COURSEWARE

Information Security Management Professional (ISMP) based on ISO/IEC 27001 Courseware

4th revised edition

Van Haren PUBLISHING

Information Security Management Professional (ISMP) based on ISO 27001

Courseware - 4th revised

English

Colofon

Title:	Information Security Management Professional (ISMP) based on ISO 27001 Courseware - 4th revised
Authors:	Ruben Zeegers & Dolf J.H. van der Haven
Publisher:	Van Haren Publishing, 's-Hertogenbosch
ISBN Hard Copy:	978 94 018 107 39
Edition:	First edition, first print, December 2017
	Second edition, first print September 2018
	Third edition, first print, March 2021
	Fourth edition, first print, September 2023
Design:	Van Haren Publishing, 's-Hertogenbosch
Copyright:	© Van Haren Publishing 2023
	For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

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.

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 was 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. For this reason, the Courseware has also been accredited, 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 have been provided with the material.

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

Although the courseware is complete, the possibility that the trainer may deviate 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 strongly recommended to follow the structure of the courseware and publications for maximum exam preparation.

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.

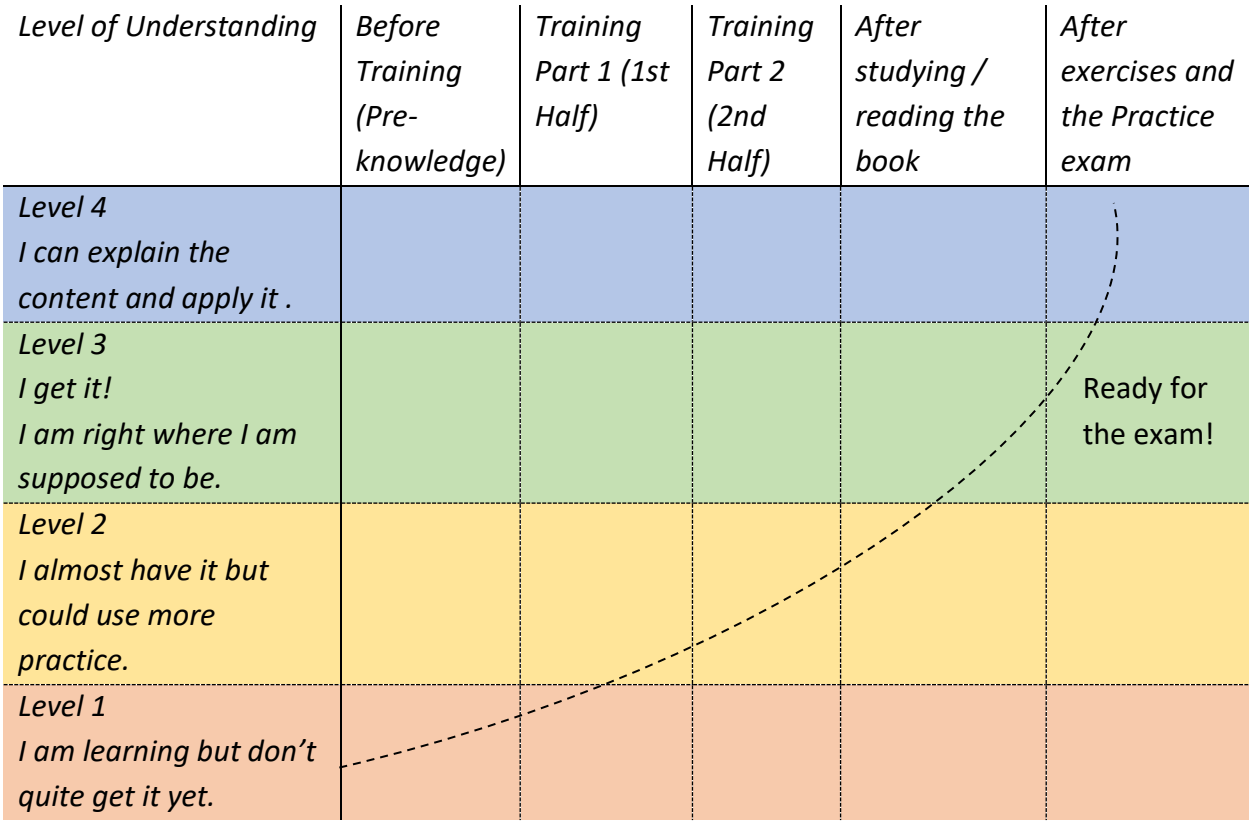
Table of content

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.



(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

Day 1

09:00 - 9:30	Introduction, About this course
09:30 - 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

09:00 – 12:00	2.1 Principles of Risk Management
12:00 - 12:30	2.2 Selecting Controls
12:30 – 14:00	Lunch
14:00 - 17:00	2.3 Residual Risk
	Practical assignment 2

Day 3

09:00 - 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 Physical en People controls

Information Security Management Professional

INFORMATION SECURITY MANAGEMENT PROFESSIONAL
based on ISO/IEC 27001

COURSEWARE

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

Additional Literature:

A	B	C	D
27000	**27001**	**27002**	**27005**
ISO Standard - Information Security Management ISO/IEC 27000:2018	**ISO Standard - Information Security Management** ISO/IEC 27001:2022	**ISO Standard - Information Security Management** ISO/IEC 27002:2022	**ISO Standard - Information Security Management** ISO/IEC 27005:2022

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 – 12:00	2.1 Principles of Risk Management
12:00 – 12:30	2.2 Selecting Controls
12:30 – 14:00	lunch
14:00 – 17:00	2.3 Residual Risk Practical assignment 2

Day 3	
9:00 – 10:30	3.1 Organizational Controls
10:30 – 12:00	3.2 Technological Controls
12:00 – 12:30	lunch
12:30 – 14:00	Technological Controls continued
14:00 – 16:00	3.3 Physical and People Controls

EXIN INFORMATION SECURITY

Information Security Management Professional
About this course

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

COURSEWARE

The course

Course subject

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

Exam requirements

Exam requirements	Exam specifications	Weight
1. Information security perspectives		**10%**
	1.1 Business interest of information security	3.3%
	1.2 Customer perspective on governance	3.3%
	1.3 Supplier's responsibilities in security assurance	3.3%
2. Risk management		**30%**
	2.1 Principles of risk management	10%
	2.2 Control risks	10%
	2.3 Deal with remaining risks	10%
3. Information security controls		**60%**
	3.1 Organizational controls	20%
	3.2 Technical controls	20%
	3.3 Physical controls and people controls	20%
	Total	**100%**

Exam specifications

1	**Information security perspective**
1.1	Business interest of information security
The candidate can…	
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 perspective on governance
The candidate can…	
1.2.1	explain the importance of information governance when outsourcing.
1.2.2	recommend a supplier based on security controls.
1.3	Supplier's responsibilities in security assurance
The candidate can…	
1.3.1	distinguish security aspects in service management processes.
1.3.2	support compliance activities.
2	**Risk management**
2.1	Principles of risk management
The candidate can…	
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	Control risks
The candidate can…	
2.2.1	categorize controls based on confidentiality, integrity, and availability.
2.2.2	choose controls based on incident cycle stages.
2.2.3	choose relevant guidelines for applying controls.
2.3	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.

Exam specifications (continued)

3	**Information security controls**
3.1	Organizational controls
The candidate can…	
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.
3.1.5	support the development and testing of a business continuity plan.
3.2	Technological controls
The candidate can…	
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	Physical controls and people controls
The candidate can…	
3.3.1	recommend controls for physical access.
3.3.2	recommend security controls for employment life cycle.

ISO/IEC 27001:2022 Overview

ISO/IEC 27001 standard

The ISO/IEC 27001 standard represents the international standard for the establishment of an Information Security Management System (ISMS). The most recent version was published in 2022 by the International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC). The standard is used world-wide by organizations that would like to implement Information Security based on a global standard.

ISO/IEC 27001:2022 Structure

- **0 Introduction –** General introduction to the standard and the wider ISO/IEC 27000 series of standards.
- **1 Scope –** description of an ISMS generic requirements suitable for any size or/and type of organization.
- **2 Normative references –** description of other ISO standards that are required to understand this standard.
- **3 Terms and definitions –** description of the main terms and definitions used by ISO/IEC 27001.
- **4 Context of the organization –** description of how organizations should look to their own context in order to define a good scope for the ISMS, to manage the stakeholders' expectations and the main items and processes that must be established, implemented, maintained and continually improved in the ISMS.
- **5 Leadership -** description of the role and responsibilities from Top Management regarding to the ISMS, as well as define the information security main roles.
- **6 Planning -** description of the actions that must be taken to identify, analyze and plan to treat information risks. A description and definition of the Information Security objectives must to take place as well.
- **7 Support –** description of the actions that must be taken to: assign adequate and competent resources, create and develop information security awareness, prepare, publish and control the required documented processes, policies and procedures.
- **8 Operation –** description of detailed actions to assess and treat information security risks, change management and documents (registers to facilitate auditing activities).
- **9 Performance evaluation -** description of the actions that must be taken to: monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving where necessary.
- **10 Improvement -** description of the actions that must be taken to continuously improve the ISMS based on audit findings, management reviews, customers inputs, among others.
- **Annex A Controls reference –** description of the main information security controls that must be adopted by the organizations. The selected and used controls as well as the non-used ones must be described on the Statement of Applicability (SoA) document.

ISO/IEC 27001:2022 Certification Path

The ISMS implementation and certification **can differ from organization to organization**. However, these are the most common steps.

1. Obtain management commitment
2. Define scope and context of the ISMS
3. Plan the project
4. ISMS objectives and overall management system
5. Information security policy
6. Risk assessment
7. Implement controls
8. Statement of Applicability (SoA)
9. Internal audit
10. Management review
11. External audit stage one
12. External audit stage two (certification)

EXIN INFORMATION SECURITY

Information Security Management Professional
Module 1 Information Security Perspective

COURSEWARE

Information security perspectives

1.1 Business perspective

1.2 Professional / Customer perspective

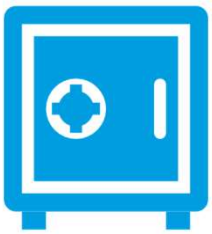
1.3 Service provider / supplier perspective

Module 1.1

BUSINESS PERSPECTIVE

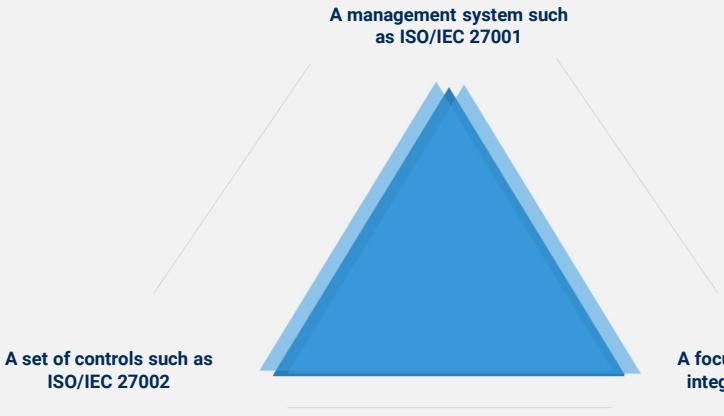
Information security deals with…

1. The definition, implementation, maintenance, compliance and evaluation of an ISMS
2. Risk management, leading to a coherent set of controls



3. safeguard the confidentiality, integrity and availability (CIA) of information
4. the (manual and automated) information supply

This implies…



Business perspective

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

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

A: §2.1; §5.3.4; §5.7; Annex A
B: Chapter 2
C: §15.1; §15.2

EXIN INFORMATION SECURITY

Module 1.2

CUSTOMER/END USER PERSPECTIVE

The customer perspective

- Customers demand 24/7 business continuity of operations.
- Due to the open marketplace customers can take their business elsewhere.
- Concerns surrounding privacy are still very strong. Although the use of social media, and the selling out of personal privacy as a result, indicate that this is highly contextual.
- Customers have become very vocal when their privacy is breached. Any security incidents therefore get a lot of media attention.
- Customers place trust in organizations that are transparent in the way they deal with risks.

The customer perspective

- In B2B environments the chain of trust requires compliance and governance
- End users receive almost no training, also information security training is mostly lacking
- End users do not perceive security risks in the same way as professionals do
- Security is often regarded as an optional add-on instead of an embedded design requirement
- Stakeholders clueless as to what proof they require to decide that information security risks are managed

A: § 2.1; Chapter 4; Annex A
B: Chapter 12
C: § 15.1; § 15.2; Chapter 18, § 12.7

Module 1.3

SERVICE PROVIDER / SUPPLIER PERSPECTIVE

Service Provider perspective

- Providers need to show due diligence regarding information security.
- The usage of best practice standards prevails.
- Incident, change, and continuity management are key processes.
- Information security performance needs to become a part of the SLA (Service Level Agreement) management processes.
- Active monitoring and vulnerability management need more attention.
- Transparency is key but difficult to maintain in a shared service environment.

Service Provider perspective

- Service providers need to understand their customers' business and requirements.
- IT service management and information security need to be implemented using best-practice standards such as ITIL, COBIT and ISO standards. SMART performance indicators are key.
- Suppliers are not always transparent about security risks inherent within the solutions they provide. Third-party assessment of the risks is vital.
- Perimeter security is still important but data security even more so, this requires a different mindset and products/solutions.

EXIN INFORMATION SECURITY

Information Security Management Professional
Module 2 Risk Management

COURSEWARE

Risk Management subjects

2.1 Analysis - Risk Assessment

2.2 Controls - Selection of mitigating controls/strategies

2.3 Residual risk

A: § 2.1.3
B: Chapter 8
C: Chapter 0 Introduction; Chapter 8

Module 2.1

ANALYSIS

Risk Assessment

Risk assessment answers a number of questions:

- What (information assets) do we need to protect
- Why do we need to protect these assets
- What are the risks
- What are the priorities in dealing with these risks
- What are the options to deal with these risks

Steps in the Risk Assessment Process

1 Assets

- Determine which assets are in scope of the assessment
- Determine who the owners of the assets are
- Discuss the threats to these assets with the owners

2 Threats

- Decide who the threat agents are
- Get expert opinions on vulnerabilities of these assets
- Get expert opinions on likelihood that the threats will occur
- Get expert opinions on the impact if/when the threats occur
- Have a brainstorm with representatives of all stakeholders

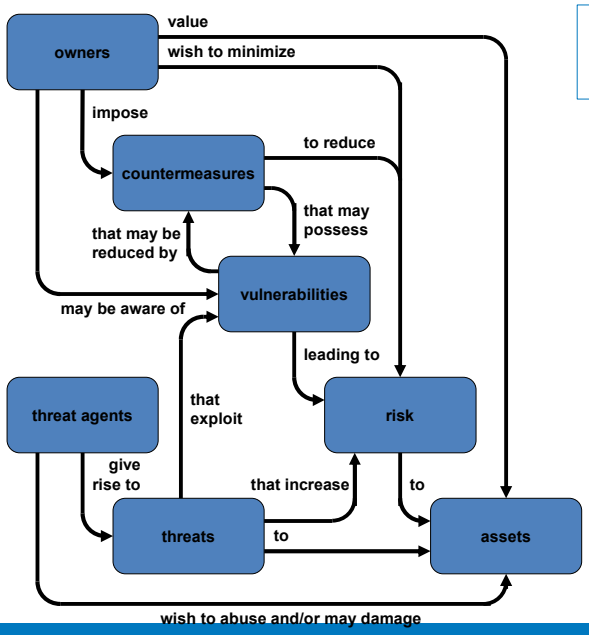
Risks 3

- Define a formula to calculate the magnitude of risks
- Define the risk appetite of the owner(s)
- Find options to mitigate unacceptable risk(s)

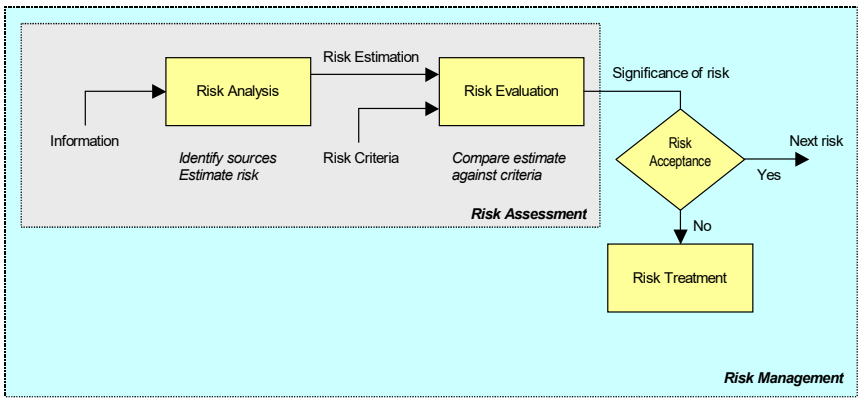
Controls 4

- Implement controls
- Understand and mitigate the new risks of the controls
- Accept any residual risks and repeat all of the above

All relevant steps



Risk Management according to ISO/IEC 27001/2



ISO/IEC 27001 explicitly refers to and aligns with
ISO/IEC 31000 – Risk management – Principles and guidelines

Caveats

- Produce a **B**usiness **I**mpact **A**nalysis first to determine where a risk assessment is required.
- Implement a baseline on the risks. However, risk mitigation controls must be implemented only when required.
- Discussing risks that have not (yet) occurred need an open mind.
- Analyzing risks can be facilitated by a specialist but requires a multi-disciplinary approach with members of each business function.
- There are many tools available, but tools can only assist the process; not perform it!
- The risk assessment will provide the direction as to which controls must be implemented to tackle the risks that are being faced by the organization. This is a must when designing an enterprise-wide information security program.
- The best way to achieve a good level of effectiveness in security governance is to perform a periodic risk assessment as part of a risk management program.
- The organization will not bring the number of risks down to zero. However, stakeholders must be informed regarding to the residual risks and accept them in agreement with the organization's risk appetite.

Business Impact Analysis

- Only deals with the impact of an event such as loss of, damage to or disclosure of information
- In business terms, i.e. monetary loss, damage to reputation, legal consequences etc.
- Enables an organization to pinpoint those processes where security is important
- Must be performed together with the business owner(s)
- Does not analyze assets, threats, vulnerabilities, probabilities etc.; only the impact of events
- Acts as a filter of activities (processes, parts of the organization, ICT functions etc.) where a risk assessment is required and where not (i.e. where a small set of baseline controls suffices)

Baseline principle

- Implement a limited set of controls for all assets.
- Be able to explain and justify why it is sufficient to implement only those controls on those assets (tool: business impact analysis).
- Do a risk assessment on all the other assets and implement extra controls only where required.

Note: Legal requirements must always be part of the baseline set of controls!

EXIN INFORMATION SECURITY

ASSESSING THE RISKS

Determine the assets in scope of the assessment

- Purpose:
  Determines what assets will be assessed during the next steps.
- How:
  The business impact analysis will have made clear what processes lead to the highest impact if loss, damage or disclosure occurs. Assets within these processes are people, systems, applications, operating systems, buildings/rooms, utilities etc. etc.
- Guidelines:
  Draft the list of assets but keep a high level of abstraction and group assets where possible.

Determine who the owners are of these assets

- Purpose:
  Only the owners can clearly discuss the value of assets.
- How:
  Mostly the business impact analysis has already clarified who the owners are.
- Guidelines:
  Determining the owners of shared assets (such as network, email infrastructure, internet access) can be tricky… then the owner will be the manager responsible for (delegated) maintenance of these assets.

Discuss with these owners the threats to the assets

- Purpose:
  To determine what threats are applicable to the assets within scope, only those threats need to be analyzed in the next steps.
- How:
  Standard lists of threats do exist but do discuss with the owner whether the list is complete.
- Guidelines:
  Be as complete as possible, do not filter out threats at this point. Try to compile a list of inherent threats, not the threats for which there are residual risks at this moment. For instance do not cancel out the threat of data loss because back-ups are already made.

Decide who the threat agents are

- Purpose:
  Knowing your enemy enables better determining probabilities and vulnerabilities of threats occurring.
- How:
  Discuss who might be interested in attacking your organization and the means these adversaries have to their disposal.
- Guidelines:
  Adversaries can be employees, criminals, all sorts of hackers, competitors, states, terrorists etc.

Get expert opinions on vulnerabilities of the assets

- Purpose:
  To enable those present during the risk assessment workshop to have enough detailed information to make informed decisions.
- How:
  Interviews with experts on information security aspects relevant to the assets in scope such as technical experts and facility managers but also local government, police, fire brigade etc.
- Guidelines:
  The obtained data need to be qualified in terms of high/medium/low vulnerability. Try to be exhaustive. Talk to as many experts as possible within scope and budget.

Get expert opinions on the likelihood that the threats occur

- Purpose:
  To enable those present during the risk assessment workshop to have enough detailed information to make informed decisions.
- How:
  Interviews with experts on information security aspects relevant to the assets in scope such as technical experts and facility managers but also local government, police, fire brigade etc.
  Also get publicly available information where available from incidents in the past within and outside of the organization.
- Guidelines:
  The obtained data needs to be qualified in terms of high/medium/low vulnerability. Try to be exhaustive. Talk to as many experts as possible within scope and budget.

Define the impact for all threats when they occur

- Purpose:
  To enable those present during the risk assessment workshop to have enough detailed information to make informed decisions.
- How:
  For every threat discuss with experts what the maximum impact would be when the threat occurs.
- Guidelines:
  It is difficult to consider impacts when a threat has never before occurred. Consider monetary losses, legal problems, loss of business, advantages to a competitor, loss of image etc.
  If possible classify all possible losses into monetary terms.

Define a formula to calculate risk

- Purpose:
  Bring all information on a threat together in one quantitative parameter which enables to decide whether the risk is above or below the acceptable risk level.
- How:
  - **Quantitative:** When only numbers are used to calculate the risk.
  - **Qualitative:** When using classes of risk, for instance LL (low likelihood, medium impact) or quantify (VL=1, L=2, M=3, H=4, VH=5) and then multiply (L*M = 1*3 = 3) or use a different formula (most accepted risk methodology).
- Guidelines:
  Be careful when quantifying not to loose the distinction between for instance L*M=1*3 and M*L=3*1 (both are 3).

Define the risk appetite of the owner(s)

- Purpose:
  Determining the level above which a risk is unacceptable (i.e. should be mitigated where possible).
- How:
  For every threat or for all threats in one go, have the process owner decide upon which level of risk is unacceptable.
- Guidelines:
  Also take an outside view; what would customers/suppliers find acceptable? What would legal entities consider acceptable?

Remarks

1.
Not always the distinction between probability and vulnerability is clear. An example; imagine two houses next to a chemical factory. An explosion at the factory causes fires in its surrounding. Both houses have the same probability for fire caused by the problem in that factory.

But if one of these houses is made from wood and the other from concrete, the wooden house has a much higher vulnerability for fire. Since vulnerability is difficult to determine, limit the number of classes to (for instance) only high or low vulnerability.

2.
Before doing a risk assessment reach consensus on classes for probability, vulnerability and impacts. For instance:

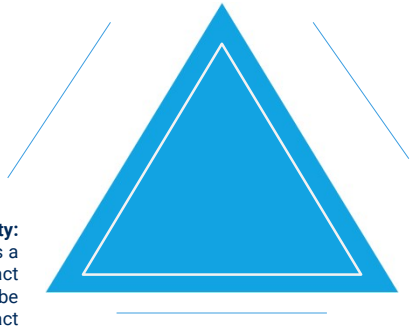
Probability:	high: it can happen any day, medium: could happen yearly, low: will never happen
Vulnerability:	high: when it happens there is a full impact, low: when it happens there will be minor impact
Impact:	high: could lead to bankruptcy, medium: impacts the bottom line, low: no impact

Remarks

Risk assessment needs to be part of the scope of every project. Usually a simple identification and rating mechanism for the threats and risks specifically related to the project is sufficient.

Before doing a risk assessment, your organization will need to reach consensus on classes for probability, vulnerability and impacts. For instance:

Impact:
high: could lead to bankruptcy
medium: impacts the bottom line
low: no impact



Vulnerability:
high: when it happens there is a big impact
low: when it happens there will be minor impact

Probability:
high: it can happen any day
medium: could happen yearly
low: will never happen

EXIN INFORMATION SECURITY

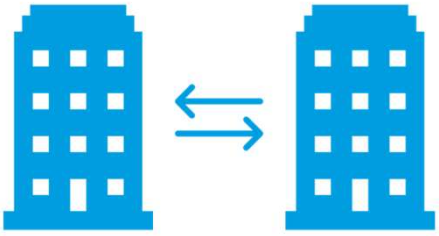
Module 2.2

CONTROLLING THE RISKS

Risk Treatment in ISO/IEC 27001:2022

- **Select Risk treatment options**
- **Determine the needed controls**
- **Compare the selected controls to ISO/IEC 27001:2022 Annex A**
- **Create a Statement of Applicability indicating which controls from Annex A match your controls**
- **Create a plan to treat risks**
- **Obtain the risk owners' approvals to treat the risks and their acceptance of residual risk**

Find Ways to Mitigate unacceptable Risk(-s)



- **Purpose:**
  Select the risks for which mitigating controls are required.
- **How:**
  Decide whether a risk can be avoided, transferred to another party, accepted or whether it needs mitigation. Or maybe the risk is already mitigated by a control.
- **Guidelines:**
  For example, avoidance of the risk means cancelling the business process in question or moving the organization to an area with a lower/other risk profile. Transferring a risk can be done by insuring against it. Both avoidance and transferring tend to be exceptions. This tends to lead to discussions to decide whether a risk can be accepted or needs mitigation. Sometimes risks are already covered, for example Escrow arrangements to protect software code.

Implementing Controls

- **Purpose:**
  Where there are risks that cannot be accepted, controls need to be selected and implemented with the aim of lowering probability, vulnerability and/or impact.
- **How:**
  Controls should always follow from your risk assessment. For inspiration, you can use a standard baseline best-practice set of controls such as ISO/IEC 27002 and select those controls from it that mitigate the risk.
- **Guidelines:**
  Whether controls mitigate a risk requires expertise in technical, legal, procedural, physical/facility aspects. Make sure the expert view on all these aspects is available.

Remarks

You can use the available controls in ISO/IEC 27001 (annex A) and ISO/IEC 27002 for further guidance or inspiration for risk mitigation activities

Statement of Applicability

- The Statement of Applicability is a document that must be produced as result of the risk assessment process.
- The document can be a matrix, by listing the used information security controls (to mitigate and/or minimize the risks), the treatment options, and often also the person(s) accountable for them.
- This document is required during auditing activities to provide an overview of which controls were implemented as part of the ISMS scope.
  - Internal audit: The internal audit will be performed by the internal auditors of the organization. They also have the responsibility of checking the compliance of the organization (according to the ISMS scope) with the Information Security Policy.
  - External audit: The external audit will be performed by an independent third party. They will also assess the documentation, processes and policies. This includes the Statement of Applicability (SoA).

B: Chapter 8; Chapter 9
C: Chapter 5

Module 2.3

RESIDUAL RISK