Training Course Change Log

GENERAL INFORMATION				
Owner, Department*	Course Development Manager, Training Development Department			
Approver, Department *	Quality Assurance Supervisor, Quality Assurance Department			
Date of Approval*	2022-02-24			
Course details*	Course name:	Language:	New Version:	Previous Version:
	ISO/IEC 27001 Lead Implementer	English	8.0	7.2
Summary of the Change: The training course has been updated based on ISO/IEC 27002:2022 and Draft Amendment 1 of ISO/IEC 27001:2013.				
Day 1:				

Slide Number	Slide Description:	Modifications:	Comments

Current version	*Previous version*		*Changed from:* © Professional Evaluation and Certification Board, 2021. All rights reserved. Version 7.2 Document number: ISMSLID1V7.2 Documents provided to participants are strictly reserved for training purposes. No part of these documents may be published, distributed, posted on the internet or an intranet, extracted, or reproduced in any form or by any mean, electronic or mechanical, including photocopying, without prior written permission from PECB.	

No.1	*No.1*		To: © Professional Evaluation and Certification Board, 2022. All rights reserved. Version 8.0 Document number: ISMSLID1V8.0 Documents provided to participants are strictly reserved for training purposes. No part of these documents may be published, distributed, posted on the internet or an intranet, extracted, or reproduced in any form or by any mean, electronic or mechanical, including photocopying, without prior written permission from PECB.	

No. 4	*No. 4*	References	Changed from: SO/IEC 27002: 2013, Information technology — Security techniques — Code of practice for information security controls To: ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls	The name of the standard has been changed.

No. 21	*No.* 21	The ISO/IEC 27002 Family	**Changed from:** **ISO/IEC 27002 (previously ISO 17799):** Code of practice for the management of information security (This standard provides objectives and implementation guidelines for the information security controls set out in ISO/IEC 27001, Annex A and it is intended to meet the needs of organizations of all types and sizes. **To:** **ISO/IEC 27002:** Provides generic information security controls and their implementation guidance **Changed from:** **ISO/IEC 27011:** Guidance on the use of ISO/IEC 27002 in the telecommunications industry **To:** **ISO/IEC 27011:** Guidance on the implementation of information security controls in the telecommunications industry	*Notes page*

No. 22	*No. 22*	Development of the ISO/IEC 27000 Family of Standards	**Slide:** The year 2022 has been added to the diagram and the following sentence has been added in the slide: *The ISO/IEC 27002 was revised and its revision will be followed by the release of an amendment for ISO/IEC 27001*. **Notes page:** The following sentence has been added: While ISO/IEC 27001 was last reviewed in 2019, ISO/IEC 27002 was revised in 2022. The release of the new version of ISO/IEC 27002 will be followed by the publication of an amendment of ISO/IEC 27001 with changes in Annex A.	

No. 23	*No. 23*	ISO/IEC 27001	Slide: **Changed from:** Annex A contains 14 clauses, 35 control objectives, and 114 controls. **To:** Annex A contains 4 clauses and 93 information security controls. The following paragraph has been added to **notes page:** “**Important note:** With the release of the new version of ISO/IEC 27002, ISO will publish an amendment to ISO/IEC 27001:2013, providing the updated Annex A based on the information security controls from ISO/IEC 27002:2022. ISO/IEC 27002:2022 introduces a new categorization of information security controls, decreasing the number of controls from 114 to 93 and clauses from 14 to 4. “	

No. 25	*No. 24*	ISO/IEC 27002	Slide: Changed from: • The standard is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. • This standard specifies requirements and provides guidance for a PIMS. • The standard’s requirements (clauses) are written using the imperative verb “shall.” • Organizations can obtain certification against this standard. To: • The standard provides guidance for codes of practice for information security controls (reference document). • Clauses are expressed with the verb “should.” • Organizations cannot obtain certification against this standard. **Notes page:** **Changed from:** **ISO/IEC 27002:** • ISO/IEC 27002 is a guide of information security management controls.	

			• The standard provides a list of security objectives and controls generally practiced in the information security industry. • Clauses 5 to 18, in particular, provide detailed guidance to support the controls specified in Annex A of ISO/IEC 27001 (control groups A.5 to A.18). • ***ISO/IEC 27002, clause 1 Scope*** *This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). This International Standard is designed to be used by organizations that intend to:* a) *select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;* b) *implement commonly accepted information security controls;* c) *develop their own information security management guidelines.* **To:** **ISO/IEC 27002:** • ISO/IEC 27002 provides guidelines for the implementation of information	

			security controls necessary to treat the information security risks of an ISMS based on ISO/IEC 27001. • It provides a list of information security controls generally practiced in the information security industry, their purpose, and implementation guidance. • Clauses 5 to 8, in particular, provide detailed guidance to support the controls specified in Annex A of ISO/IEC 27001, Amendment 1. • **Important note:** Information security controls provided in ISO/IEC 27002:2022 are aligned with Amendment 1 of ISO/IEC 27001 that will be published by ISO in 2022. ***ISO/IEC 27002, clause 1 Scope*** *This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:* a) *within the context of an information security management system (ISMS) based on ISO/IEC 27001;* b) *for implementing information security controls based on internationally recognized best practices;* c) *for developing organization-specific information security management guidelines.*	

No. 31	*No. 31*	Quiz 1	Question 3: Changed from: **Which international standard provides guidelines for codes of practice for information security controls?** A. ISO/IEC 27002 B. ISO/IEC 27003 C. ISO/IEC 27005 **To:** **Which international standard provides a reference set of information security controls?** A. ISO/IEC 27002 B. ISO/IEC 27701 C. ISO/IEC 27005	

No.33	*No. 33*	Section Summary:	**Changed from:** ISO/IEC 27002 is a guideline standard that provides guidance for codes of practice for information security controls. **To:** ISO/IEC 27002 provides guidance for the implementation of information security controls.	
No. 42	*No. 42*	Structure of ISO/IEC 27001	**Changed from:** Annex A Reference control objectives and controls **To:** Annex A Information security controls reference	

No. 50	*No. 50*	Annex A	**Changed from:** • Annex A is part of ISO/IEC 27001 and it is comprised of 114 controls that should be considered when intending to comply with the standard. • The list of control objectives and controls of Annex A is not exhaustive. The organization may add additional controls from other sources, when needed. • If a certain control is not applicable, the organization should provide an acceptable justification for its exclusion. **To:** • Annex A is part of ISO/IEC 27001 and it contains 93 controls that should be considered when intending to comply with the standard. • The list of information security controls of Annex A is not exhaustive. The organization may add additional controls from other sources, when needed. • If a certain control is not applicable, the organization	

			should provide an acceptable justification for its exclusion.	

No. 51	*No.51*	Annex A	**Subtitle:** **Changed from:** Security objectives and controls **To:** Information security controls **Slide:** **Changed from:** ISO/IEC 27001 **To:** ISO/IEC 27001, Amendment 1 **Changed from:** ISO/IEC 27002 **To:** ISO/IEC 27002:2022 **Changed from:** (List of security objectives and controls) **To:** (List of information security controls) **Changed from:** Objectives and controls **To:** Controls and their purpose **Changed from:** Recommendations for implementation **To:** Implementation guidance **Changed from:** **Important note:** Since ISO/IEC 27002 is a code of practice, there is no requirement to follow its guidance in order to obtain an ISO/IEC 27001 certification. **To:**	

			Important note: Since ISO/IEC 27002 is a guideline standard, there is no requirement to follow its recommendations in order to obtain an ISO/IEC 27001 certification. Notes page: The content in notes page has been deleted. Two new paragraphs have been added: Amendment 1 of ISO/IEC 27001 that will be officially published in 2022 provides the updated information security controls of Annex A which are aligned with controls listed in clauses 5 to 8 of ISO/IEC 27002:2022. This training course provides the updated Annex A controls based on the latest version of ISO/IEC 27002 and the draft document of Amendment 1 of ISO/IEC 27001.	
No.52	*No.52*	Framework	The content in the slide has changed completely.	

No.59	*No.59*	Section Summary	**Changed from:** • Annex A is part of ISO/IEC 27001 and it is comprised of 114 controls that should be considered when intending to comply with the standard. • The list of control objectives and controls of Annex A is not exhaustive. **To:** • An organization must comply with requirements set out in clauses 4 to 10 of ISO/IEC 27001 if seeking certification against this standard. • Annex A is part of ISO/IEC 27001 and contains 93 controls that should be considered when intending to comply with the standard.	

No.61	*No.61*	Information and Asset	**Notes page:** **Changed from:** ISO/IEC 27001, Annex A.8 defines the objectives for security controls linked to asset management. *ISO/IEC 27001, Annex A.8.1* *Responsibility for assets* *Objective: To identify organizational assets and define appropriate protection responsibilities.* *ISO/IEC 27001, Annex A.8.1.1 Inventory of assets* *Control: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.* *ISO/IEC 27001, Annex A.8.1.2 Ownership of assets* *Control: Assets maintained in the inventory shall be owned.* *ISO/IEC 27001, Annex A.8.1.3 Acceptable use of assets* *Control: Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.* *ISO/IEC 27001, Annex A.8.1.4 Return of assets*	

			Control: All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. **To:** ISO/IEC 27001, Annex A.5 specifies the security controls linked to asset management. ***ISO/IEC 27001, Annex A.5.9 Inventory of information and other associated assets*** ***Control:*** *An inventory of information and other associated assets, including owners, shall be developed and maintained.* ***ISO/IEC 27001, Annex A.5.10 Acceptable use of information and other associated assets*** ***Control:*** *Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.* ***ISO/IEC 27001, Annex A.5.11 Return of assets*** ***Control:*** *Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.*	

No. 63	*No.63*	Information Security	Changed from: ***ISO/IEC 27002, clause 0.2 Information security requirements*** *It is essential that an organization identifies its security requirements.* *There are three main sources of security requirements:* a) *the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;* b) *the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;* c) *the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.*	

			Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. *ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.* To: ***ISO/IEC 27002, clause 0.2 Information security requirements*** *It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:* a) *the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through*	

			an information security specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria; b) *the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with their sociocultural environment;* c) *the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.*	

No.64	*No.64*	Slide Notes Extension	**Changed from:** Annex A includes control objectives related to the classification of information: ***ISO/IEC 27001, Annex A.8.2 Information classification*** *Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.* ***ISO/IEC 27001, Annex A.8.2.1 Classification of information*** *Control: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.* ***ISO/IEC 27001, Annex A.8.2.2 Labelling of information*** *Control: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.* ***ISO/IEC 27001, Annex A.8.2.3 Handling of assets*** *Control: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.*	

			To: Annex A includes controls related to the classification of information: ***ISO/IEC 27001, Annex A.5.12 Classification of information*** ***Control:*** *Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.* ***ISO/IEC 27001, Annex A.5.13 Labelling of information*** ***Control:*** *An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.*	
No.107	*No.107*	Laws and regulations	The clause has been updated based on the new version of the standard	

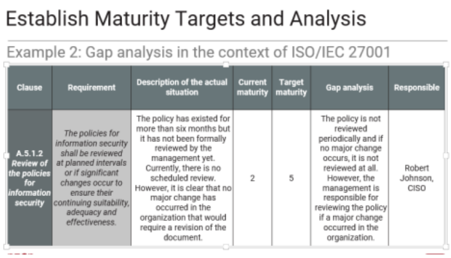
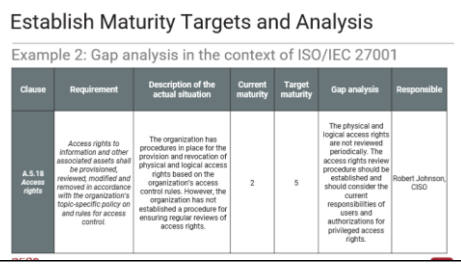
Day 2:				
Slide Number		***Slide Description:***	***Modifications:***	***Comments***
Current version	*Previous version*			

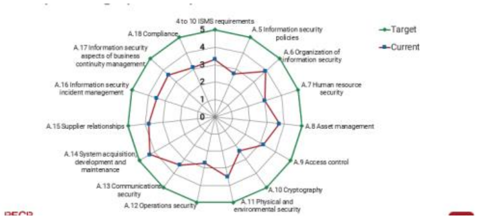
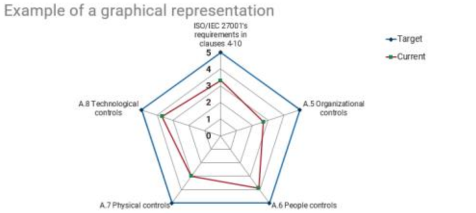
No.1	*No.1*		**Changed from:** © 2021 PECB. All rights reserved. Version 7.2 Document number: ISMSLID2V7.2 Documents provided to participants are strictly reserved for training purposes. No part of these documents may be published, distributed, posted on the internet or an intranet, extracted, or reproduced in any form or by any mean, electronic or mechanical, including photocopying, without prior written permission from PECB. **To:** © Professional Evaluation and Certification Board, 2022. All rights reserved. Version 8.0 Document number: ISMSLID2V8.0 Documents provided to participants are strictly reserved for training purposes. No part of these documents may be published, distributed, posted on the internet or an intranet, extracted, or reproduced in any form or by any mean, electronic or mechanical, including photocopying, without prior written permission from PECB.	

No. 3	*No. 3*	Learning objective of the day	**Changed from:** Acquire knowledge on how to review and select the applicable security objectives and controls and how to draft a Statement of Applicability (SoA) **To:** Acquire knowledge on how to review and select the applicable information security controls and how to draft a Statement of Applicability (SoA)	

<table>
<tr>
<td><em>No.51</em></td>
<td><em>No. 51</em></td>
<td>Establish maturity targets and analysis</td>
<td>Changed from:
<table>
<tr>
<td><strong><em>A.5.1.1 Policies for information security</em></strong></td>
<td><em>A set of policies for information security s
defined, approved
by management, publ
and communicated t
employees and
relevant external part</em></td>
</tr>
</table>
To:</td>
<td></td>
</tr>
</table>

			A.5.1 ***Policies for information security***	*Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.*

<table>
<tr>
<td><em>No. 52</em></td>
<td><em>No. 52</em></td>
<td>Establish Maturity Targets and Analysis</td>
<td>
<p>The content in the slide has been changed completely.</p>
<p><strong>Changed from:</strong></p>

<p>Establish Maturity Targets and Analysis</p>
<p>Example 2: Gap analysis in the context of ISO/IEC 27001</p>
<table>
<tr><th>Clause</th><th>Requirement</th><th>Description of the actual situation</th><th>Current maturity</th><th>Target maturity</th><th>Gap analysis</th><th>Responsible</th></tr>
<tr><td><strong>A.5.1.2</strong> <em>Review of the policies for information security</em></td><td><em>The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.</em></td><td>The policy has existed for more than six months but it has not been formally reviewed by the management yet. Currently, there is no scheduled review. However, it is clear that no major change has occurred in the organization that would require a revision of the document.</td><td>2</td><td>5</td><td>The policy is not reviewed periodically and if no major change occurs, it is not reviewed at all. However, the management is responsible for reviewing the policy if a major change occurred in the organization.</td><td>Robert Johnson, CISO</td></tr>
</table>
<p><strong>To:</strong></p>

<p>Establish Maturity Targets and Analysis</p>
<p>Example 2: Gap analysis in the context of ISO/IEC 27001</p>
<table>
<tr><th>Clause</th><th>Requirement</th><th>Description of the actual situation</th><th>Current maturity</th><th>Target maturity</th><th>Gap analysis</th><th>Responsible</th></tr>
<tr><td><strong>A.5.18</strong> <em>Access rights</em></td><td><em>Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.</em></td><td>The organization has procedures in place for the provision and revocation of physical and logical access rights based on the organization's access control rules. However, the organization has not established a procedure for ensuring regular reviews of access rights.</td><td>2</td><td>5</td><td>The physical and logical access rights are not reviewed periodically. The access rights review procedure should be established and should consider the current responsibilities of users and authorizations for privileged access rights.</td><td>Robert Johnson, CISO</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

No. 54	*No.54*	Publish a Gap Analysis Report	The content in the slide has been changed completely. **Changed from:**  **To :**  Example of a graphical representation 	

No.72	*No.72*	Ensure management approval	Notes page : **Changed from :** *ISO/IEC 27002, clause 5.1.1 Policies for information security* *Implementation guidance* *At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.* **To :** ***ISO/IEC 27002, clause 5.1 Policies for information security*** ***Guidance*** *At the highest level, the organization should define an "information security policy" which is approved by top management and which sets out the organization's approach to managing its information security.*	
No.73	*No.73*	1.7.5 Publish and Disseminate Policies	Notes page : Clause of the standard has been updated.	

No. 82	*No. 82*	ISO/IEC 27001 Requirements	Notes page : The following sentence has been added : **Important note:** Amendment 1 of ISO/IEC 27001 will replace the term “comprehensive list of control objectives and controls” used in clause 6.1.3, *Information security risk treatment*, with “possible information security controls.”	
No. 132	*No.132*	Section 13	**Changed from:** Review and selection of the applicable security objectives and controls **To:** Review and selection of the applicable information security controls	
No. 135	*No. 135*	Statement of Applicability	**Changed from:** “A Statement of Applicability (SoA) is a documented statement listing the control objectives and controls that are relevant” **To:** “A Statement of Applicability (SoA) is a documented statement listing the controls that are relevant”	
No. 136	*No. 136*	Statement of Applicability	Same change as in slide 132.	

No. 137	*No. 137*	Review and select the applicable security objectives and controls	The title of the slide **changed to:** "Review and select the applicable information security controls" The number of controls updated to 93 in both the slide and notes page.	
No. 140	*No. 140*	Justify the selected controls	**Changed from:** **Addressing security within supplier agreements (ISO/IEC 27001, Annex A.15.1.2):** *All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.* To: **Addressing information security within supplier agreements (ISO/IEC 27001, Annex A.5.20):** *Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.* Notes page: Clauses from the standard have been updated.	

No. 141	*No. 141*	Justify the excluded controls	**Changed from:** Annex A.7.1.1 *Screening*. **To:** Annex A.6.1 *Screening* **Changed from**: Annex A.6.2.2 *Teleworking* **To:** Annex A.6.7 *Remote working* Notes page: Clauses from the standard have been updated.	
No.142	*No.142*	Finalize the Statement of Applicability	**Changed from**: ISO/IEC 27001, Annex A.5.1.1 *Policies for information security* **To:** ISO/IEC 27001, Annex A.5.1 *Policies for information security*	
No.143	*No.143*	Finalize the Statement of Applicability (cont'd)	**Changed from:** ISO/IEC 27001 Annex A.5.1.2 *Review of the policies information security* **To:** ISO/IEC 27001 Annex A.5.1 *Policies for information security* **Changed from:** ISO/IEC 27001 Annex A.6.2.2 *Teleworking* **To:** ISO/IEC 27001 Annex A.6.7 *Remote working*	

No.149	*No.149*	Homework (optional)	Homework 4: **Changed from:** control A.9 of ISO/IEC 27001 on access control **To:** control A.5.15 of ISO/IEC 27001 on access control.	

Day 3:				
Slide Number		***Slide Description:***	***Modifications:***	***Comments***
Current Version	*Previous version*			
No. 14	*No. 14*	ISMS Documented Information	Changed from: • Terms and conditions of employment (Control A.7.1.2) • Inventory of assets (Control A.8.1.1) • Acceptable use of assets (Control A.8.1.3) • Access control policy (Control A.9.1.1) • Documented operating procedures (Control A.12.1.1) • Confidentiality or non-disclosure agreements (Control A.13.2.4) • Secure system engineering principles (Control A.14.2.5) • Information security policy for supplier relationships (Control A.15.1.1)	

			• Response to information security incidents (Control A.16.1.5) • Implementing information security continuity (Control A.17.1.2) • Identification of applicable legislation and contractual requirements (Control A.18.1.1) To: • Terms and conditions of employment (Control A.6.2) • Inventory of information and other associated assets (Control A.5.9) • Acceptable use of information and other associated assets (Control A.5.10) • Access control (Control A.5.15) • Documented operating procedures (Control A.5.37) • Confidentiality or non-disclosure agreements (Control A.6.6) • Secure system architecture and engineering principles (Control A.8.27) • Information security in supplier relationships (Control A.5.19) • Response to information security incidents (Control A.5.26) • Information security during disruption (Control A.5.29) • Legal, statutory, regulatory and contractual requirements(Control A.5.31)	

			Notes page: Changed from: • Mobile devices and teleworking (Control A.6.2) • Information classification (Control A.8.2) • User access management (Control A.9.2) • Disposal of media (Control A.8.3.2) • Secure disposal or re-use of equipment (Control A.11.2.7) • Working in secure areas (Control A.11.1.5) • Clear desk and clear screen policy (Control A.11.2.9) • Change management (Control A.12.1.2) • Restrictions on changes to software packages (Control A.14.2.4) • Information backup (Control A.12.3.1) • Information transfer (Control A.13.2) • Information security continuity (Control A.17.1) • Redundancies (Control 17.2) To: • Remote working (Control A.6.7) • Classification of information (Control A.5.12) • Access rights (Control A.5.18) • Storage media (Control A.7.10)	

			- Secure disposal or re-use of equipment (Control A.7.14) - Working in secure areas (Control A.7.6) - Clear desk and clear screen (Control A.7.7) - Change management (Control A.8.32) - Information backup (Control A.8.13) - Information transfer (Control A.5.14) - Redundancy of information processing facilities (Control A.8.14)	
No. 49-75	*No. 49-68*	Section 16	These slides have been changed completely.	
No. 76	*No. 69*	Exercise 3	**Changed from:** **Exercise 3: Security controls** Provide an action plan constituting at least two actions to be taken to ensure conformity to the following clauses and controls of ISO/IEC 27001. ***Example: Annex 11.2.3 Cabling security*** • *Use shielded network cabling conduit to isolate and protect power and telecommunications cabling from interception* • *Document the authorized cabling material to avoid the usage of low quality material* 1. Clause 7.2 a) Determine the necessary competence of person(s) doing work under its control that affects its	

			information security performance 2. Clause 10.1 a) React to the nonconformity 3. Annex 12.1.3 Capacity management 4. Annex 12.2.1 Controls against malware 5. Annex 13.2.3 Electronic messaging Duration of the exercise: 30 minutes Comments: 15 minutes **To:** **Exercise 3: Security controls** Provide an action plan constituting at least two actions to be taken to ensure conformity to the following clauses and controls of ISO/IEC 27001. ***Example: Control A.7.12 Cabling security*** • *Use shielded network cabling conduit to isolate and protect power and telecommunications cabling from interception* • *Document the authorized cabling material to avoid the usage of low quality material* 1. Clause 7.2 a) Determine the necessary competence of person(s) doing work under its control that affects its information security performance 2. Clause 10.1 a) React to the nonconformity	

			3. Control A.8.6 Capacity management 4. Control A.8.7 Protection against malware 5. Control A.5.14 Information transfer	
No.77		Quiz 16	All questions of quiz 16 have been updated so they can be aligned with changes made in the training course.	
No. 155	*No. 148*		Changed from: ISO/IEC 27002, clause 16.1.7 • *Internal procedures should be developed and followed when dealing with evidence for the purposes of disciplinary and legal action.* • *In general, these procedures for evidence should provide processes of identification, collection, acquisition and preservation of evidence in accordance with different types of media, devices and status of devices, e.g. powered on or off.* To: ISO/IEC 27002, clause 5.28 • *Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of*	

			admission across the relevant jurisdictions. • *In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off).*	
No.165	*No.158*	Homework (optional)	**Changed from:** **Homework 8: Master list of documented information** The top management of e-Scooter has decided to implement all the information security controls on business continuity management (ISO/IEC 27001, Annex 17). Propose a list of documented information that should be generated to ensure conformity to the information security controls of Annex 17. **To:** **Homework 8: Master list of documented information** The top management of e-Scooter has decided to implement all the information security controls on business continuity management (ISO/IEC 27001, Annex A.5). Propose a list of documented information that should be generated to ensure conformity to the information security control A.5.29.	

Day 4:				
Slide Number		***Slide Description:***	***Modifications:***	***Comments***
Current Version	*Previous version*			
No. 46	*No. 46*	Nonconformity report	**Changed from :** clause number: A.8.1.1 **To :** Clause number: A.5.9 **Changed from :** Audit criteria: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. **To** : Audit criteria: An inventory of information and other assets, including owners, shall be developed and maintained.	
No. 142	*No. 142*	Homework (optional)	**Changed from :** Homework 11: Development of information security indicators Provide at least two examples of metrics that would be sufficient to measure the level of conformity to the following clauses and controls of ISO/IEC 27001. *Example: Clause 5.1 Leadership and commitment*	

			• *The number of management review meetings completed to date* • *The average participation rate in management review meetings to date* 1. Clause 10.1 d) Review the effectiveness of any corrective action taken 2. Clause 5.3 Organizational roles, responsibilities and authorities 3. Control A.8.1.2 Ownership of assets 4. Control A.8.1.4 Return of assets 5. Control A.9.3.1 Use of secret authentication information **To :** Homework 11: Development of information security indicators Provide at least two examples of metrics that would be sufficient to measure the level of conformity to the following clauses and controls of ISO/IEC 27001. *Example: Clause 5.1 Leadership and commitment* • *The number of management review meetings completed to date* • *The average participation rate in management review meetings to date* 1. Clause 10.1 d) Review the effectiveness of any corrective action taken	

			2. Clause 5.3 Organizational roles, responsibilities and authorities 3. Control A.5.9 Inventory of information and other associated assets 4. Control A.5.11 Return of assets 5. Control A.5.17 Authentication information	
No.	*No.*			
No.	*No.*			

Other Materials	***Task***	***Description***	***Comments***	***Completed***
Case Study	*Update the case study*	*Case study should be aligned with the new version of the course*		☒
Exercises	*Update the exercises*	*Exercises should be aligned with the new version of the course*		☒
Correction Keys	*Update the correction keys*	*Correction keys should be aligned with the new version of the course*		☒
Exam 01	*Update the exam*	*The exam should be aligned with the new version of the course*		☒
Exam 02	*Update the exam*	*The exam should be aligned with the new version of the course*		☒
Candidate Handbook (CH)	*Update CH*	*The CH should be aligned with the new version of the course*		☒
Course Description	*Update Course Description on the web*	*The CD should be aligned with the new version of the course*		☒
Other Supporting Materials (Ex. Videos, Samples)	*Update other supporting materials of the course*	*Other supporting materials should be aligned with the new version of the course*		□

Comments:

NOTE: This part is for internal purposes only.

Revision history

Version	Change description	Date
1.0	Initial release	n/a
1.4	Branding and logo update	2020-02-10
1.5	Font changed to Roboto. Minor technical modifications. Name of the form changed from “Change Log” to “Training Course Change Log” Removed EPG from the list of “Other Materials”	2021-02-01