COURSEWARE

Information Security Management Professional based on ISO/IEC 27001 Courseware – English

Courseware

Van Haren
PUBLISHING

EXIN
INFORMATION SECURITY MANAGEMENT PROFESSIONAL
based on ISO/IEC 27001

Information Security Management Professional based on ISO/IEC 27001 Courseware – English

Colofon

Title: Information Security Management Professional based on ISO/IEC 27001 Courseware – English

Author: ing Ruben Zeegers CISSP RSE

Publisher: Van Haren Publishing, Zaltbommel

ISBN Hard copy: 978 94 018 025 67

Edition: First edition, first impression, December 2017

Design & layout: Van Haren Publishing, Zaltbommel

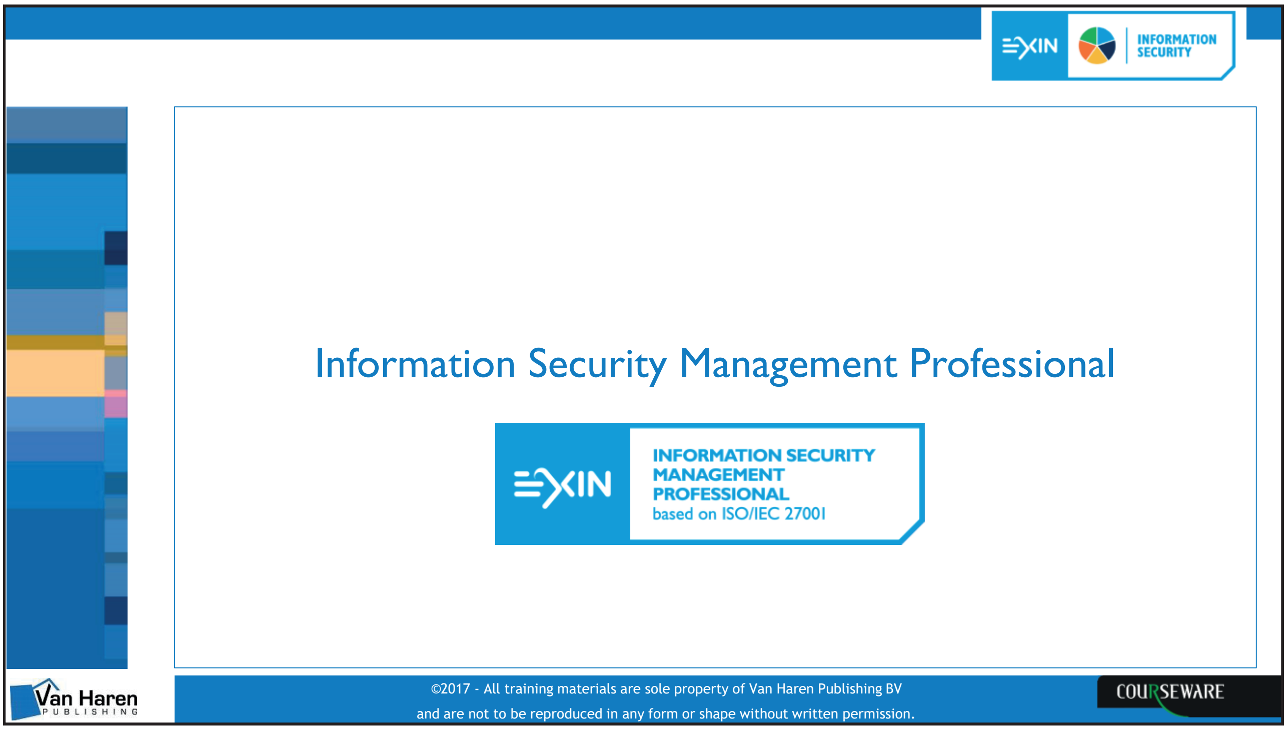
For further information about Van Haren Publishing, please send an email to: info@vanharen.net

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.

The Certificate EXIN Information Security Management Professional based on ISO/IEC 27001 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 27001 and EXIN Information Security Management Expert based on ISO/IEC 27001.

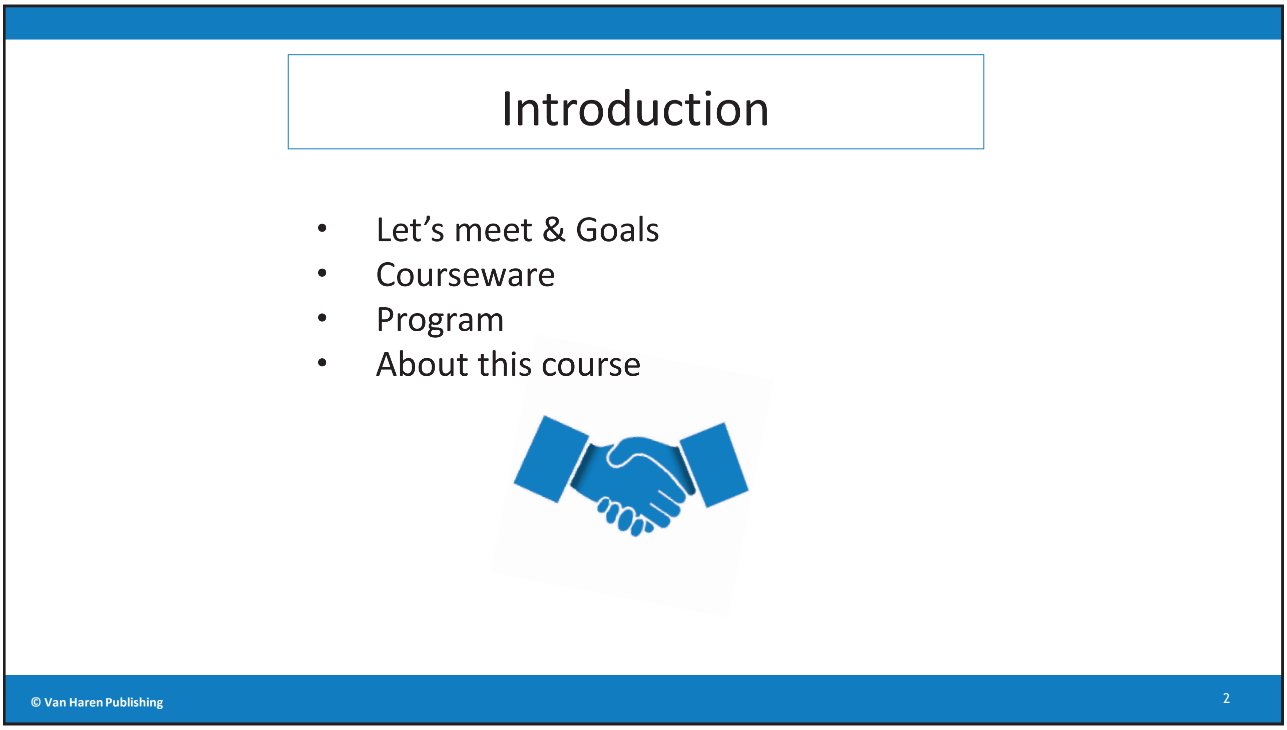
Contents

This number is a reference to the sheet number



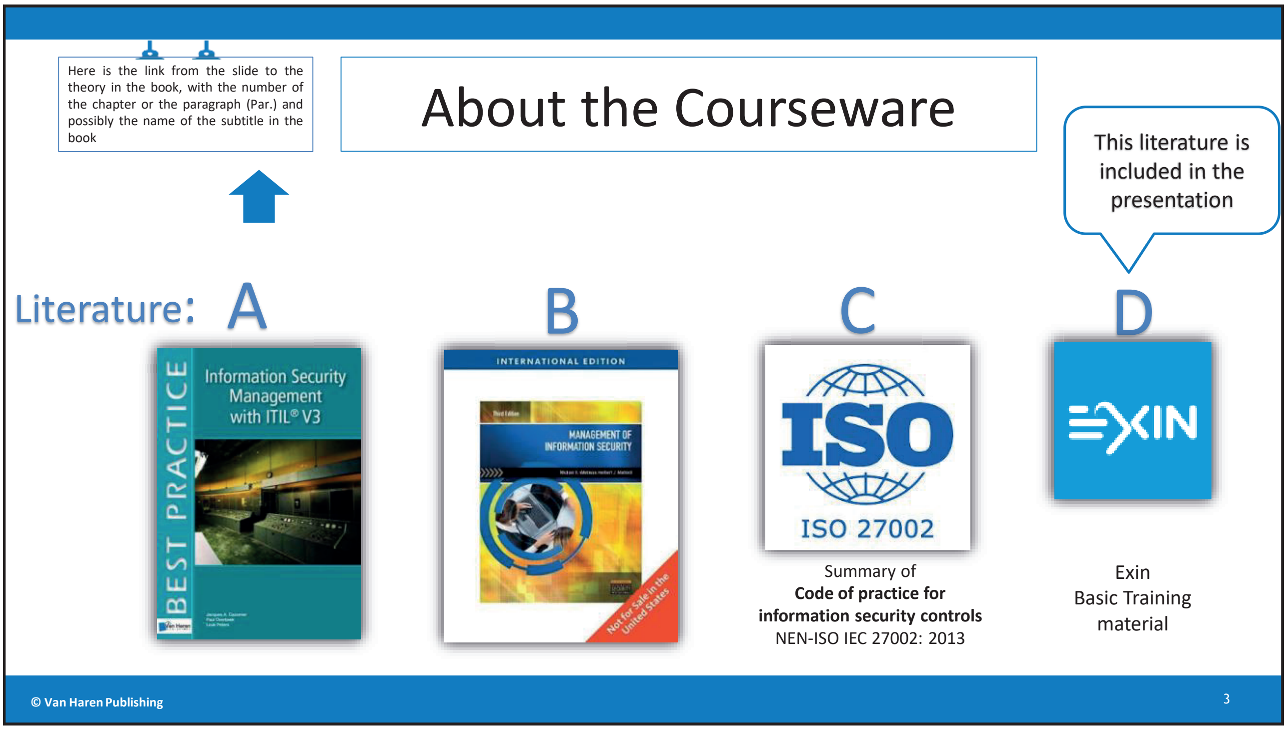
Information Security Management Professional

INFORMATION SECURITY MANAGEMENT PROFESSIONAL
based on ISO/IEC 27001



Introduction

- Let’s meet & Goals
- Courseware
- Program
- About this course



Here is the link from the slide to the theory in the book, with the number of the chapter or the paragraph (Par.) and possibly the name of the subtitle in the book

About the Courseware

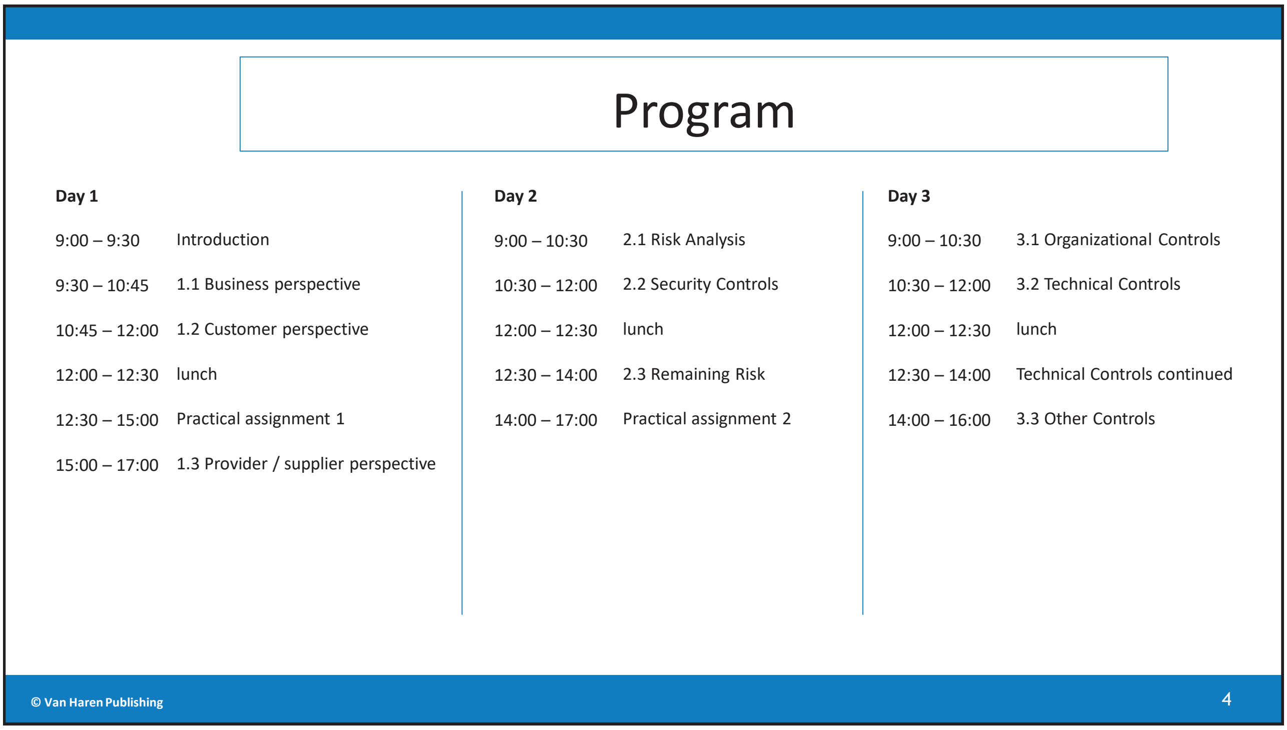
This literature is included in the presentation

Literature: A B C D

BEST PRACTICE
Information Security Management with ITIL® V3
INTERNATIONAL EDITION
MANAGEMENT OF INFORMATION SECURITY
Not for Sale in the United States
ISO
ISO 27002
EXIN

Summary of
Code of practice for information security controls
NEN-ISO IEC 27002: 2013

Exin
Basic Training
material

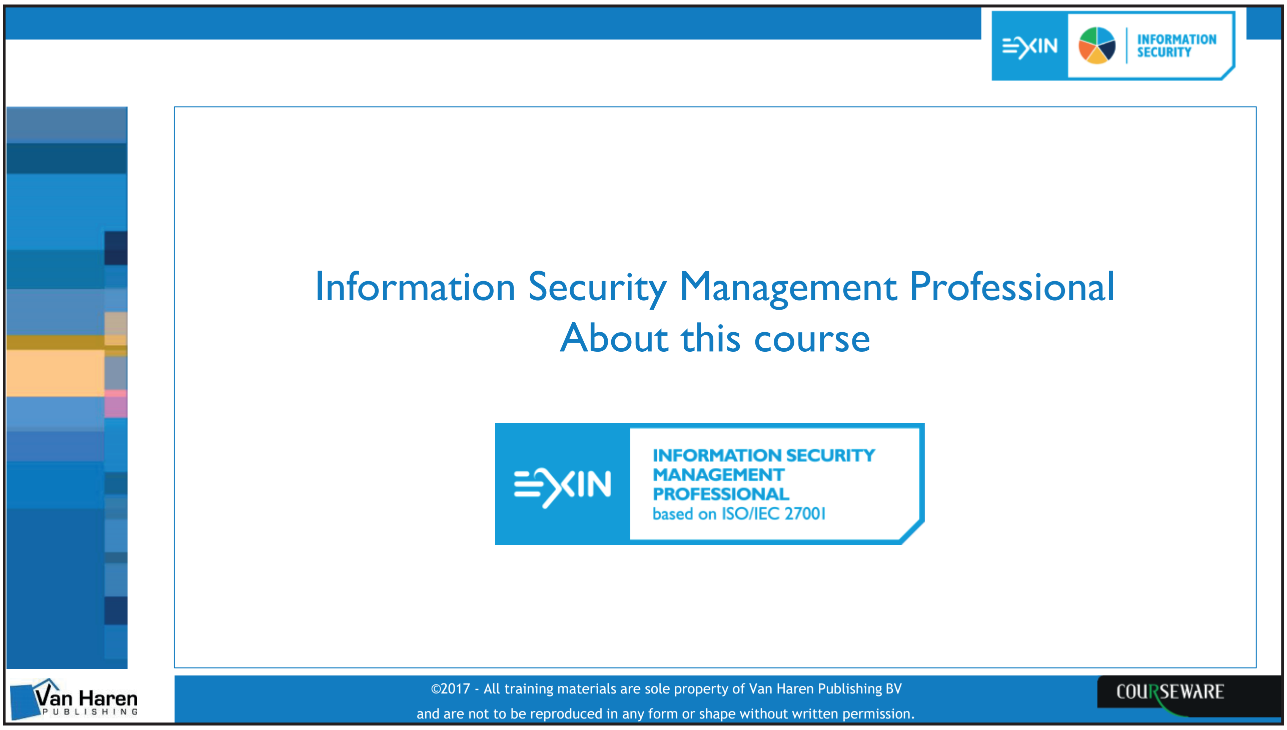


Program

Day 1	
9:00 – 9:30	Introduction
9:30 – 10:45	1.1 Business perspective
10:45 – 12:00	1.2 Customer perspective
12:00 – 12:30	lunch
12:30 – 15:00	Practical assignment 1
15:00 – 17:00	1.3 Provider / supplier perspective

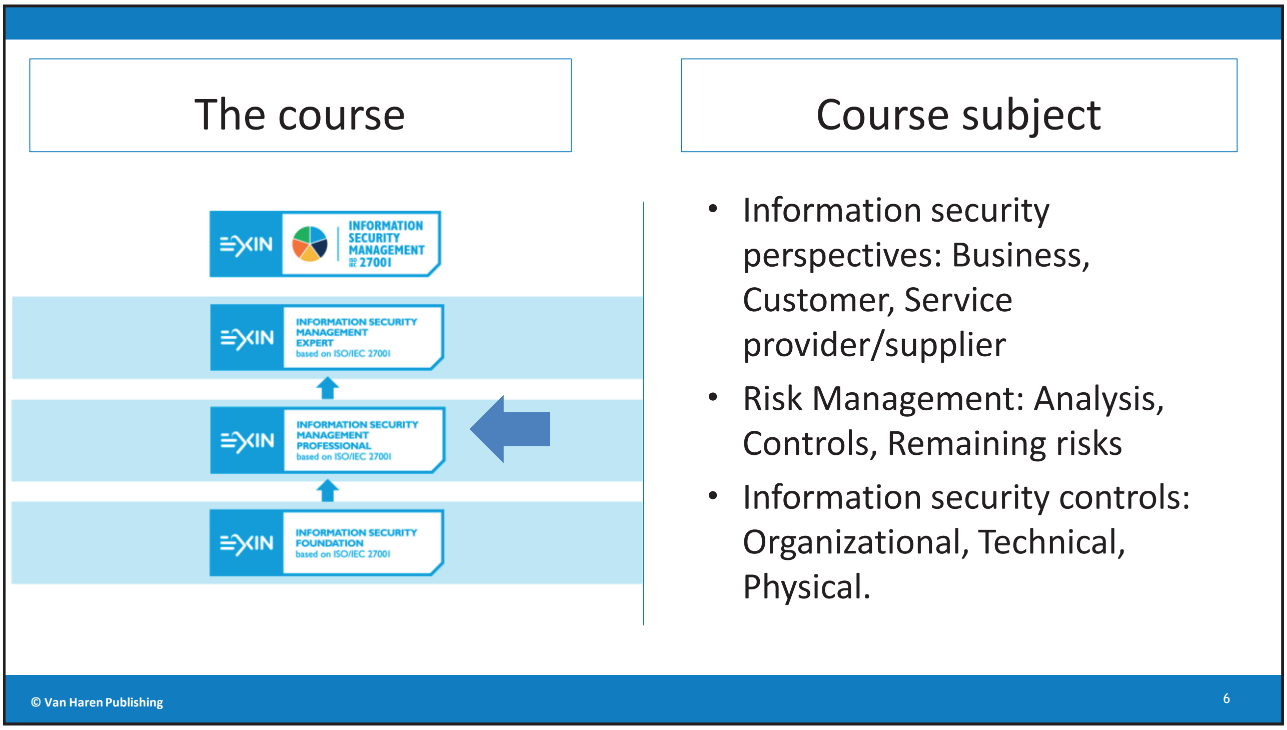
Day 2	
9:00 – 10:30	2.1 Risk Analysis
10:30 – 12:00	2.2 Security Controls
12:00 – 12:30	lunch
12:30 – 14:00	2.3 Remaining Risk
14:00 – 17:00	Practical assignment 2

Day 3	
9:00 – 10:30	3.1 Organizational Controls
10:30 – 12:00	3.2 Technical Controls
12:00 – 12:30	lunch
12:30 – 14:00	Technical Controls continued
14:00 – 16:00	3.3 Other Controls



Information Security Management Professional
About this course

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

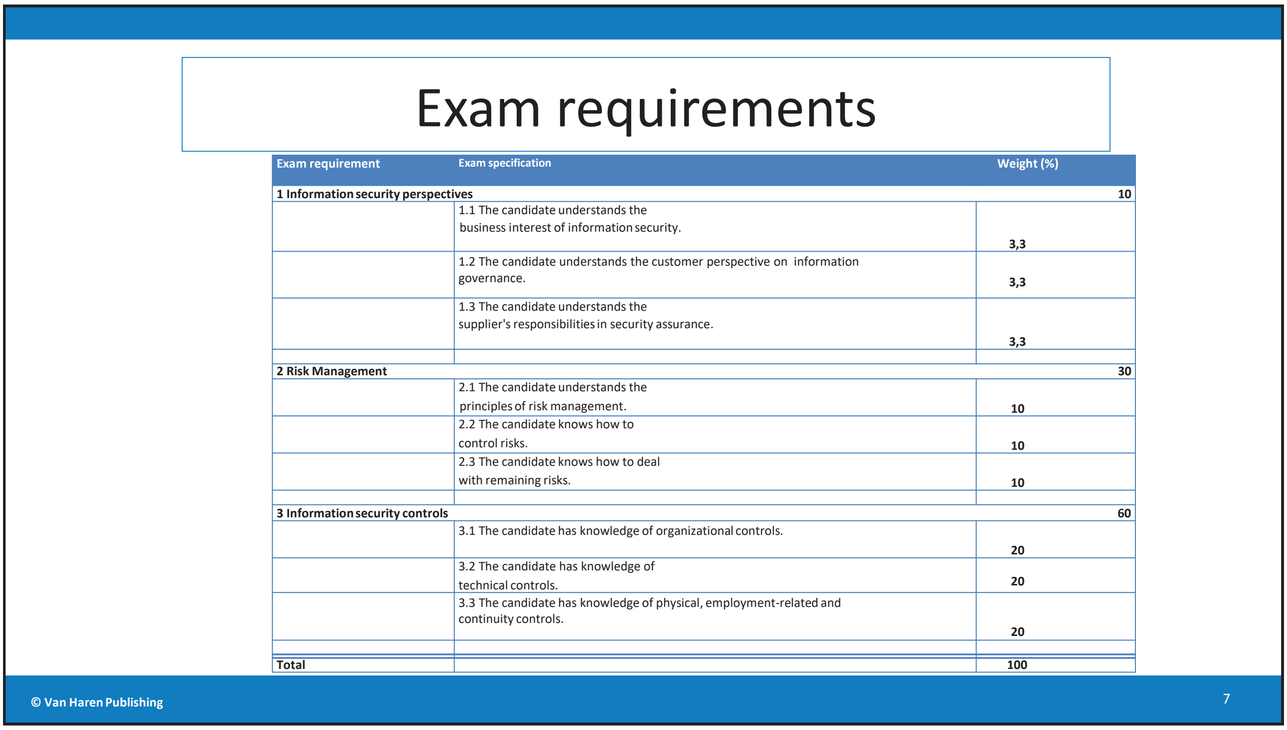


The course

EXIN INFORMATION SECURITY MANAGEMENT ISO/IEC 27001
EXIN INFORMATION SECURITY MANAGEMENT EXPERT based on ISO/IEC 27001
EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001
EXIN INFORMATION SECURITY FOUNDATION based on ISO/IEC 27001

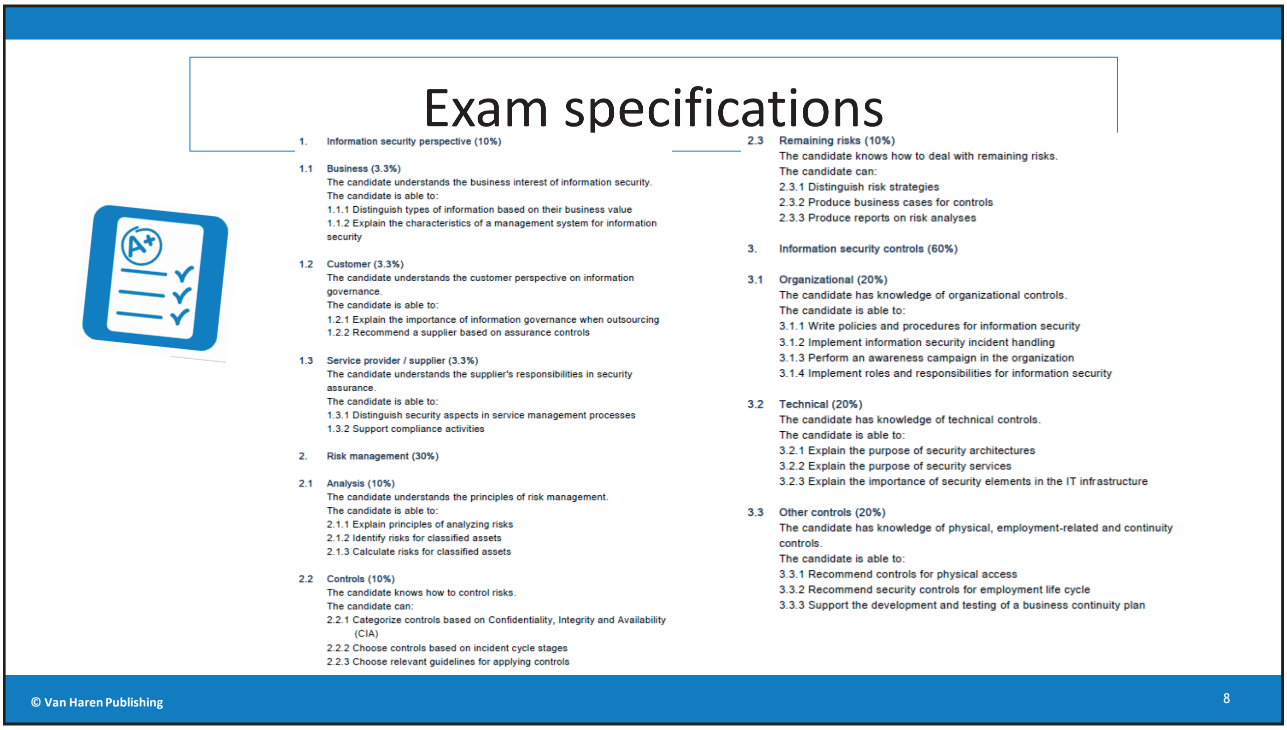
Course subject

- Information security perspectives: Business, Customer, Service provider/supplier
- Risk Management: Analysis, Controls, Remaining risks
- Information security controls: Organizational, Technical, Physical.



Exam requirements

Exam requirement	Exam specification	Weight (%)
1 Information security perspectives		10
	1.1 The candidate understands the business interest of information security.	3,3
	1.2 The candidate understands the customer perspective on information governance.	3,3
	1.3 The candidate understands the supplier's responsibilities in security assurance.	3,3
2 Risk Management		30
	2.1 The candidate understands the principles of risk management.	10
	2.2 The candidate knows how to control risks.	10
	2.3 The candidate knows how to deal with remaining risks.	10
3 Information security controls		60
	3.1 The candidate has knowledge of organizational controls.	20
	3.2 The candidate has knowledge of technical controls.	20
	3.3 The candidate has knowledge of physical, employment-related and continuity controls.	20
Total		100



Exam specifications

1. Information security perspective (10%)

1.1 Business (3.3%)
The candidate understands the business interest of information security.
The candidate is able to:
1.1.1 Distinguish types of information based on their business value
1.1.2 Explain the characteristics of a management system for information security

1.2 Customer (3.3%)
The candidate understands the customer perspective on information governance.
The candidate is able to:
1.2.1 Explain the importance of information governance when outsourcing
1.2.2 Recommend a supplier based on assurance controls

1.3 Service provider / supplier (3.3%)
The candidate understands the supplier's responsibilities in security assurance.
The candidate is able to:
1.3.1 Distinguish security aspects in service management processes
1.3.2 Support compliance activities

2. Risk management (30%)

2.1 Analysis (10%)
The candidate understands the principles of risk management.
The candidate is able to:
2.1.1 Explain principles of analyzing risks
2.1.2 Identify risks for classified assets
2.1.3 Calculate risks for classified assets

2.2 Controls (10%)
The candidate knows how to control risks.
The candidate can:
2.2.1 Categorize controls based on Confidentiality, Integrity and Availability (CIA)
2.2.2 Choose controls based on incident cycle stages
2.2.3 Choose relevant guidelines for applying controls

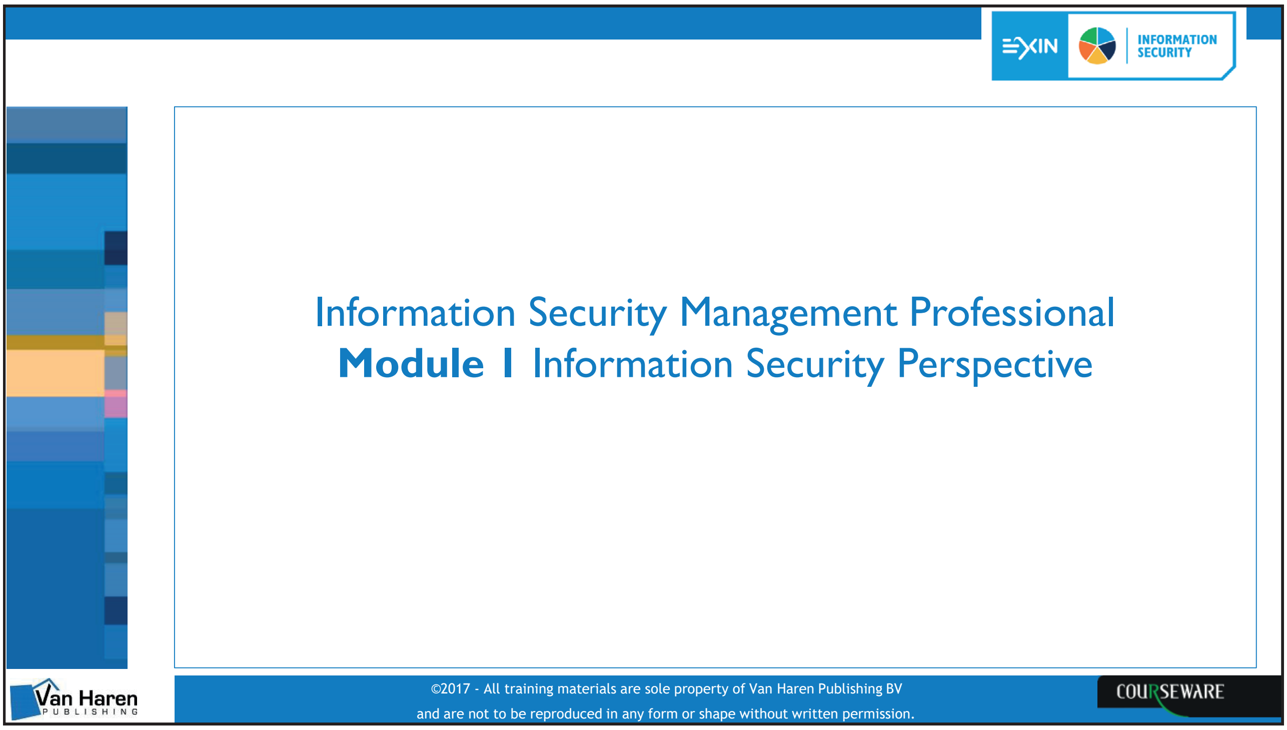
2.3 Remaining risks (10%)
The candidate knows how to deal with remaining risks.
The candidate can:
2.3.1 Distinguish risk strategies
2.3.2 Produce business cases for controls
2.3.3 Produce reports on risk analyses

3. Information security controls (60%)

3.1 Organizational (20%)
The candidate has knowledge of organizational controls.
The candidate is able to:
3.1.1 Write policies and procedures for information security
3.1.2 Implement information security incident handling
3.1.3 Perform an awareness campaign in the organization
3.1.4 Implement roles and responsibilities for information security

3.2 Technical (20%)
The candidate has knowledge of technical controls.
The candidate is able to:
3.2.1 Explain the purpose of security architectures
3.2.2 Explain the purpose of security services
3.2.3 Explain the importance of security elements in the IT infrastructure

3.3 Other controls (20%)
The candidate has knowledge of physical, employment-related and continuity controls.
The candidate is able to:
3.3.1 Recommend controls for physical access
3.3.2 Recommend security controls for employment life cycle
3.3.3 Support the development and testing of a business continuity plan

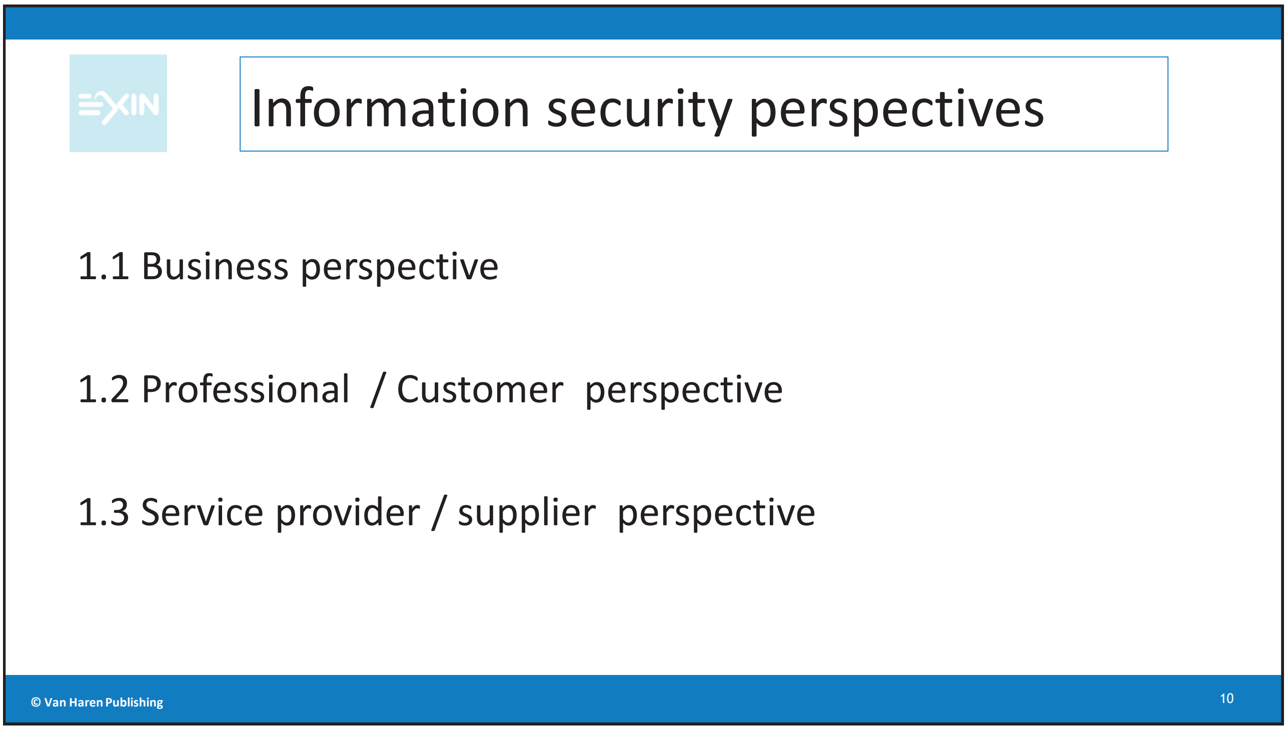


INFORMATION SECURITY

Information Security Management Professional

Module I Information Security Perspective

COURSEWARE



Information security perspectives

1.1 Business perspective

1.2 Professional / Customer perspective

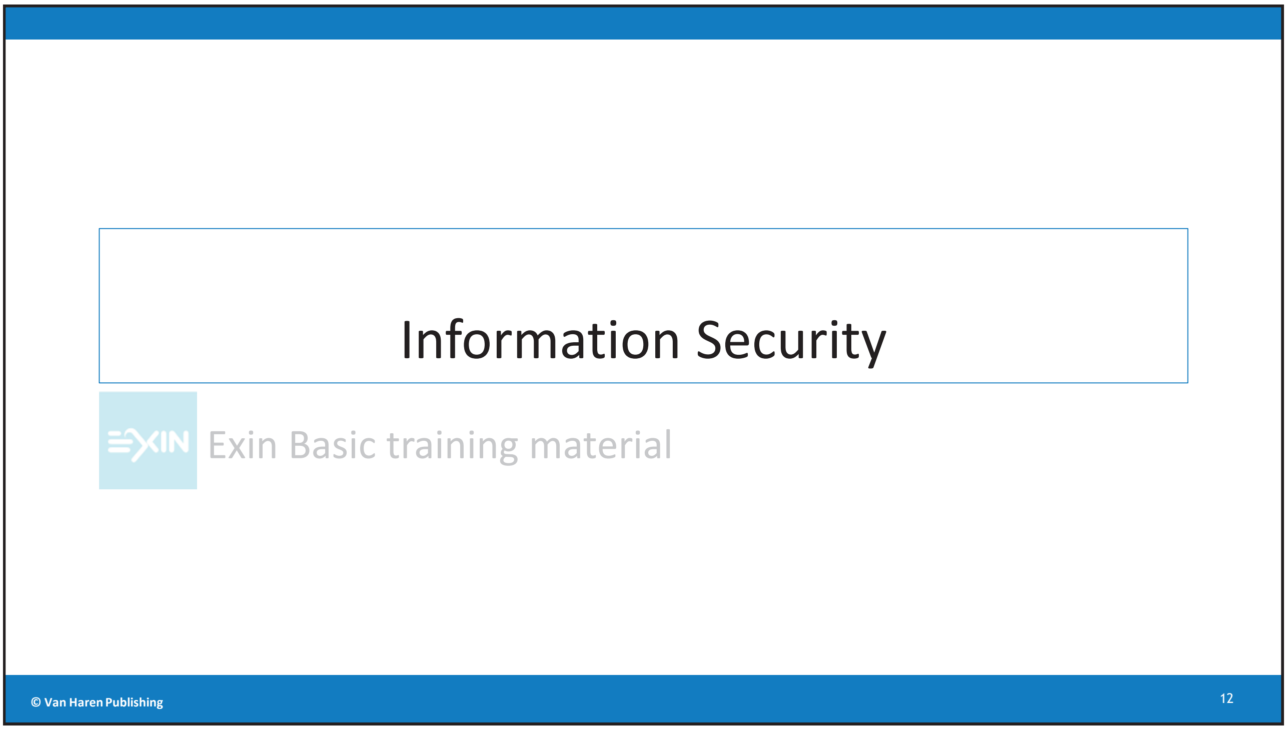
1.3 Service provider / supplier perspective

A: § 2.1; Chapter 3; §5.6
B: Chapter 4; Chapter 9

EXIN INFORMATION SECURITY

Module 1.1

BUSINESS PERSPECTIVE



Information Security

EXIN Exin Basic training material

What is information security?

Information security is the protection of information and its critical characteristics (**confidentiality, integrity, and availability**), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology.

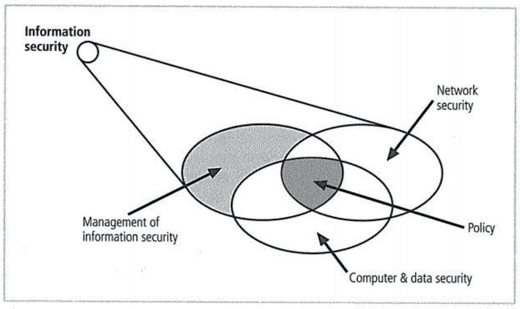


Figure 1-1 Components of information security

Perspectives on Information Security

10 Information Security Management with ITIL V3

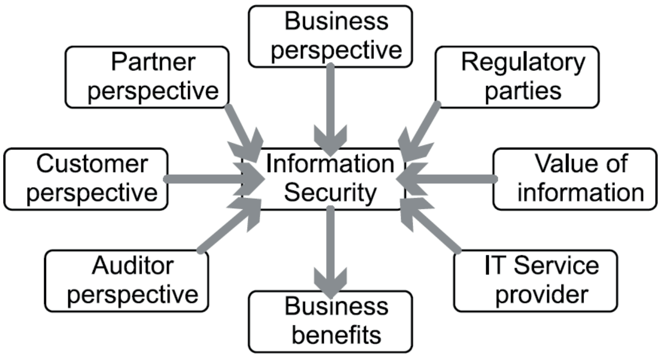
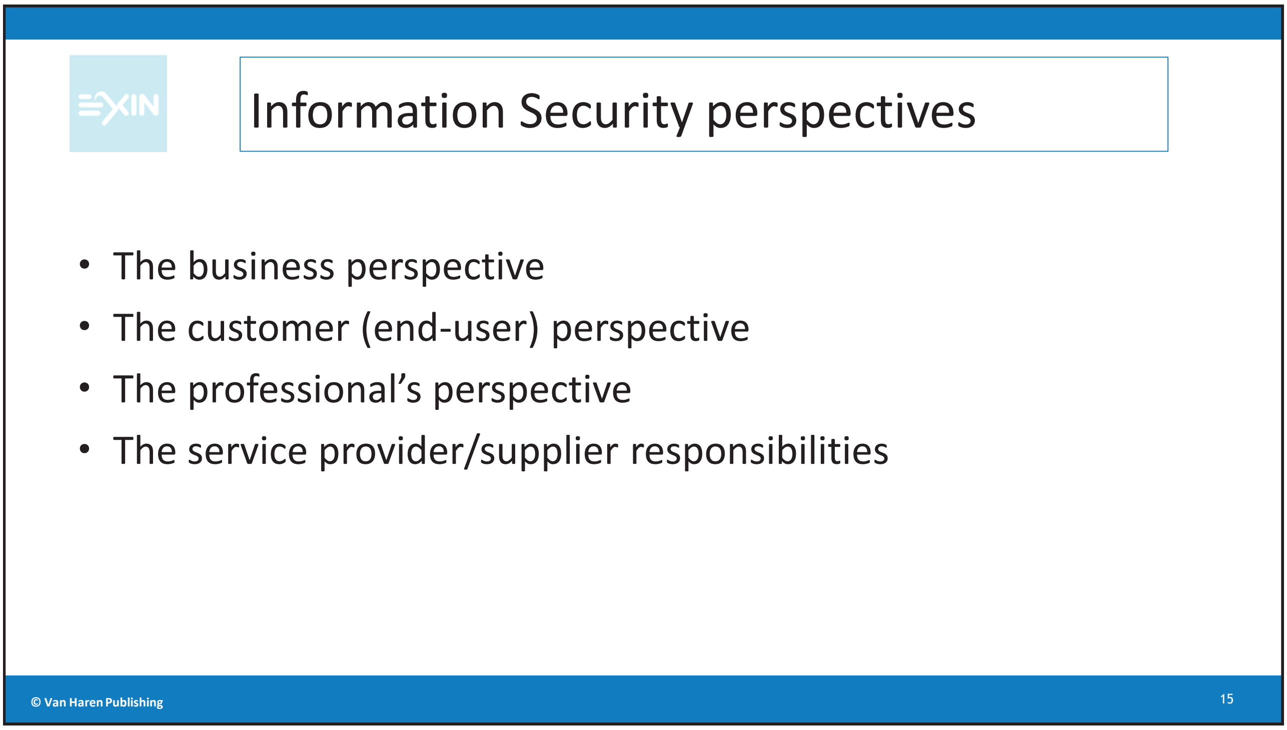


Figure 2.1: Different perspectives on information security

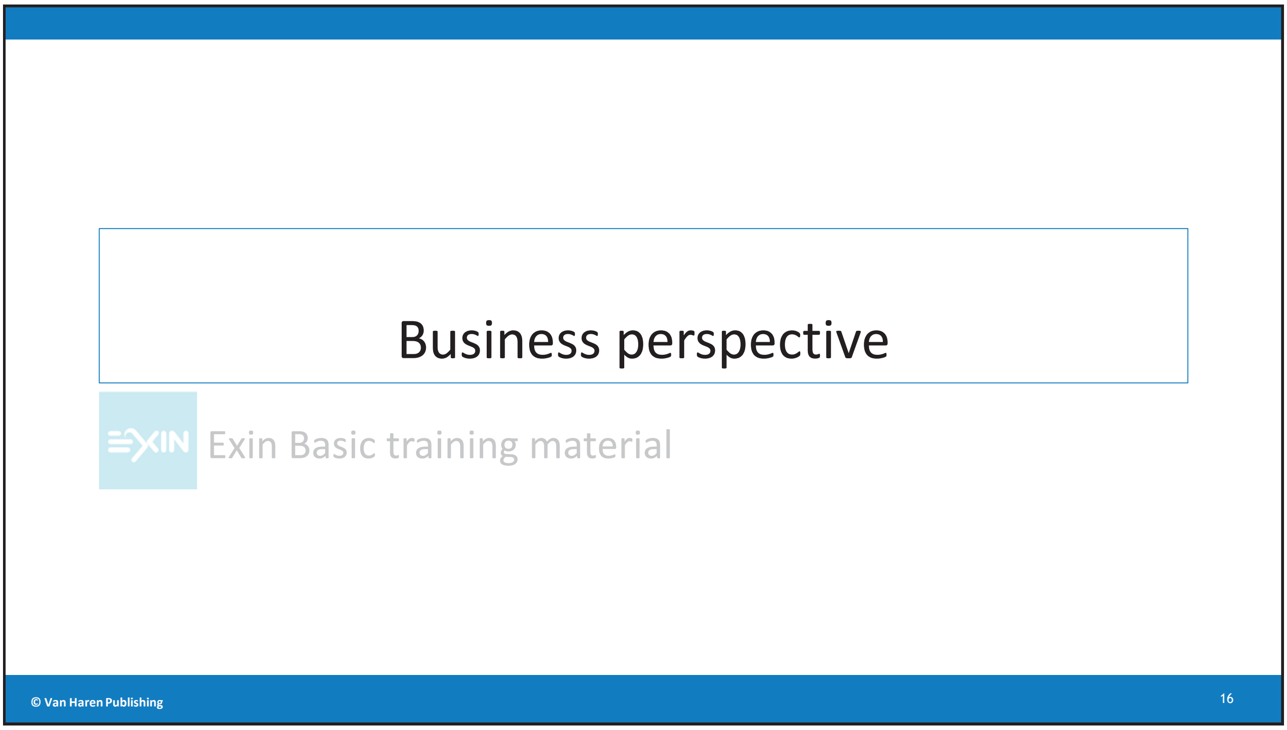


Information Security perspectives

- The business perspective
- The customer (end-user) perspective
- The professional’s perspective
- The service provider/supplier responsibilities

© Van Haren Publishing

15

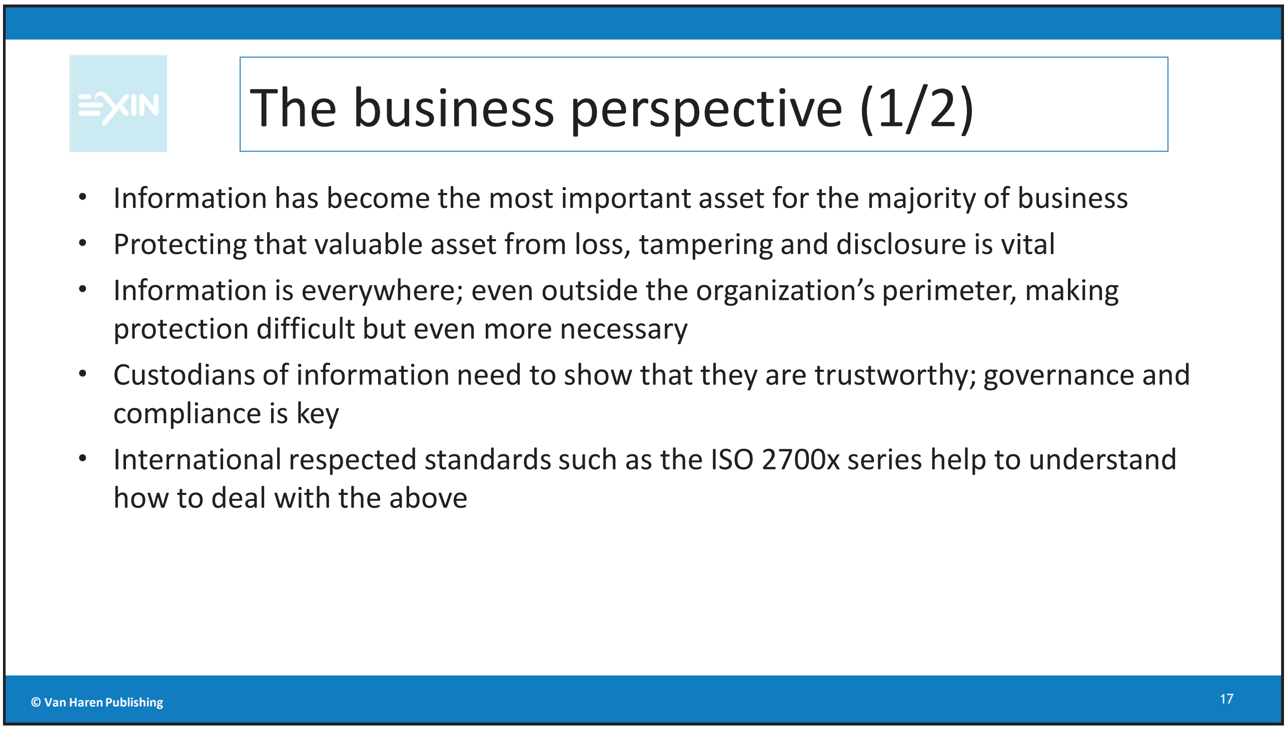


Business perspective

Exin Basic training material

© Van Haren Publishing

16

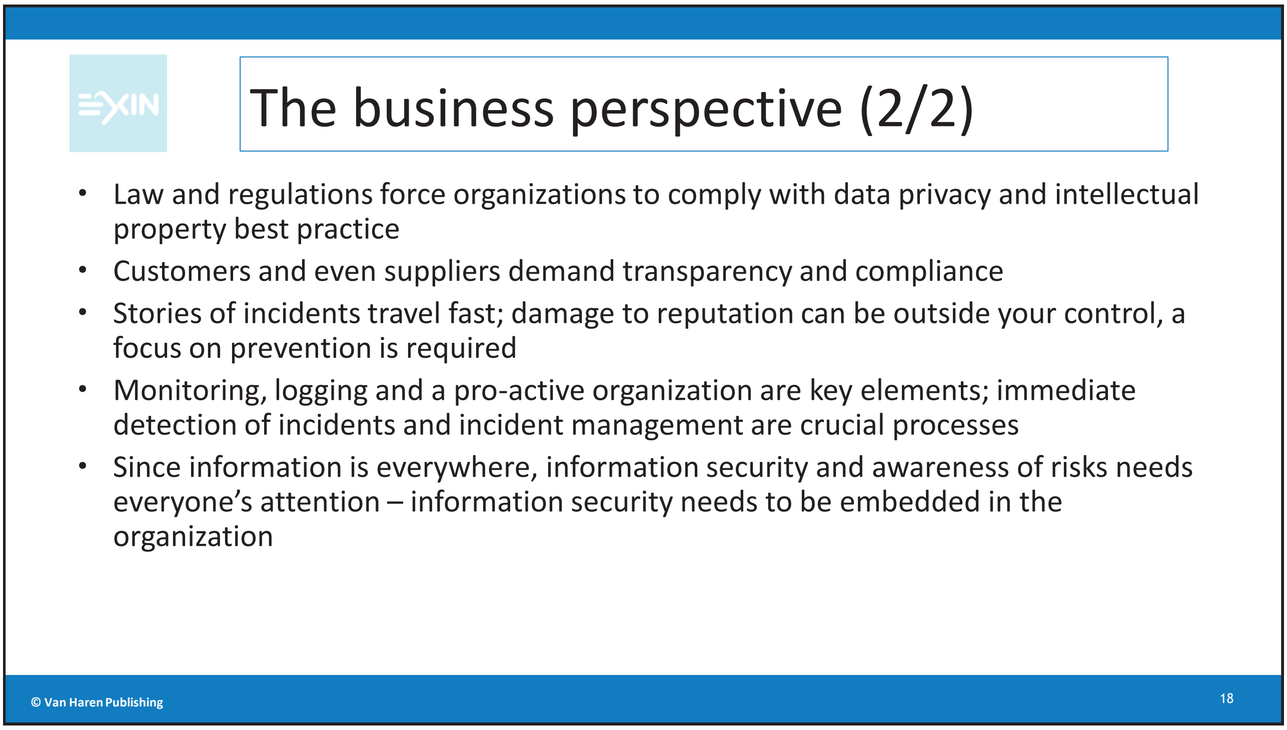


The business perspective (1/2)

- Information has become the most important asset for the majority of business
- Protecting that valuable asset from loss, tampering and disclosure is vital
- Information is everywhere; even outside the organization’s perimeter, making protection difficult but even more necessary
- Custodians of information need to show that they are trustworthy; governance and compliance is key
- International respected standards such as the ISO 2700x series help to understand how to deal with the above

© Van Haren Publishing

17

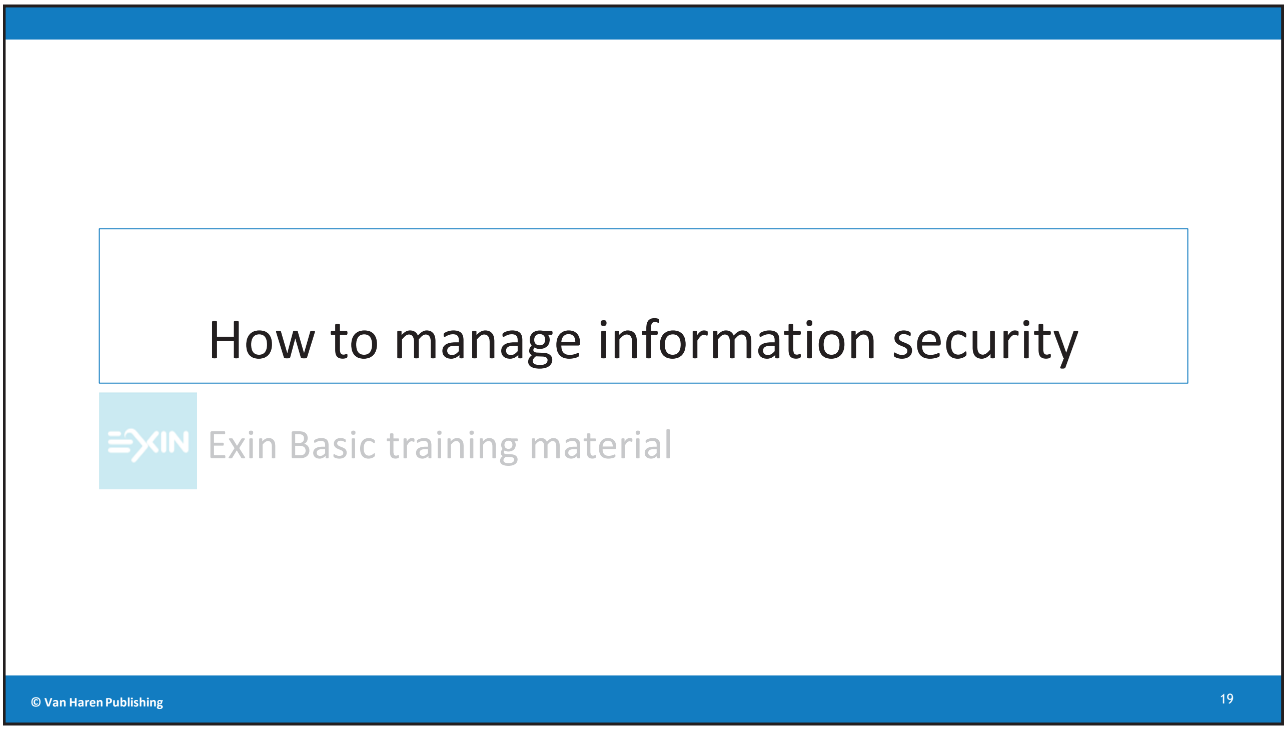


The business perspective (2/2)

- Law and regulations force organizations to comply with data privacy and intellectual property best practice
- Customers and even suppliers demand transparency and compliance
- Stories of incidents travel fast; damage to reputation can be outside your control, a focus on prevention is required
- Monitoring, logging and a pro-active organization are key elements; immediate detection of incidents and incident management are crucial processes
- Since information is everywhere, information security and awareness of risks needs everyone’s attention – information security needs to be embedded in the organization

© Van Haren Publishing

18

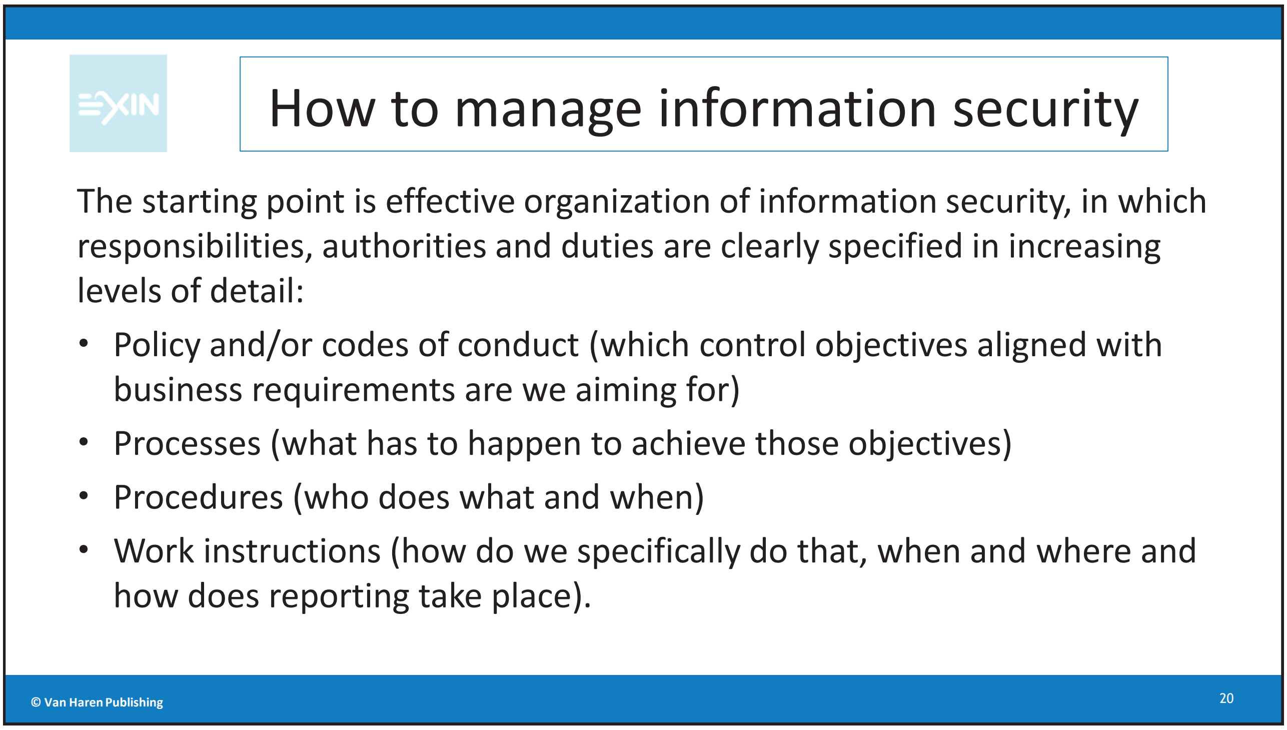


How to manage information security

Exin Basic training material

© Van Haren Publishing

19



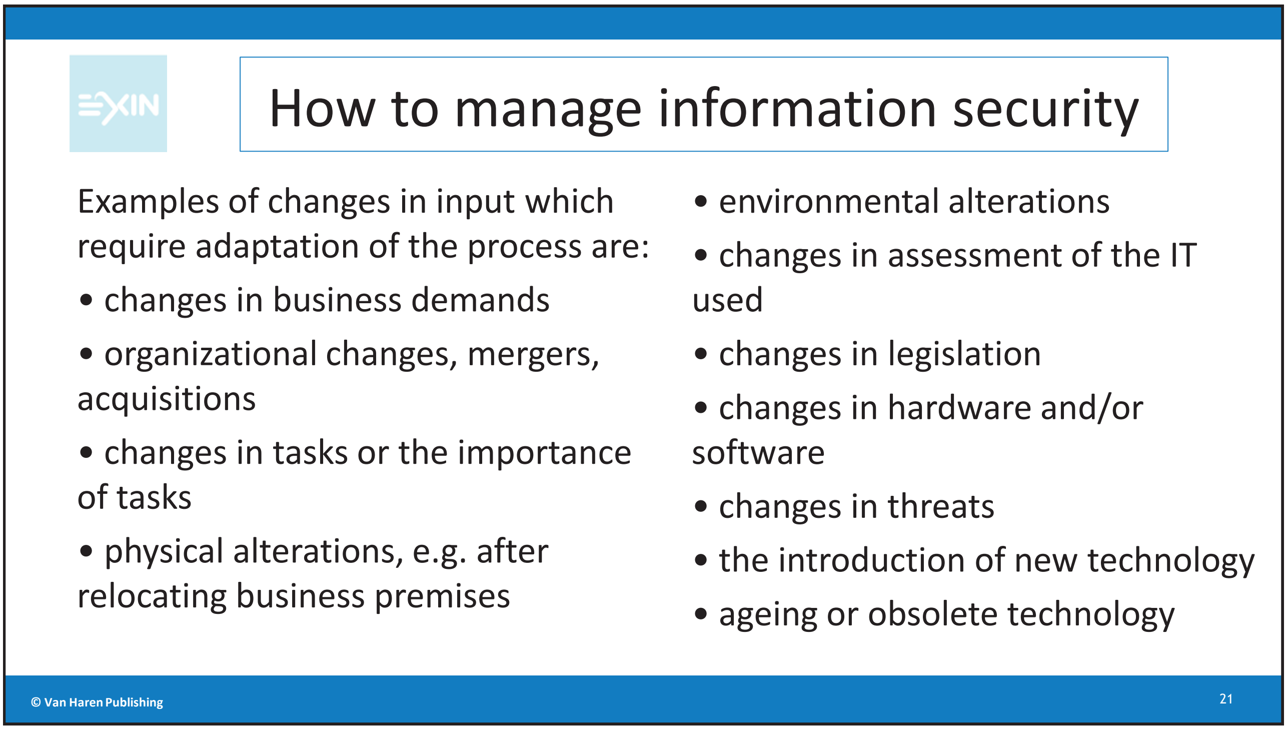
How to manage information security

The starting point is effective organization of information security, in which responsibilities, authorities and duties are clearly specified in increasing levels of detail:

- Policy and/or codes of conduct (which control objectives aligned with business requirements are we aiming for)
- Processes (what has to happen to achieve those objectives)
- Procedures (who does what and when)
- Work instructions (how do we specifically do that, when and where and how does reporting take place).

© Van Haren Publishing

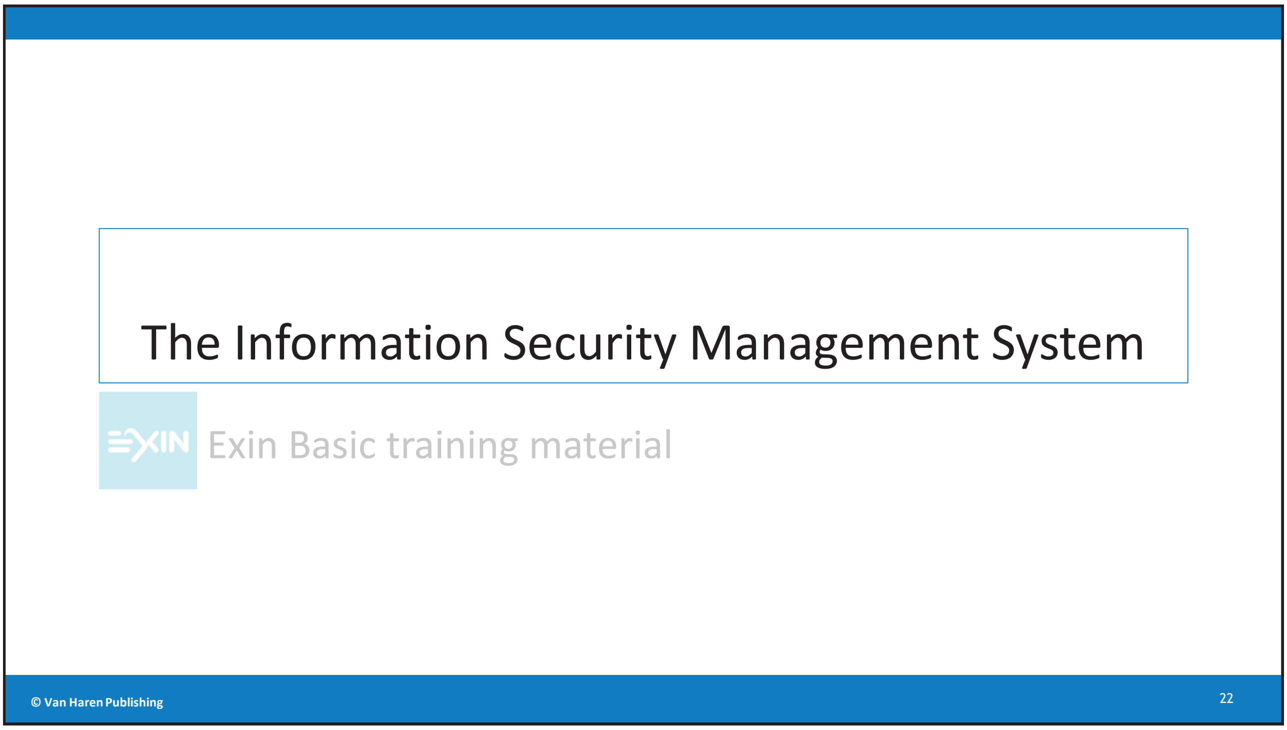
20



How to manage information security

Examples of changes in input which require adaptation of the process are:

- changes in business demands
- organizational changes, mergers, acquisitions
- changes in tasks or the importance of tasks
- physical alterations, e.g. after relocating business premises
- environmental alterations
- changes in assessment of the IT used
- changes in legislation
- changes in hardware and/or software
- changes in threats
- the introduction of new technology
- ageing or obsolete technology



The Information Security Management System

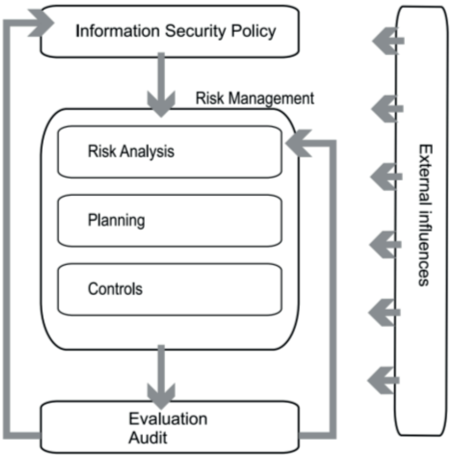
Exin Basic training material

The Information Security Management System

The management system represents the complete information security process during all the phases of its cycle, from policy to maintenance.

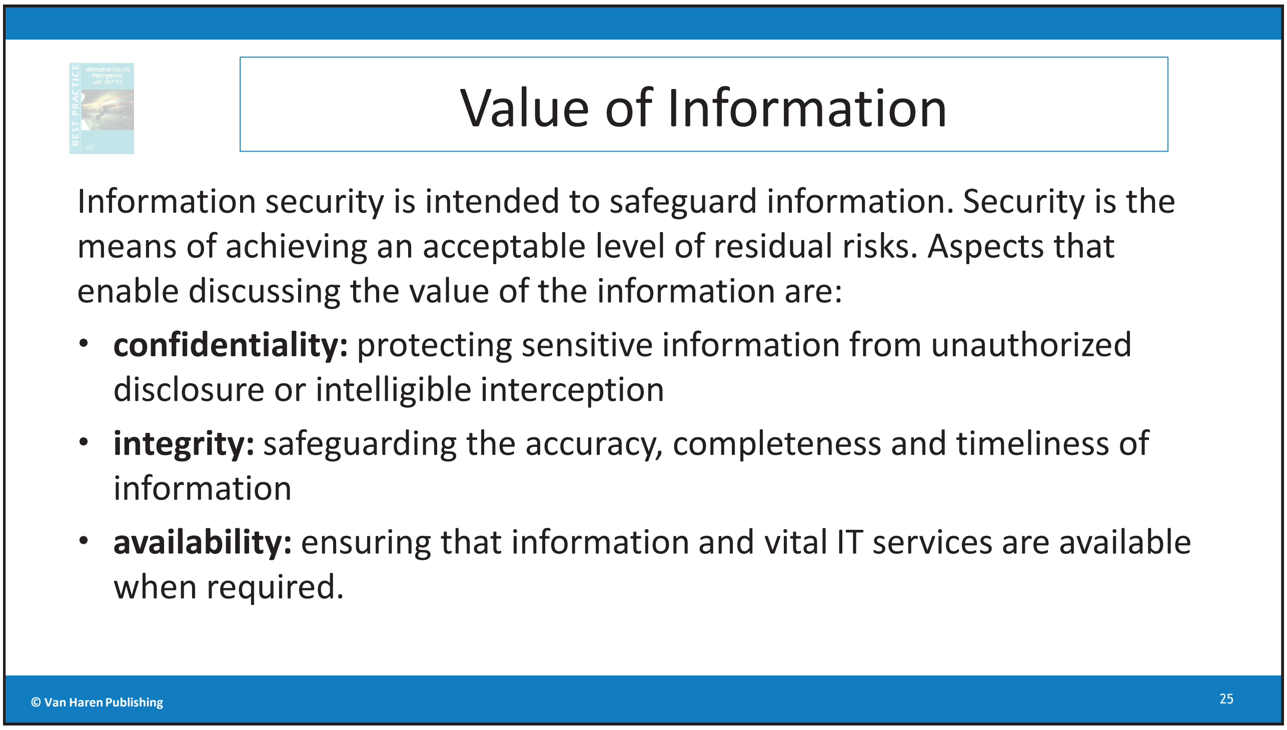
It is comparable to the management systems found in standards such as ISO 9000 and ISO/IEC 27001.

Plan-do- check-act (Deming circle)



Value and importance of Information

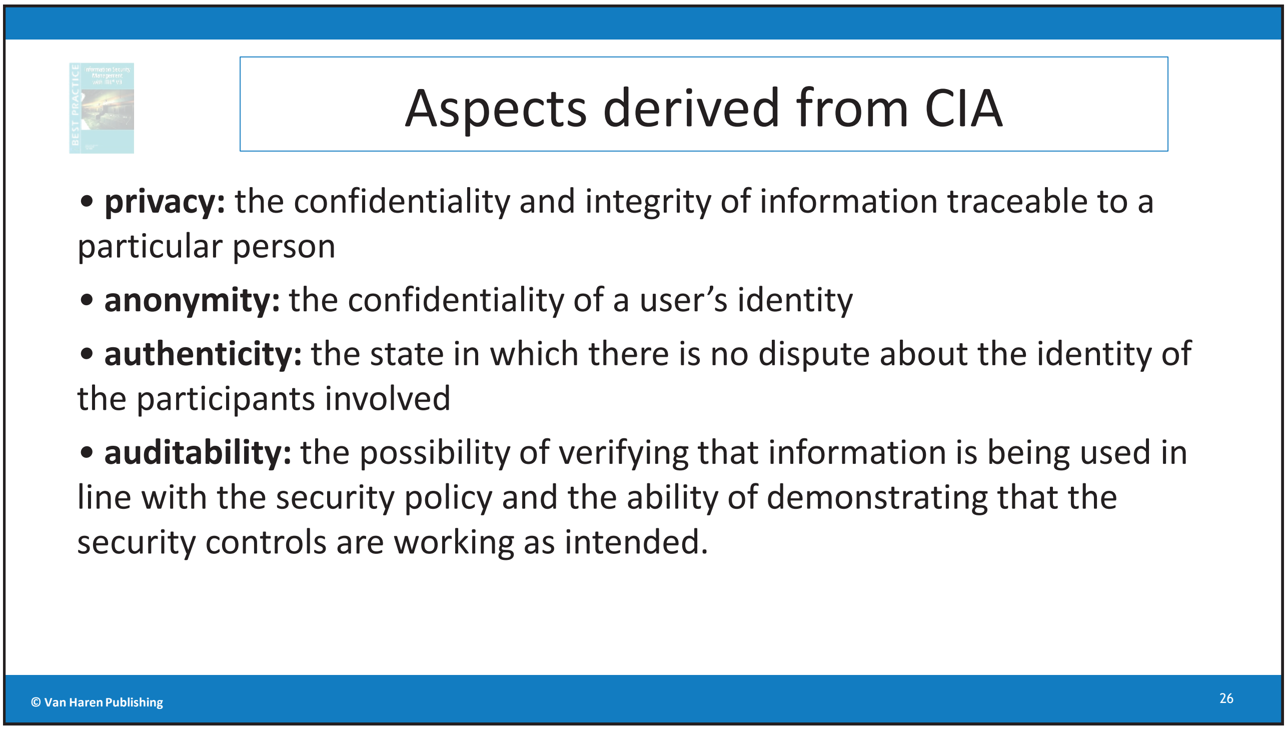
Literature A: Information Security Management with ITIL v3



Value of Information

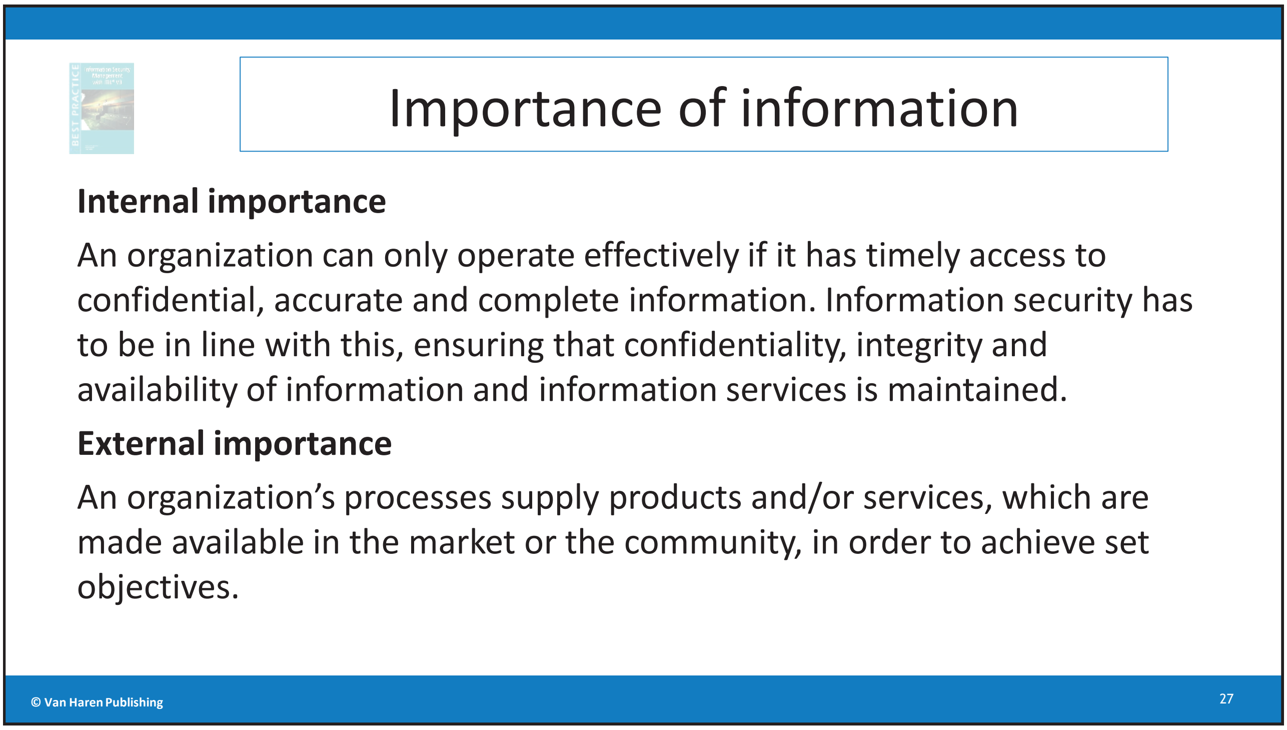
Information security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. Aspects that enable discussing the value of the information are:

- **confidentiality:** protecting sensitive information from unauthorized disclosure or intelligible interception
- **integrity:** safeguarding the accuracy, completeness and timeliness of information
- **availability:** ensuring that information and vital IT services are available when required.



Aspects derived from CIA

- **privacy:** the confidentiality and integrity of information traceable to a particular person
- **anonymity:** the confidentiality of a user's identity
- **authenticity:** the state in which there is no dispute about the identity of the participants involved
- **auditability:** the possibility of verifying that information is being used in line with the security policy and the ability of demonstrating that the security controls are working as intended.



Importance of information

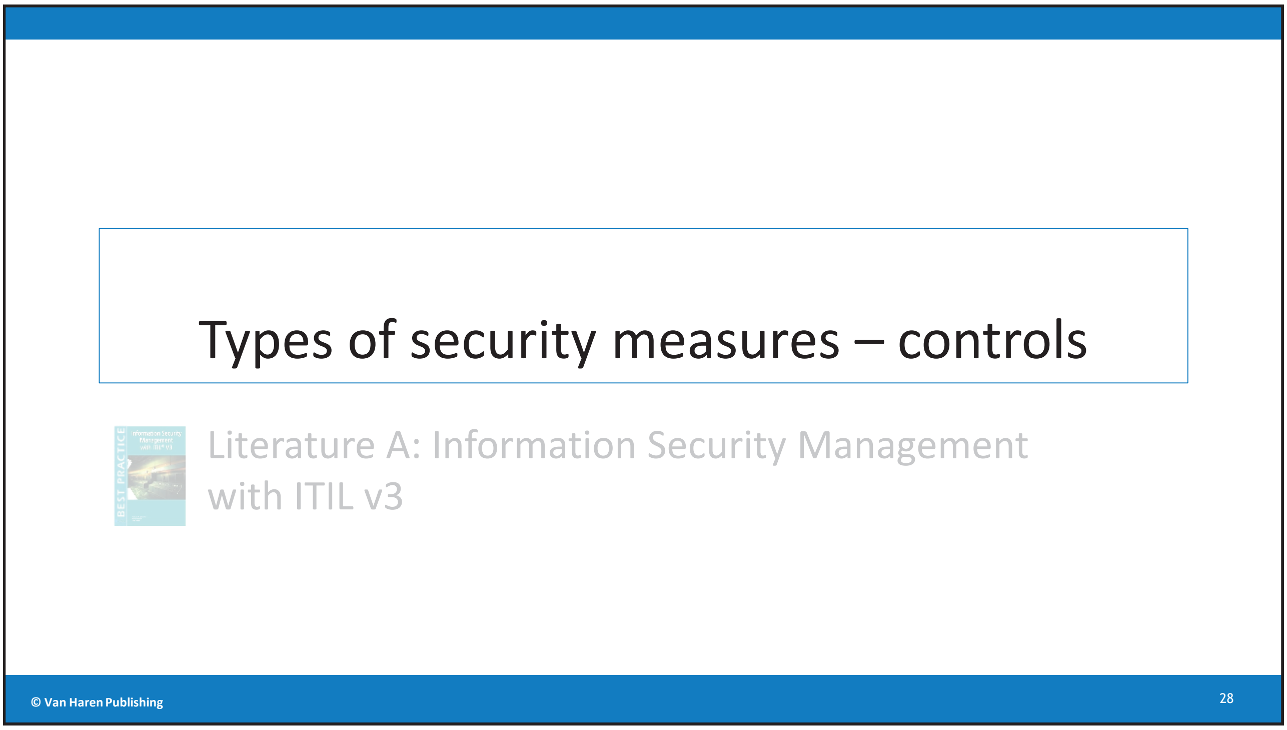
Internal importance

An organization can only operate effectively if it has timely access to confidential, accurate and complete information. Information security has to be in line with this, ensuring that confidentiality, integrity and availability of information and information services is maintained.

External importance

An organization's processes supply products and/or services, which are made available in the market or the community, in order to achieve set objectives.

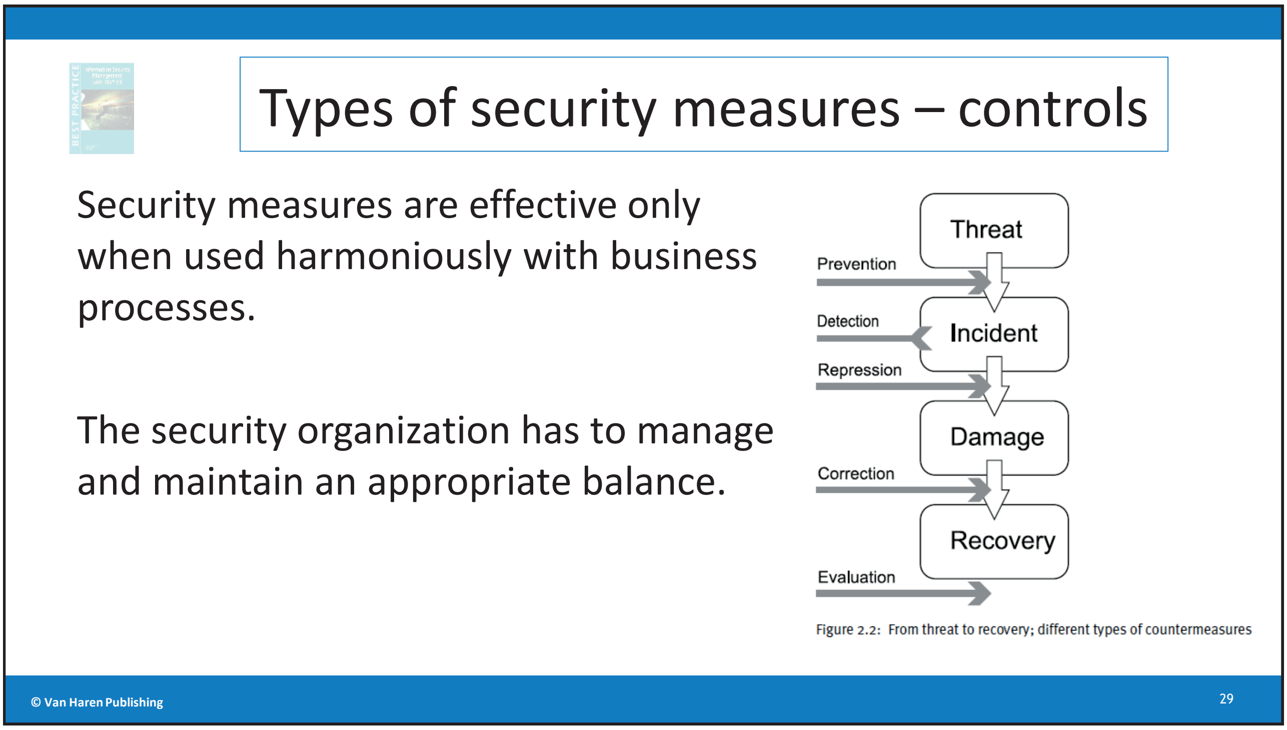
© Van Haren Publishing 27



Types of security measures – controls

Literature A: Information Security Management with ITIL v3

© Van Haren Publishing 28



Types of security measures – controls

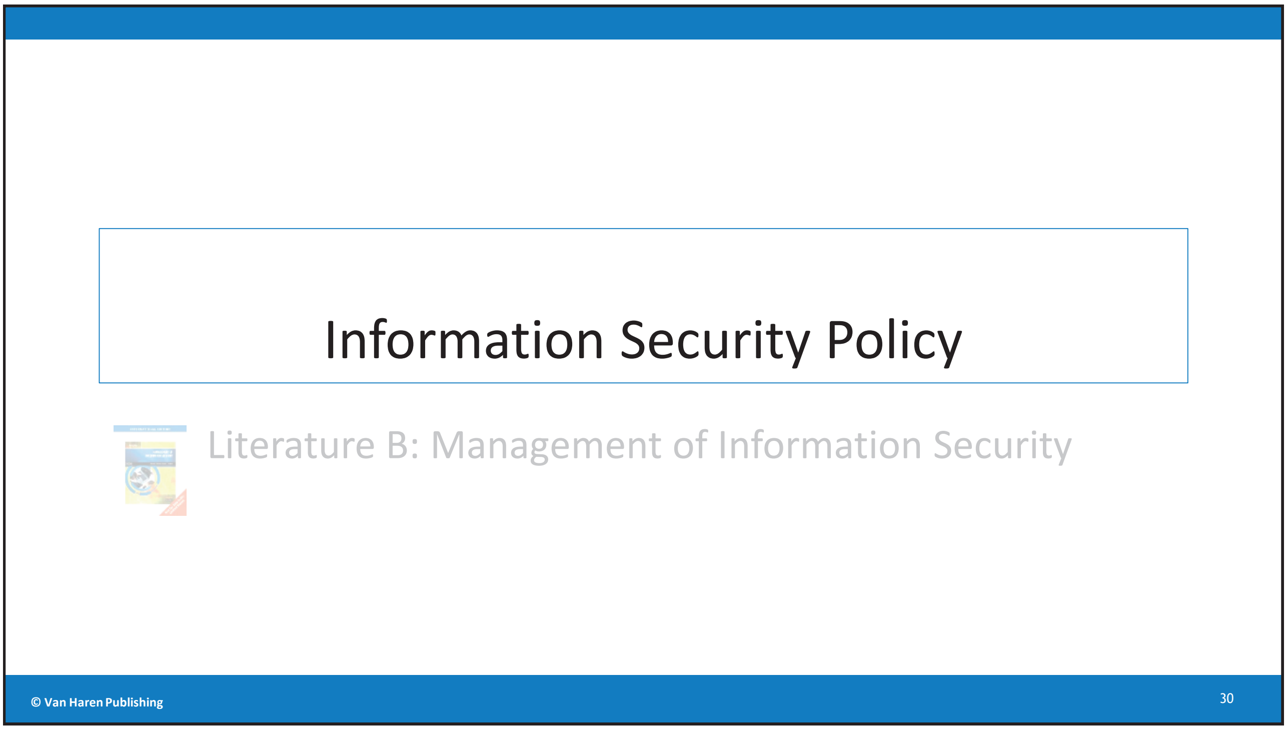
Security measures are effective only when used harmoniously with business processes.

The security organization has to manage and maintain an appropriate balance.

Figure 2.2: From threat to recovery; different types of countermeasures

© Van Haren Publishing

29

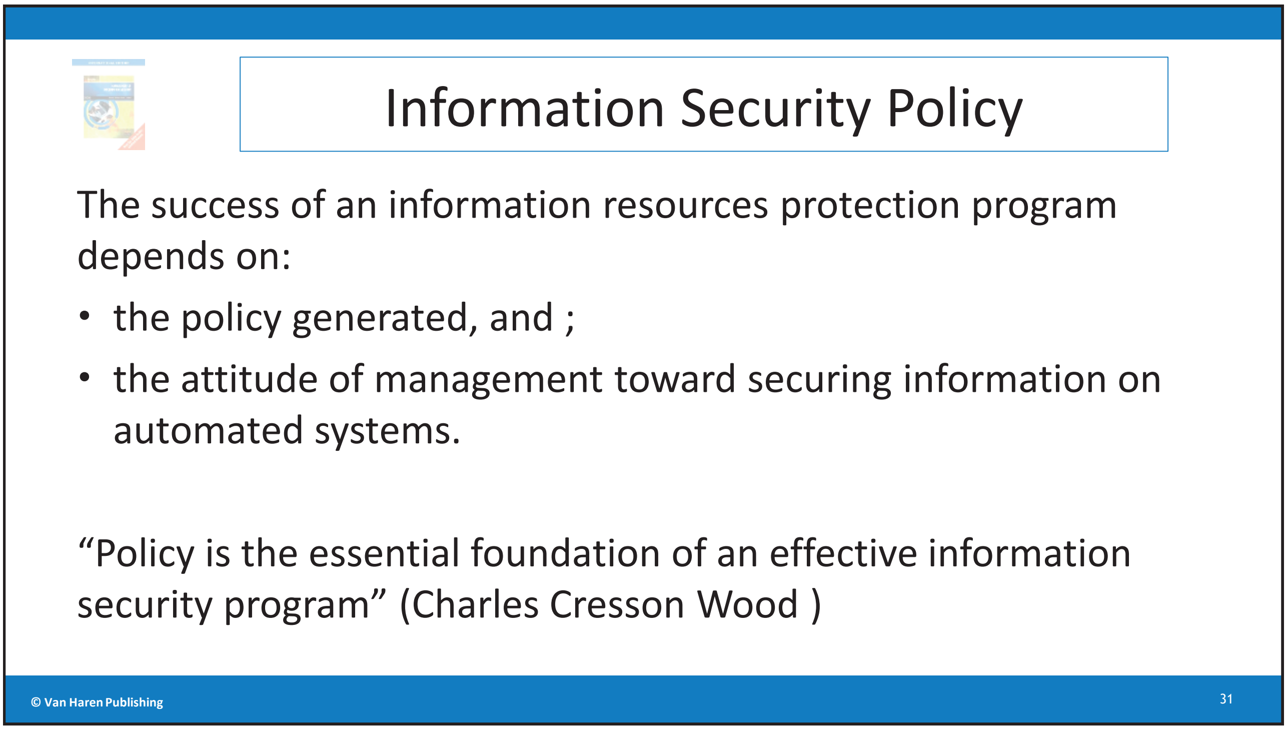


Information Security Policy

Literature B: Management of Information Security

© Van Haren Publishing

30



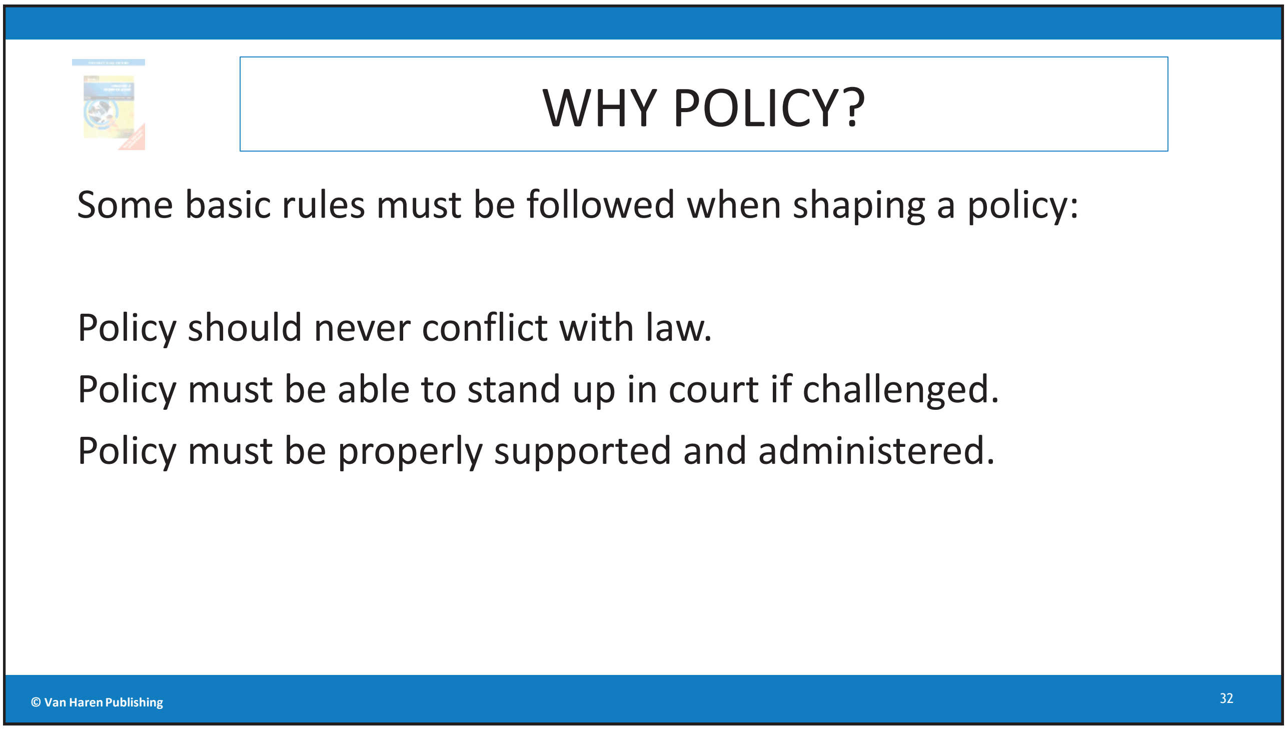
Information Security Policy

The success of an information resources protection program depends on:

- the policy generated, and ;
- the attitude of management toward securing information on automated systems.

“Policy is the essential foundation of an effective information security program” (Charles Cresson Wood)

© Van Haren Publishing 31



WHY POLICY?

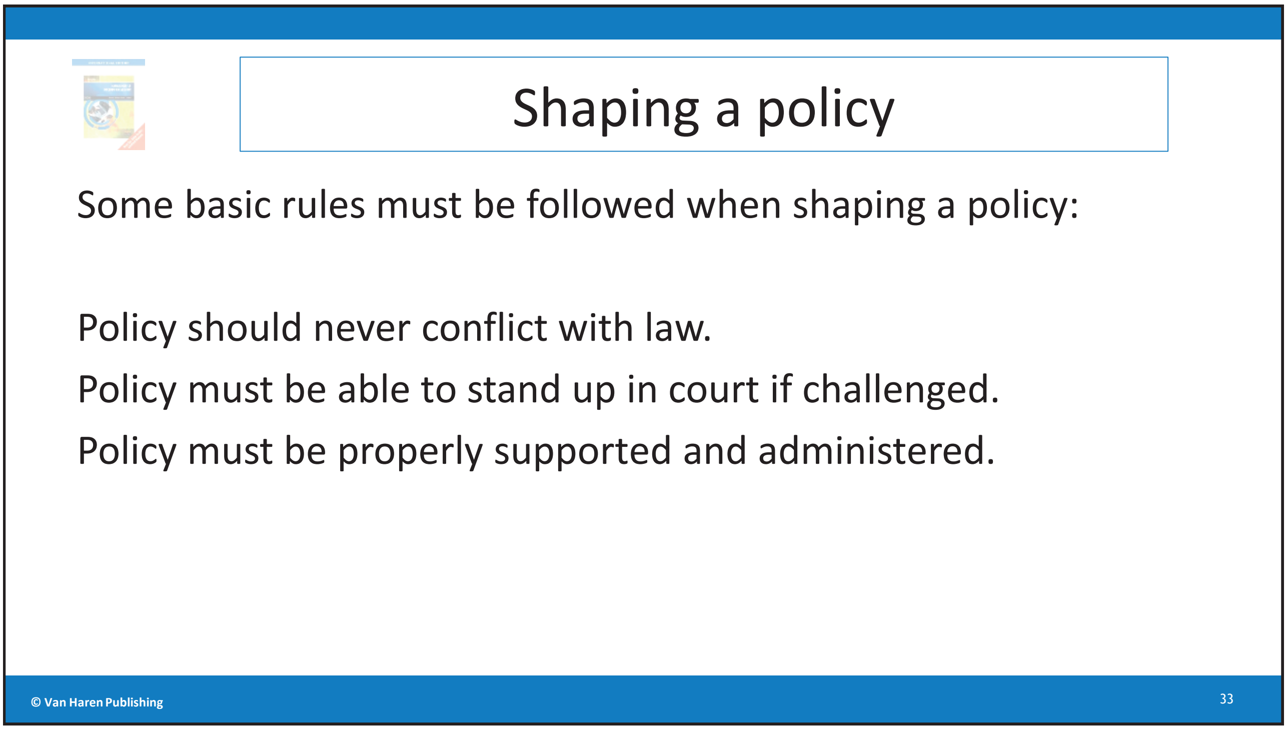
Some basic rules must be followed when shaping a policy:

Policy should never conflict with law.

Policy must be able to stand up in court if challenged.

Policy must be properly supported and administered.

© Van Haren Publishing 32



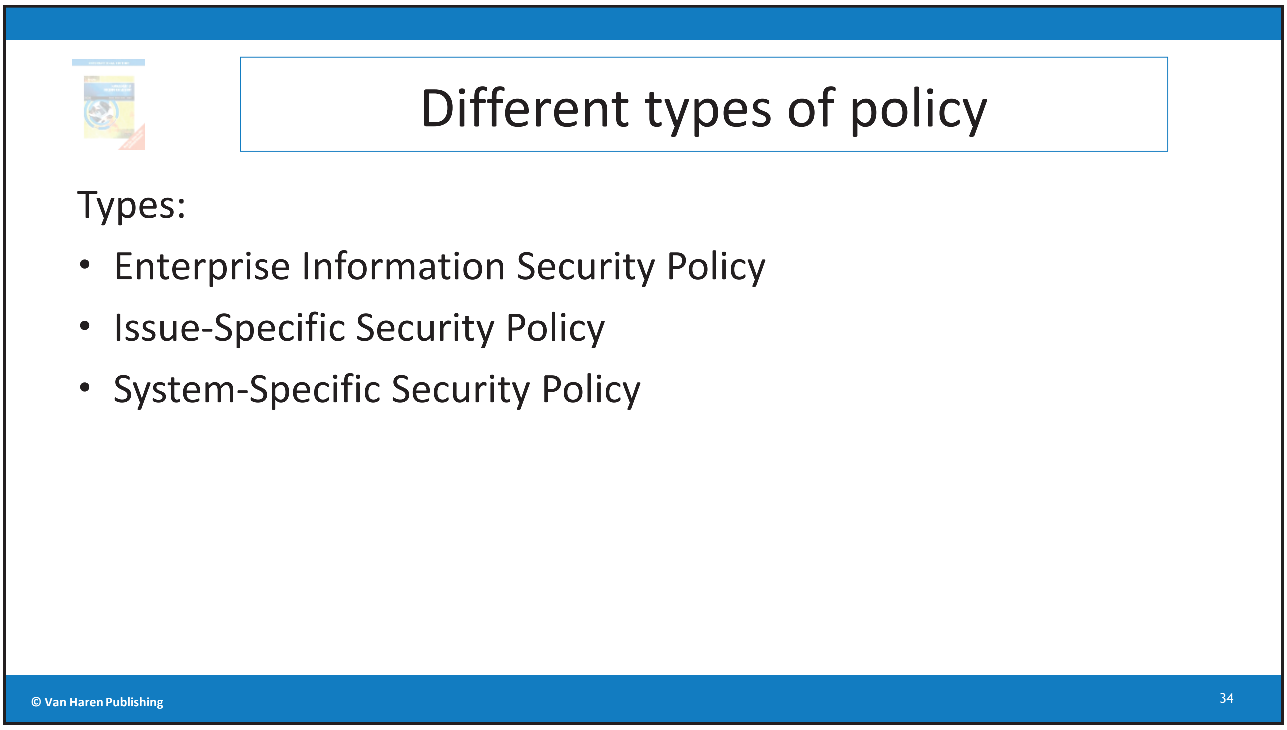
Shaping a policy

Some basic rules must be followed when shaping a policy:

Policy should never conflict with law.

Policy must be able to stand up in court if challenged.

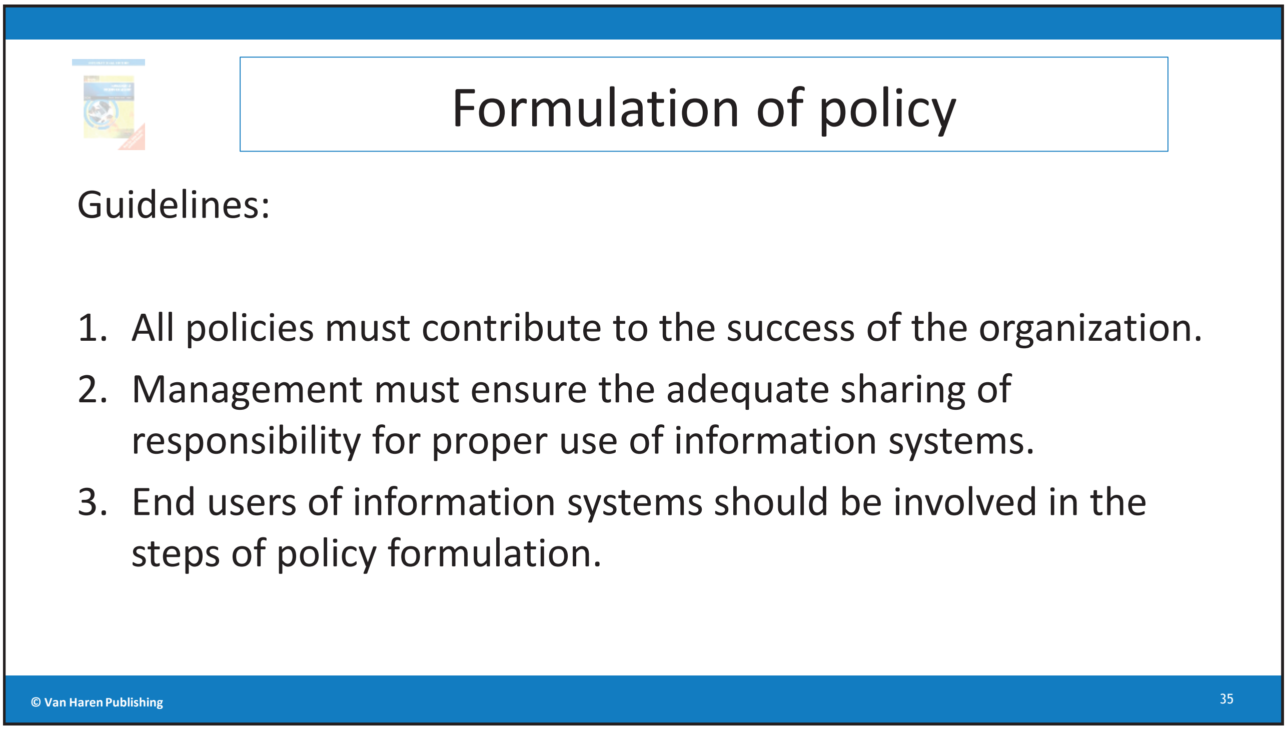
Policy must be properly supported and administered.



Different types of policy

Types:

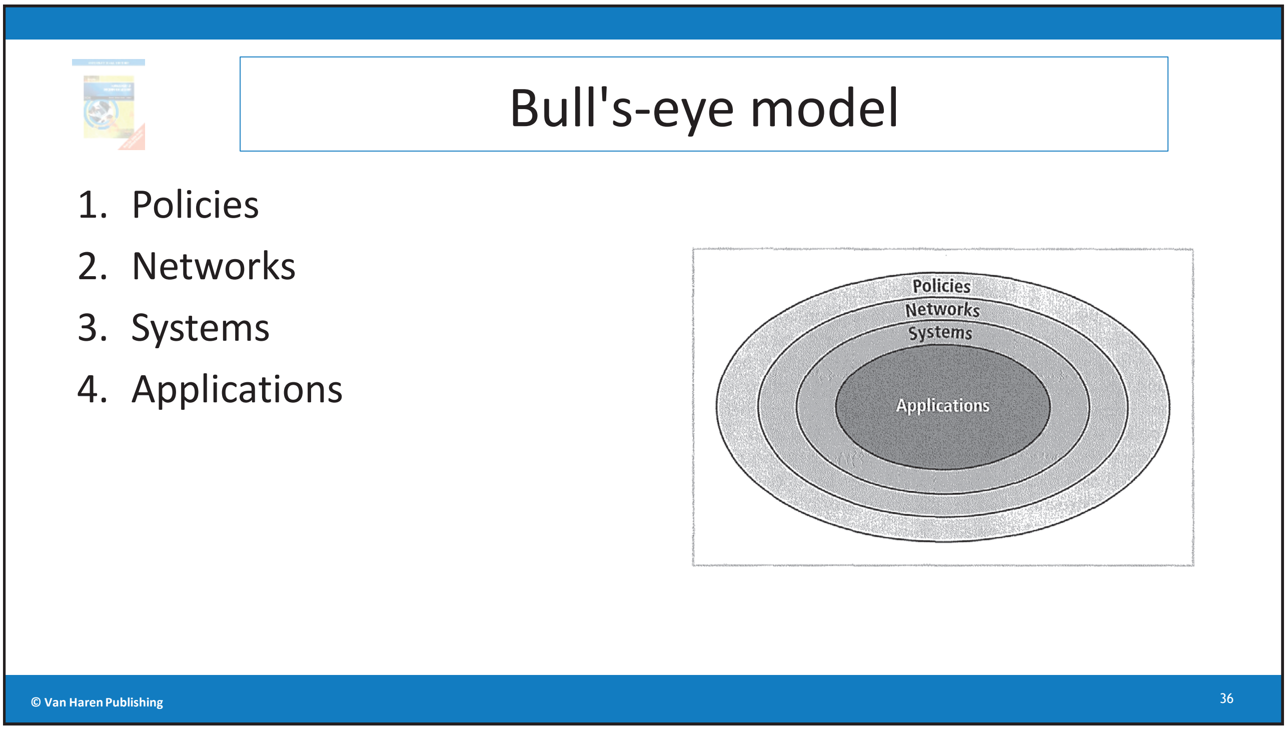
- Enterprise Information Security Policy
- Issue-Specific Security Policy
- System-Specific Security Policy



Formulation of policy

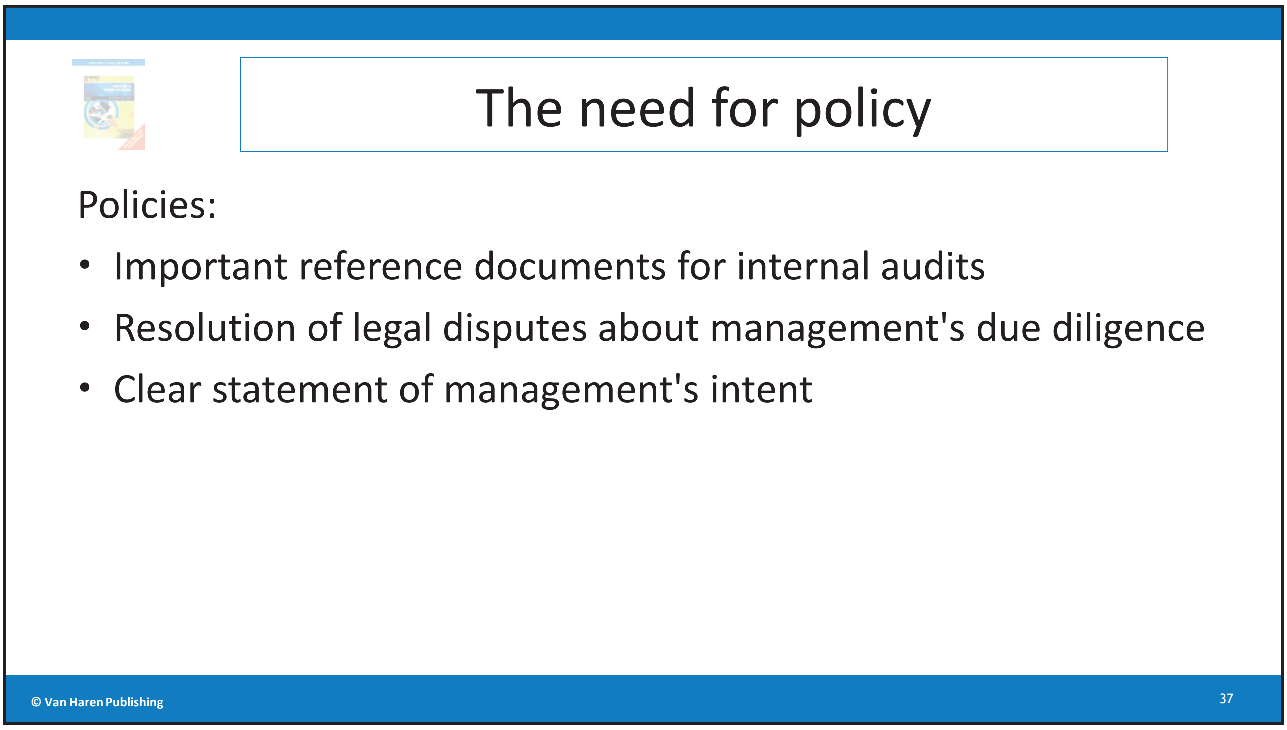
Guidelines:

1. All policies must contribute to the success of the organization.
2. Management must ensure the adequate sharing of responsibility for proper use of information systems.
3. End users of information systems should be involved in the steps of policy formulation.



Bull's-eye model

1. Policies
2. Networks
3. Systems
4. Applications

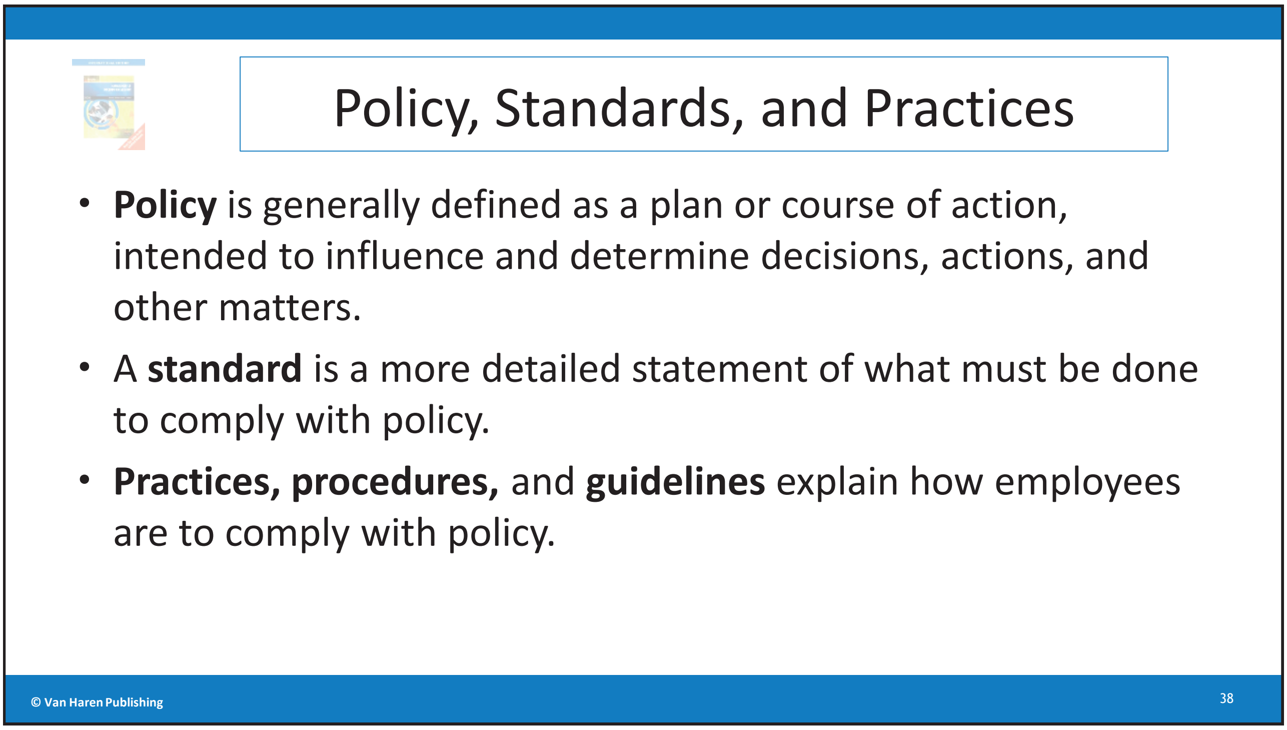


The need for policy

Policies:

- Important reference documents for internal audits
- Resolution of legal disputes about management's due diligence
- Clear statement of management's intent

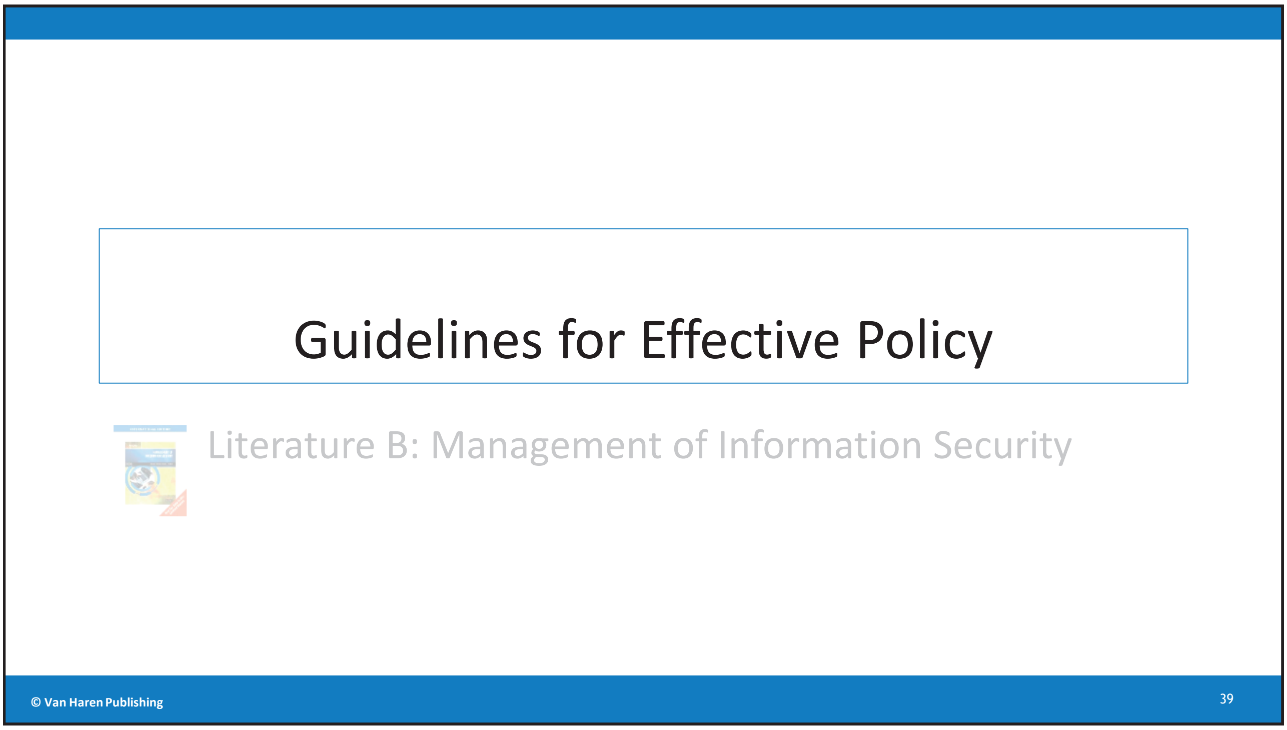
© Van Haren Publishing 37



Policy, Standards, and Practices

- **Policy** is generally defined as a plan or course of action, intended to influence and determine decisions, actions, and other matters.
- A **standard** is a more detailed statement of what must be done to comply with policy.
- **Practices, procedures,** and **guidelines** explain how employees are to comply with policy.

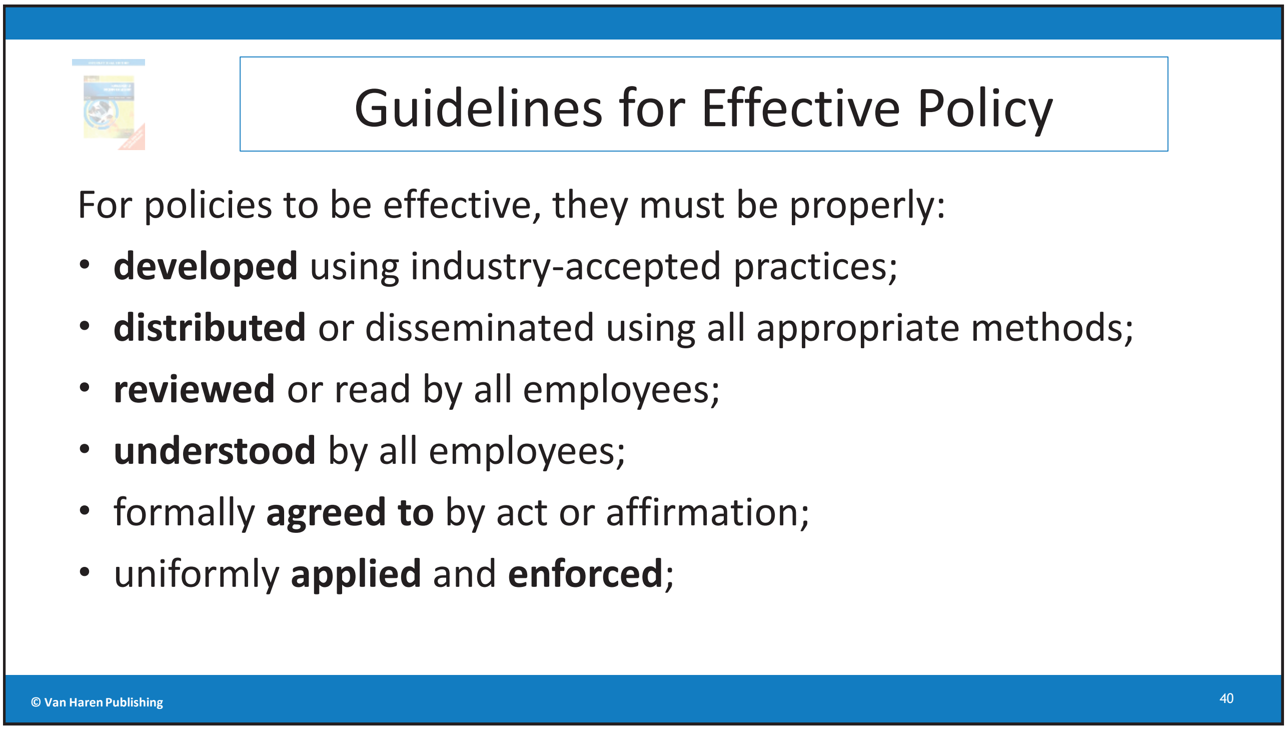
© Van Haren Publishing 38



Guidelines for Effective Policy

Literature B: Management of Information Security

© Van Haren Publishing 39

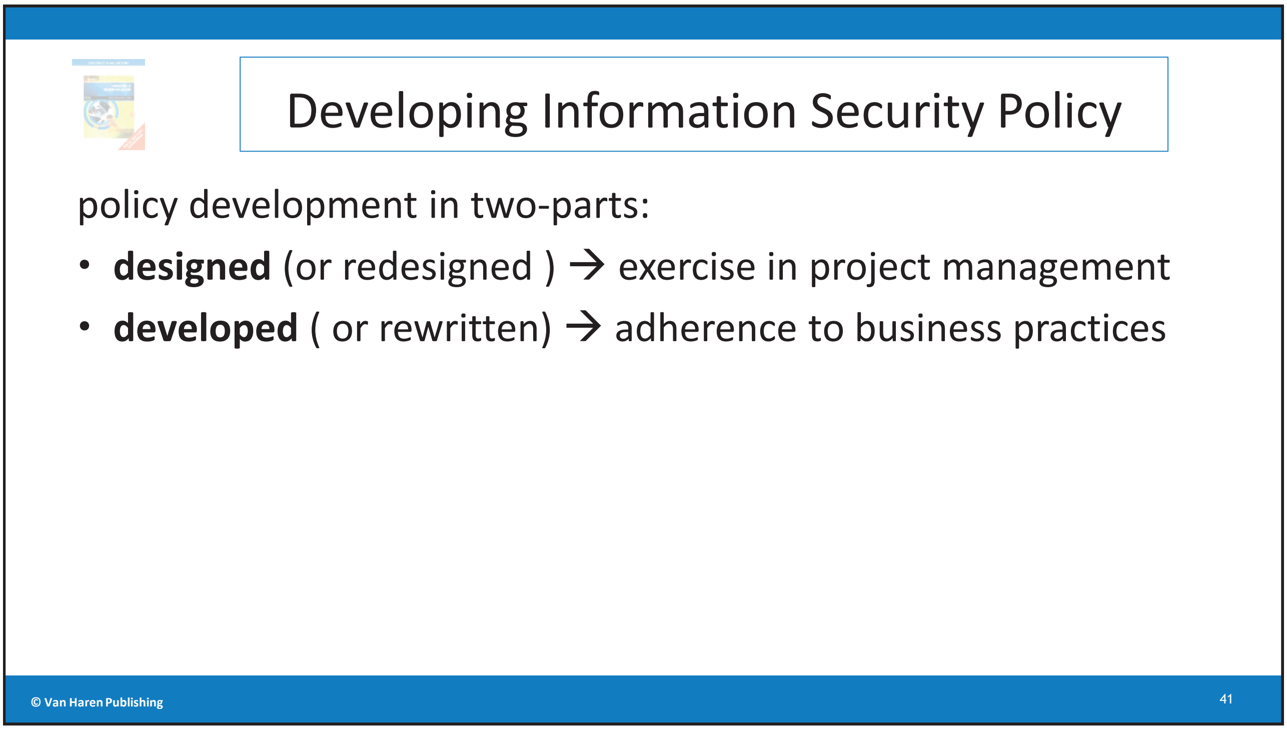


Guidelines for Effective Policy

For policies to be effective, they must be properly:

- **developed** using industry-accepted practices;
- **distributed** or disseminated using all appropriate methods;
- **reviewed** or read by all employees;
- **understood** by all employees;
- formally **agreed to** by act or affirmation;
- uniformly **applied** and **enforced**;

© Van Haren Publishing 40

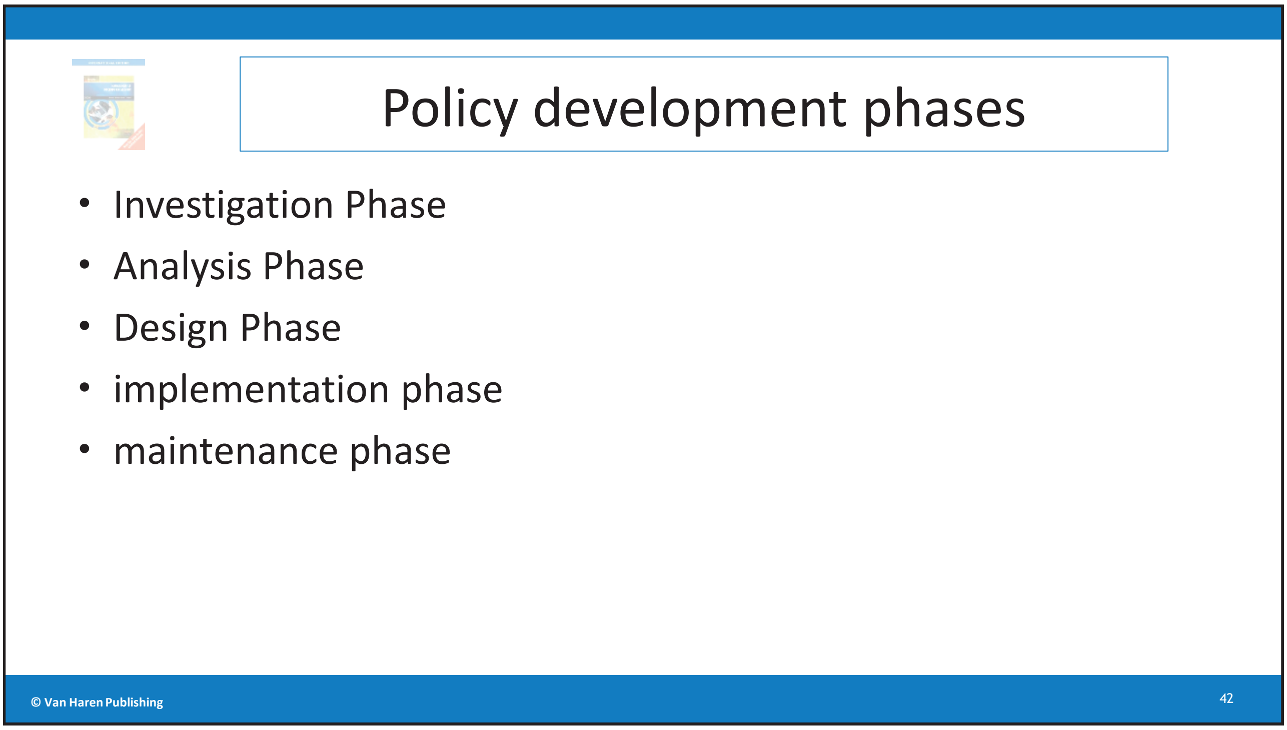


Developing Information Security Policy

policy development in two-parts:

- **designed** (or redesigned) → exercise in project management
- **developed** (or rewritten) → adherence to business practices

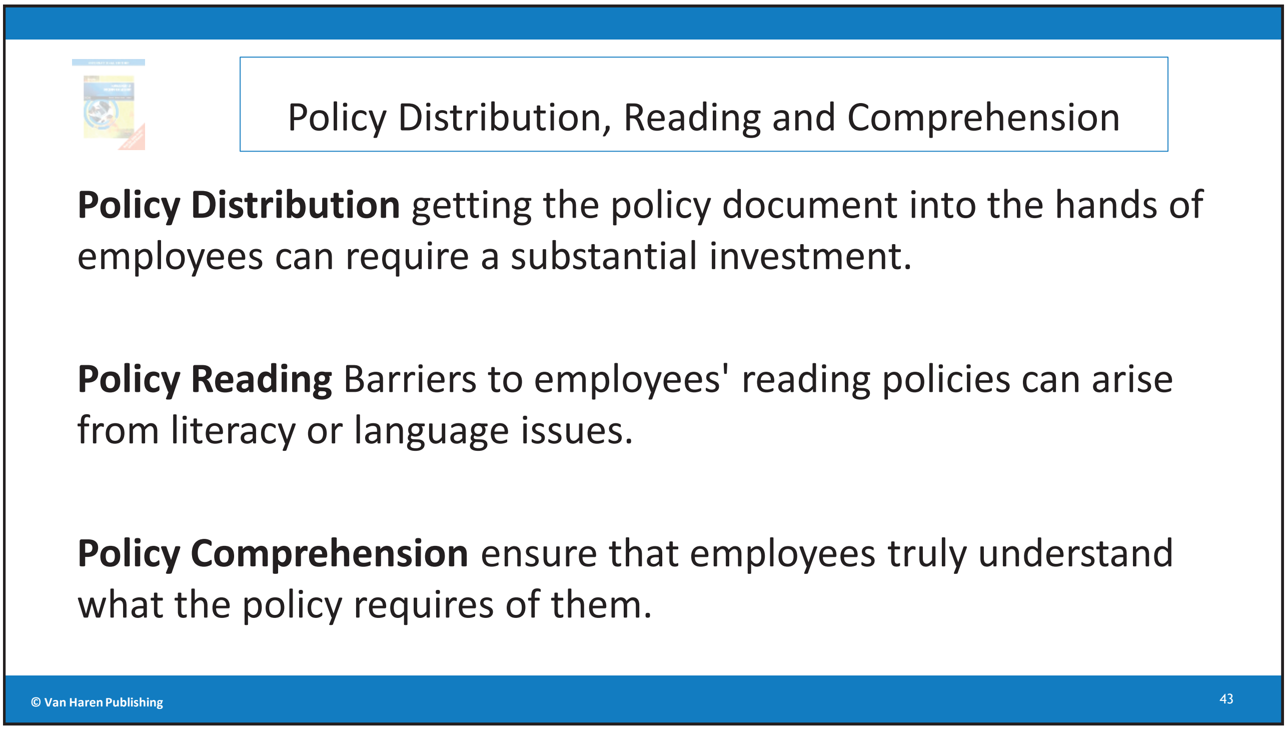
© Van Haren Publishing 41



Policy development phases

- Investigation Phase
- Analysis Phase
- Design Phase
- implementation phase
- maintenance phase

© Van Haren Publishing 42



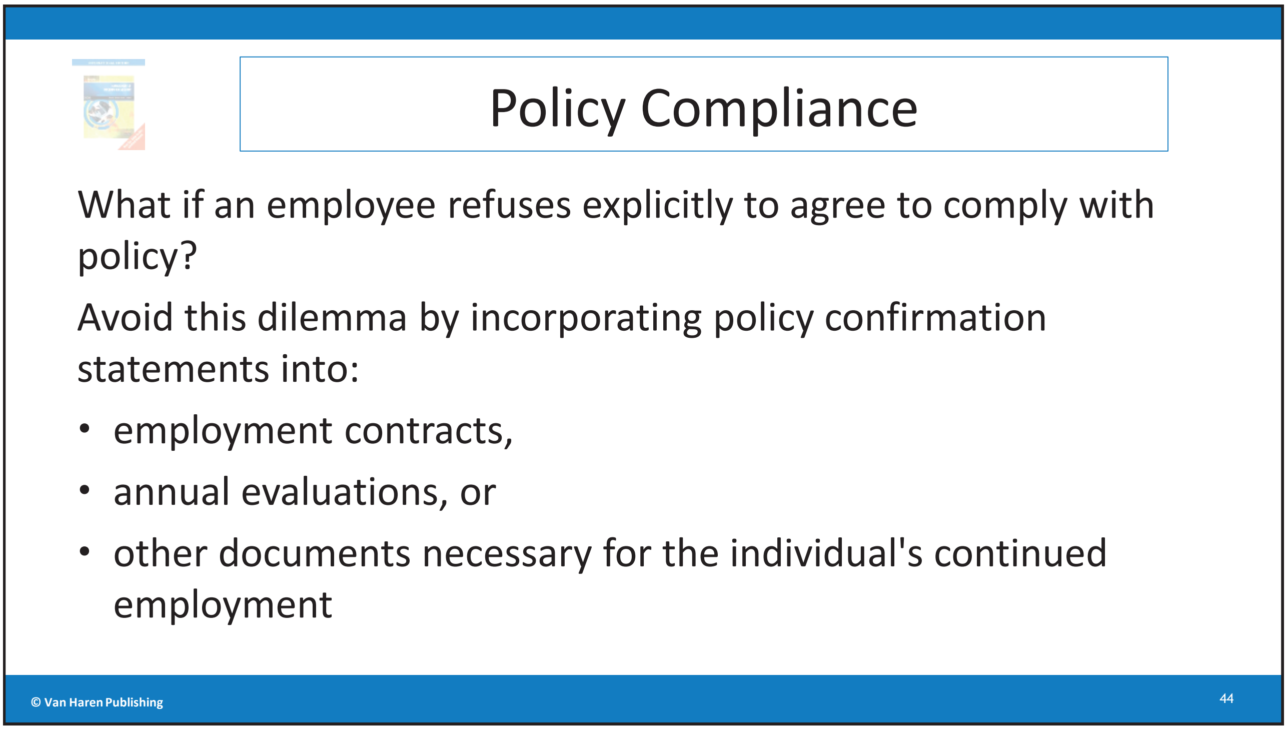
Policy Distribution, Reading and Comprehension

Policy Distribution getting the policy document into the hands of employees can require a substantial investment.

Policy Reading Barriers to employees' reading policies can arise from literacy or language issues.

Policy Comprehension ensure that employees truly understand what the policy requires of them.

© Van Haren Publishing 43



Policy Compliance

What if an employee refuses explicitly to agree to comply with policy?

Avoid this dilemma by incorporating policy confirmation statements into:

- employment contracts,
- annual evaluations, or
- other documents necessary for the individual's continued employment

© Van Haren Publishing 44