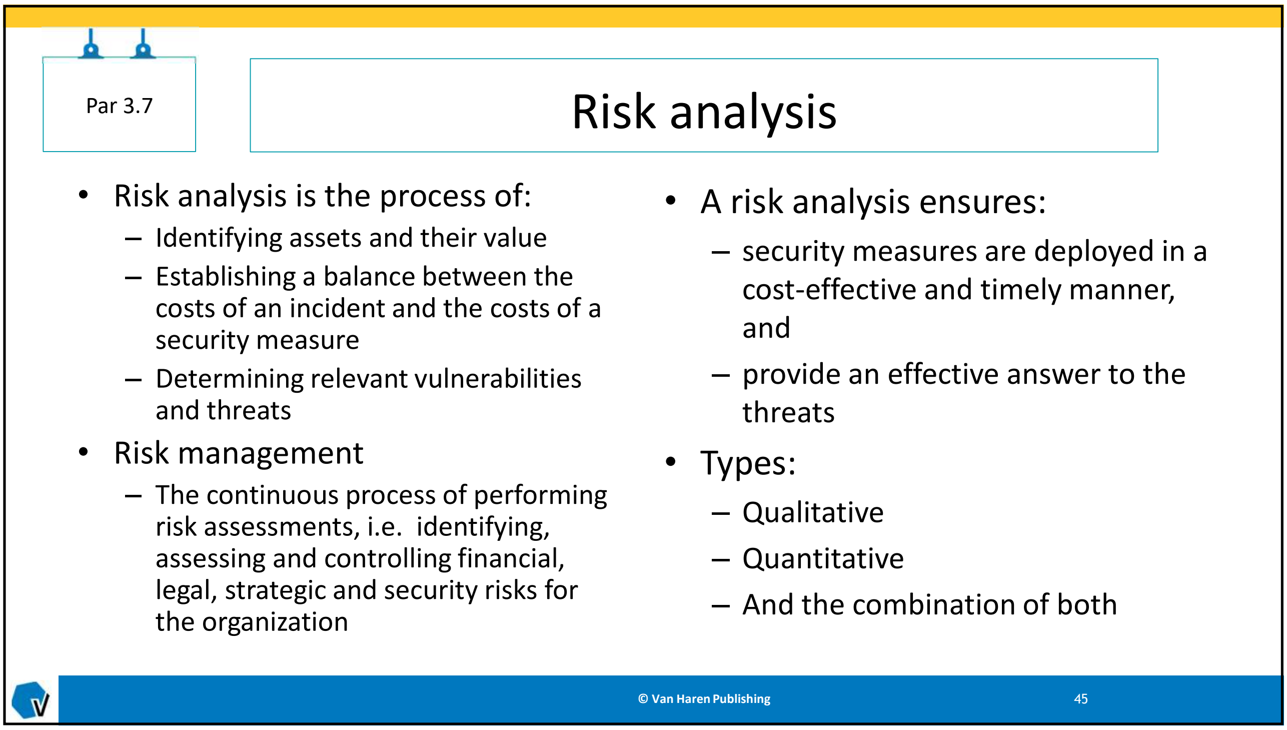
Par 3.5.1

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 44

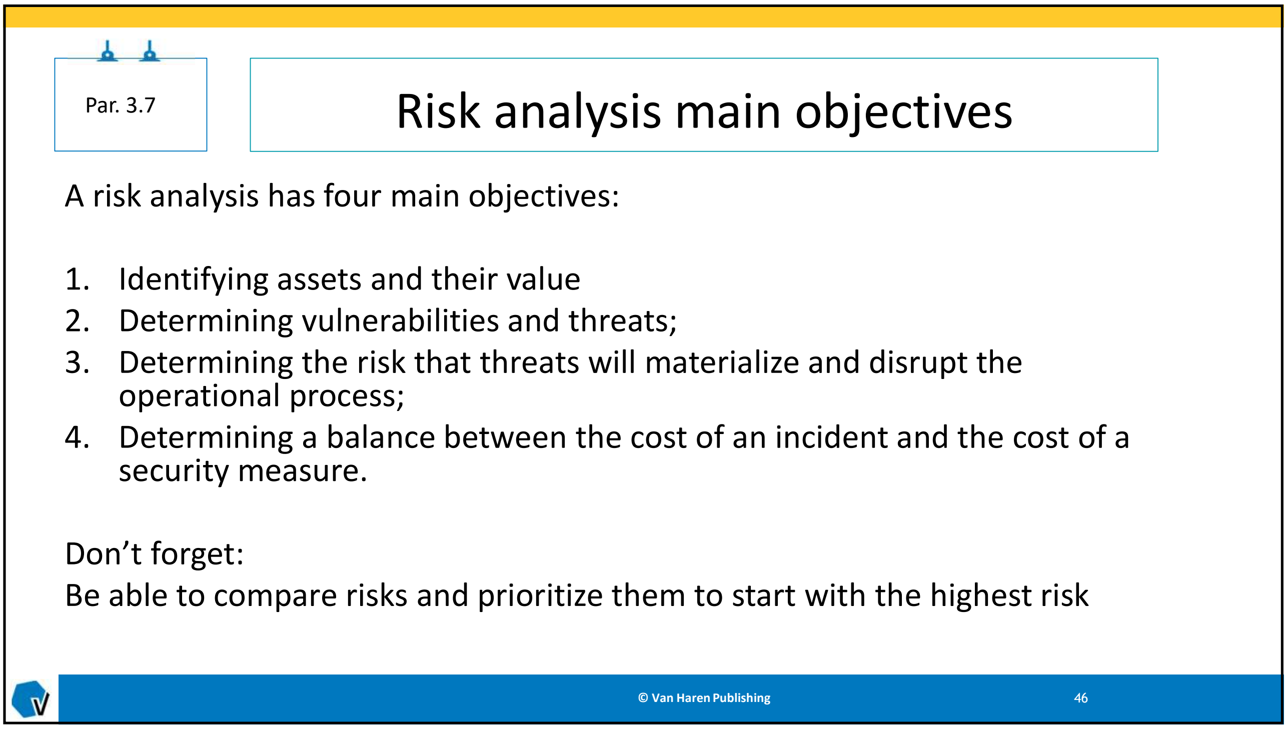


Par 3.7

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
- Risk management
  - The continuous process of performing risk assessments, i.e. identifying, assessing and controlling financial, legal, strategic and security risks for the organization
- A risk analysis ensures:
  - security measures are deployed in a cost-effective and timely manner, and
  - provide an effective answer to the threats
- Types:
  - Qualitative
  - Quantitative
  - And the combination of both

© Van Haren Publishing 45



Par. 3.7

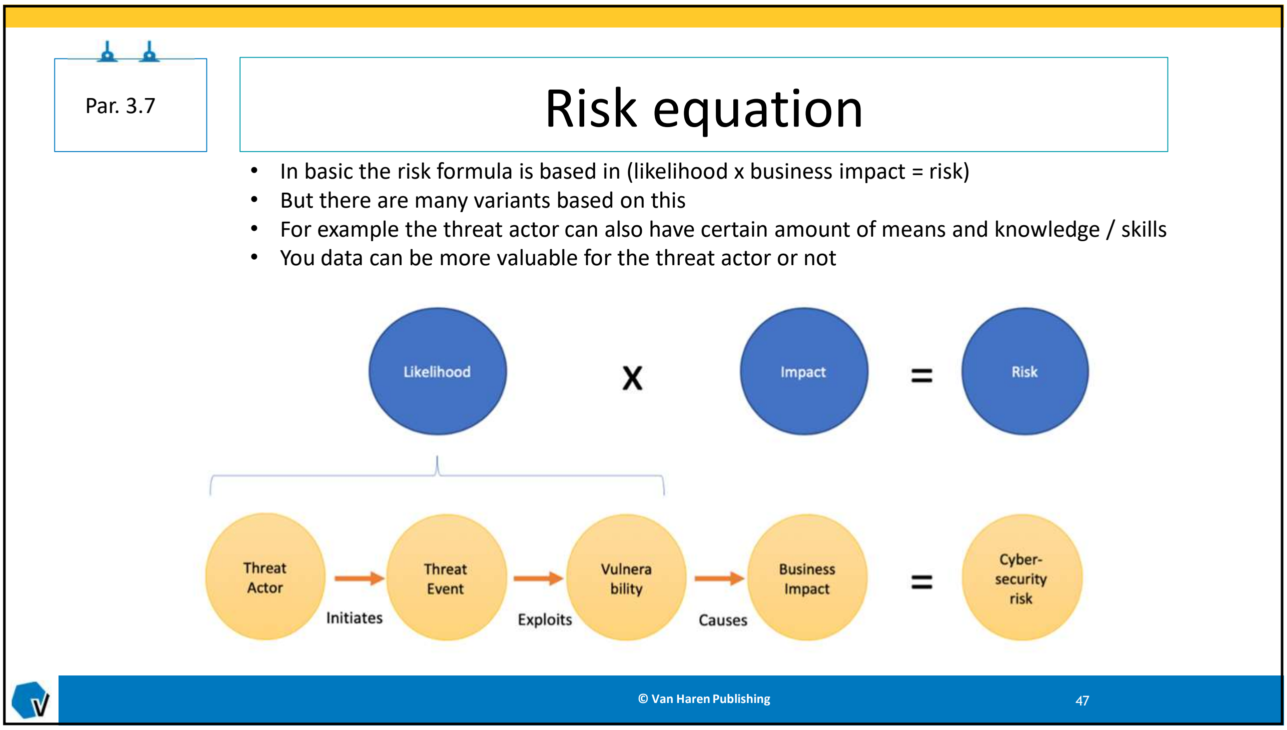
Risk analysis main objectives

A risk analysis has four main objectives:

1. Identifying assets and their value
2. Determining vulnerabilities and threats;
3. Determining the risk that threats will materialize and disrupt the operational process;
4. Determining a balance between the cost of an incident and the cost of a security measure.

Don’t forget:
Be able to compare risks and prioritize them to start with the highest risk

© Van Haren Publishing 46



Par. 3.7

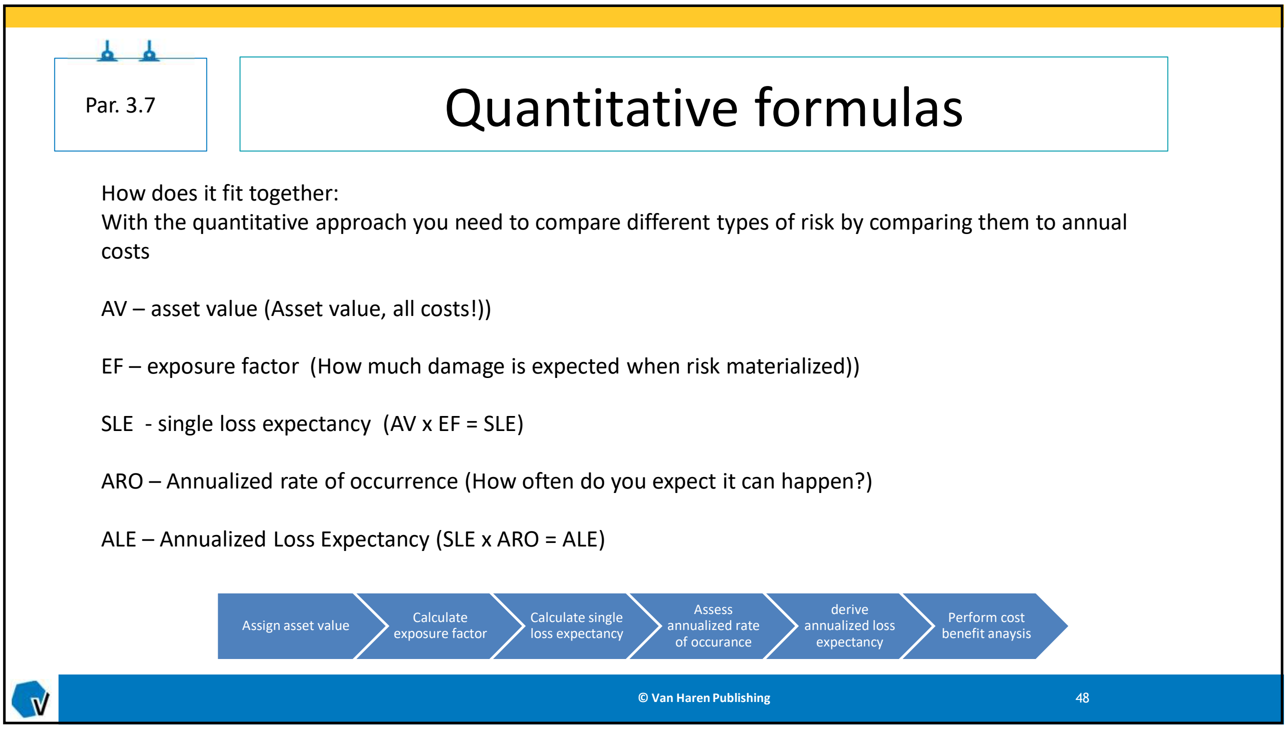
Risk equation

- In basic the risk formula is based in (likelihood x business impact = risk)
- But there are many variants based on this
- For example the threat actor can also have certain amount of means and knowledge / skills
- You data can be more valuable for the threat actor or not

Likelihood X Impact = Risk

Threat Actor → Initiates → Threat Event → Exploits → Vulnera bility → Causes → Business Impact = Cyber-security risk

© Van Haren Publishing 47



Par. 3.7

Quantitative formulas

How does it fit together:
With the quantitative approach you need to compare different types of risk by comparing them to annual costs

AV – asset value (Asset value, all costs!))

EF – exposure factor (How much damage is expected when risk materialized))

SLE - single loss expectancy (AV x EF = SLE)

ARO – Annualized rate of occurrence (How often do you expect it can happen?)

ALE – Annualized Loss Expectancy (SLE x ARO = ALE)

Assign asset value → Calculate exposure factor → Calculate single loss expectancy → Assess annualized rate of occurance → derive annualized loss expectancy → Perform cost benefit anaysis

© Van Haren Publishing 48

Par. 5.7

Threat intelligence and analytics

- Threat and Vulnerability Management ensures that vulnerabilities are discovered and closed in a timely manner.
- Security patches are installed as soon as they are known.
- When patches are not available, temporary other security measures are taken, if possible, to ensure that the vulnerability cannot be exploited

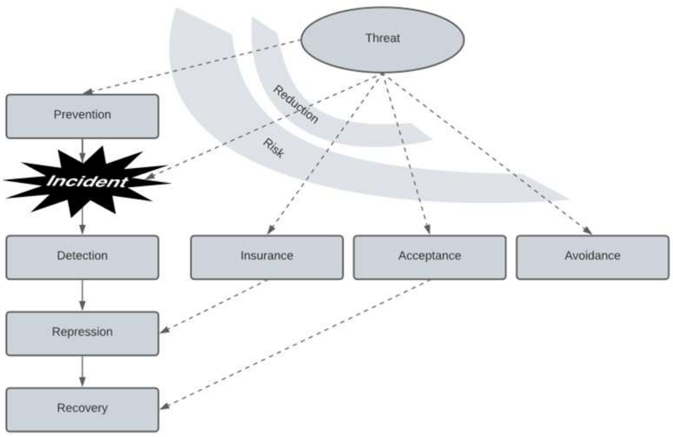
Threat intelligence is leading the way in this.

The organization does not wait for a notification from the vendor that a vulnerability has been found and that a patch is being worked on. The organization actively investigates whether new vulnerabilities have been found

Par 3.5.1/3.5.2

Explain the 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.


Threat
Reduction
Risk
Prevention
Incident
Detection
Insurance
Acceptance
Avoidance
Repression
Recovery