# 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**** | *2022-02-25* | | | |
| ***Course details**** | ***Course name:*** | ***Language:*** | ***New Version:*** | ***Previous Version:*** |
| | *ISO/IEC 27001 Lead Auditor* | *English* | *12.0* | *11.2* |

***Summary of the Change:***

*The training course has been updated based on ISO/IEC 27002:2022 and ISO/IEC 27001 Draft Amendment 1.*

***Day 1:***

| ***Slide Number*** | | ***Slide Description:*** | ***Modifications:*** | ***Comments*** |
|---|---|---|---|---|
| *Current version* | *Previous version* | | | |

| | | | | |
|---|---|---|---|---|
| *No.1* | *No.1* | Certified ISO/IEC 27001 Lead Auditor | Changed from:<br><br>© Professional Evaluation and Certification Board, 2021. All rights reserved.<br><br>Version 11.2<br><br>Document number: ISMSLAD1V11.2<br><br>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.<br><br>To:<br><br>© Professional Evaluation and Certification Board, 2022. All rights reserved.<br><br>Version 12.0<br><br>Document number: ISMSLAD1V12.0<br><br>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:<br><br>**ISO/IEC 27002:2013**<br>Information technology — Security techniques — Code of practice for information security controls<br><br>To:<br><br>**ISO/IEC 27002:2022**<br>Information security, cybersecurity and privacy protection – Information security controls | |

| | | | | |
|---|---|---|---|---|
| *No.6* | *No.6* | Note on Terminology Used ** | **Changed from:**<br>***ISO/IEC 27001, Annex A.18.1.3***<br>***Protection of records***<br>*Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.*<br><br>**To: *ISO/IEC 27001, Annex A.5.33***<br>***Protection of records***<br>***Control***<br>*Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.* | |

| | | | | |
|---|---|---|---|---|
| *No. 21* | *No. 21* | The ISO/IEC 27000 Family of Standards | Changed from:<br>**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.)<br><br>To:<br>**ISO/IEC 27002:** Provides generic information security controls and their implementation guidance.<br><br>**Changed from:**<br>**ISO/IEC 27011:** Guidance on the use of ISO/IEC 27002 in the telecommunications industry<br><br>**To:**<br>**ISO/IEC 27011:** Guidance on the implementation of information security controls in the telecommunications industry | |

| | | | | |
|---|---|---|---|---|
| *No. 22* | *No. 22* | The Development of ISO/IEC 27000 Family of Standards | Year 2022 should be added to the slide. In addition, the following sentence should be added in the slide:<br>"The ISO/IEC 27002 was revised and its revision will be followed by the release of an amendment for ISO/IEC 27001."<br><br>**Notes page:**<br>Added:<br><br>• 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:**<br>**Changed to:** Annex A contains 4 clauses and 93 information security controls.<br><br>**Notes page:**<br>The following paragraph has been added:<br><br>**Important note:** With the release of the new version of the ISO/IEC 27002 standard, 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. This training course provides the updated controls of Annex A based on the latest version of ISO/IEC 27002. The list of the updated Annex A controls will be officially published in 2022. | |

| | | | | |
|---|---|---|---|---|
| *No. 26* | *No. 25* | ISO/IEC 27002 | **Changed from:**<br>• The standard provides guidance for codes of practice for information security controls (reference document).<br>• Clauses are expressed with the verb "should."<br>• Organizations cannot obtain certification against this standard.<br><br>**To:**<br>• The standard provides a list of generic information security controls and their implementation guidance.<br>• Clauses are expressed with the verb "should."<br>• Organizations cannot obtain certification against this standard.<br><br>Notes page:<br><br>Changed from: **ISO/IEC 27002:**<br>• ISO/IEC 27002 is a guide of information security management controls.<br>• The standard provides a list of security objectives and controls generally practiced in the information security industry.<br>• 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).<br><br>***ISO/IEC 27002, clause 1 Scope***<br><br>*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).*<br><br>*This International Standard is designed to be used by organizations that intend to:*<br><br>a) *select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;*<br>b) *implement commonly accepted information security controls;*<br>c) *develop their own information security management guidelines.*<br><br>To:<br><br>**ISO/IEC 27002:**<br><br>• 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.<br>• It provides a list of information security controls generally practiced in the information security industry, their purpose, and implementation guidance.<br>• Clauses 5 to 8, in particular, provide detailed guidance to support the controls specified in Annex A of ISO/IEC 27001, Amendment 1.<br><br>**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.<br><br>***ISO/IEC 27002, clause 1 Scope***<br><br>*This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:*<br><br>a) *within the context of an information security management system (ISMS) based on ISO/IEC 27001;*<br>b) *for implementing information security controls based on* | |

| | | | | |
|---|---|---|---|---|
| | | | *internationally recognized best practices;*<br>c) *for developing organization-specific information security management guidelines.* | |
| *No. 30* | *No. 30* | Legal and Regulatory Conformity | Notes page:<br>Clause of ISO/IEC 27002 has been updated. | |
| *No. 35* | *No. 34* | Section Summary | **Changed from:**<br>ISO/IEC 27002 is a standard guideline of information security management best practices.<br>**To:**<br>ISO/IEC 27002 provides guidance for the implementation of information security controls. | |
| *No. 38* | *No. 38* | Certification Scheme | “baodies” changed to “bodies”. | |

| | | | | |
|---|---|---|---|---|
| *No. 46* | *No. 45* | Information and Asset | **Changed from:**<br>ISO/IEC 27001, Annex A.8 defines the objectives for the security controls linked to the management of assets.<br>*ISO/IEC 27001, Annex A.8.1*<br>*Responsibility for assets*<br>*Objective: To identify organizational assets and define appropriate protection responsibilities.*<br>*ISO/IEC 27001, Annex A.8.1.1 Inventory of assets*<br>*Control*<br>*Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.*<br>*ISO/IEC 27001, Annex A.8.1.2 Ownership of assets*<br>*Control*<br>*Assets maintained in the inventory shall be owned.*<br>*ISO/IEC 27001, Annex A.8.1.3 Acceptable use of assets*<br>*Control*<br>*Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.*<br>*ISO/IEC 27001, Annex A.8.1.4 Return of assets* | |

| | | | | |
|---|---|---|---|---|
| | | | *Control*<br>*All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.*<br><br>**To:**<br>ISO/IEC 27001, Annex A.5 specifies the security controls linked to asset management.<br>*ISO/IEC 27001, Annex A.5.9 Inventory of information and other associated assets*<br>*Control*<br>*An inventory of information and other associated assets, including owners, shall be developed and maintained.*<br>*ISO/IEC 27001, Annex A.5.10 Acceptable use of information and other associated assets*<br>*Control*<br>*Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.*<br>*ISO/IEC 27001, Annex A.5.11 Return of assets*<br>*Control*<br>*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. 48* | *No. 47* | Information Security | Clause 0.2 has been updated in notes page. | |

| | | | | |
|---|---|---|---|---|
| *No.49* | *No.48* | Slide Notes Extension** | **Changed from:**<br>**A**nnex A includes control objectives related to the classification of information:<br>*ISO/IEC 27001, Annex A.8.2 Information classification*<br>*Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.*<br>*ISO/IEC 27001, Annex A.8.2.1 Classification of information*<br>*Control*<br>*Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.*<br>*ISO/IEC 27001, Annex A.8.2.2 Labelling of information*<br>*Control*<br>*An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.*<br>*ISO/IEC 27001, Annex A.8.2.3 Handling of assets*<br>*Control*<br>*Procedures for handling assets shall be developed and implemented in accordance with the information* | |

| | | | | |
|---|---|---|---|---|
| | | | *classification scheme adopted by the organization.*<br><br>**To:**<br>Annex A includes controls related to the classification of information:<br>*ISO/IEC 27001, Annex A.5.12 Classification of information*<br>*Control*<br>*Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.*<br>*ISO/IEC 27001, Annex A.5.13 Labelling of information*<br>*Control*<br>*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. 72* | *No.71* | Strategic, General, and Specific Controls | Changed from:<br>**Control of system development**<br><br>To:<br>**Control of development life cycle**<br><br>Changed from:<br>**Asset management**<br><br>To:<br>**Acceptable use of assets** | |
| *No. 87* | *No. 86* | The Structure of ISO/IEC 27001 | Changed from:<br>**Annex A** Information security controls reference<br><br>To:<br>**Annex A** Information security controls reference | |

| | | | | |
|---|---|---|---|---|
| *No. 103* | *No.102* | Select Controls | **Slide:**<br>**Changed to:**<br>Annex A is part of ISO/IEC 27001. Annex A of Amendment 1 of ISO/IEC 27001 comprises 93 controls that should be considered when aiming to comply with the standard.<br><br>**Changed from:**<br>The list of control objectives and controls of Annex A<br>**To:**<br>The list of Annex A controls<br><br>**Notes page:**<br>The following paragraphs have been added:<br><br>Annex A of Amendment 1 of ISO/IEC 27001 provides the information security controls aligned with ISO/IEC 27002. ISO/IEC 27002:2022 introduces 11 new controls while 24 controls have been merged with existing controls and 58 controls have been updated.<br>Annex B of ISO/IEC 27002 provides a mapping of ISO/IEC 27002:2013 and ISO/IEC 27002:2022 controls.<br>**Important note:** Since ISO/IEC 27002 controls are aligned with Annex A controls specified in ISO/IEC 27001, the controls from Annex A used in this training course have been updated based on ISO/IEC 27002:2022. This list of the updated Annex A controls of | |

| | | | | |
|---|---|---|---|---|
| | | | ISO/IEC 27001 will be officially published in 2022. | |
| *No. 104* | *No.103* | Information security controls | New slide. | |
| *No. 106* | *No. 105* | Applicable Security Objectives and Security Controls | **Changed from:**<br>ISO/IEC 27001's 114 security controls<br>**To:**<br>ISO/IEC 27001's 93 security controls | |

| | | | | |
|---|---|---|---|---|
| *No.107* | *No. 106* | Justification of the Selected Controls | **Changed from:** Addressing security within supplier agreements (ISO/IEC 27001, 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.*<br><br>**To:** Addressing information security within supplier agreements (ISO/IEC 27001, A.5.20): *Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.*<br><br>**Notes page:**<br>**Changed from:** *ISO/IEC 27001, Annex A.12.1.2 Change management Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.* Justification of the selection: Ensuring the confidentiality, integrity, and availability of information and the means of processing information belonging to the organization when there are changes to systems and methods of information processing<br><br>*ISO/IEC 27001, Annex A.17.1.2 Implementing information security continuity* | |

| | | | | |
|---|---|---|---|---|
| | | | *The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.*<br>Justification of the selection: Ensuring availability of information on time when an interruption or outage affects critical business processes<br><br>**To:**<br>*ISO/IEC 27001, Annex A.5.29 Information security during disruption*<br>*The organization shall plan how to maintain information security at an appropriate level during disruption.*<br>Justification of the selection: Ensuring the availability of information in a timely manner when an interruption or power outage affects critical business processes<br>*ISO/IEC 27001, Annex A.8.32 Change management*<br>*Changes to information processing facilities and information systems shall be subject to change management procedures.*<br>Justification of the selection: Ensuring the confidentiality, integrity, and availability of information and means of processing information belonging to the organization when there are changes to systems and information processing methods | |

| | | | | |
|---|---|---|---|---|
| *No. 109* | *No.108* | Statement of Applicability | **Changed from**: A.5.1.1. Policies for information security<br><br>**To:** A.5.1 Policies for information security | |
| *No. 110* | *No.109* | Statement of Applicability | The controls from Annex A have been updated (first columns).<br><br>In addition the following sentence has been **changed from:**<br>Our organization has no activities related to teleworking.<br><br>**To:**<br>Our organization has no activities related to remote working. | |

| | | | | |
|---|---|---|---|---|
| *No. 133* | *No. 132* | Homework (optional) | **Changed from:**<br>Homework 3: Information security controls<br>Determine how you would verify the organization's conformity to the following controls of Annex A of ISO/IEC 27001. State at least two actions that you would take to verify that the organization conforms to each control.<br>1. Policies for information security (Annex A.5.1.1)<br>2. Removal or adjustment of access rights (Annex A.9.2.6)<br>3. Controls against malware (Annex A.12.2.1)<br>4. Review of user access rights (Annex A.9.2.5)<br><br>**To:**<br>Homework 3: Information security controls<br>Determine how you would verify the organization's conformity to the following controls of Annex A of ISO/IEC 27001. State at least two actions that you would take to verify that the organization conforms to each control.<br>1. Policies for information security (Annex A.5.1)<br>2. Access rights (Annex A.5.18)<br>3. Protection against malware (Annex A.8.7)<br>4. Information backup (Annex A.8.13) | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |

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

| | | | | |
|---|---|---|---|---|
| *No. 1* | *No.1* | Certified ISO/IEC 27001 Lead Auditor | Changed from:<br>© Professional Evaluation and Certification Board, 2021. All rights reserved.<br>Version 11.2<br>Document number: ISMSLAD2V11.2<br>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.<br><br>To:<br>© Professional Evaluation and Certification Board, 2022. All rights reserved.<br>Version 12.0<br>Document number: ISMSLAD2V12.0<br>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.70* | *No.70* | Quiz 6 | Question 6 has been changed. | |

| | | | | |
|---|---|---|---|---|
| *No. 76* | *No. 76* | 1. Physical Evidence | **Changed from:**<br>**ISO/IEC 27001, Annex A.8.1.1 Inventory of assets:** Documented auditor observations and inspection notes of the asset inventory<br>**ISO/IEC 27001, Annex A.11.1.2 Physical entry controls:** Documented auditor observations of the physical entry controls<br><br>**To:**<br>**ISO/IEC 27001, Annex A.5.9 Inventory of information and other associated assets:** Documented auditor observations and inspection notes of the asset inventory<br>**ISO/IEC 27001, Annex A.7.2 Physical entry:** Documented auditor observations of the physical entry controls | |

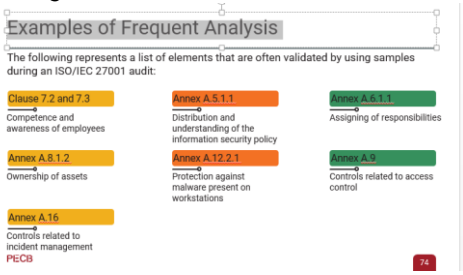
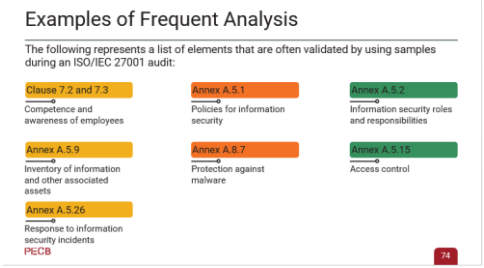
| | | | | |
|---|---|---|---|---|
| *No. 77* | *No. 77* | 2. Mathematical Evidence | **Changed from:**<br>**ISO/IEC 27001, Annex A.7.2.2 Information security awareness, education and training:** Calculate the number of training hours (related to the ISMS) received by employees and confirm whether this meets the objectives<br>**ISO/IEC 27001, Annex A.16.1.6 Learning from information security incidents:** Calculate the average resolution time of information security incidents from a sample taken by the auditor<br><br>**To:**<br>**ISO/IEC 27001, Annex A.6.3 Information security awareness, education and training:** Calculate the number of training hours (related to the ISMS) received by employees and confirm whether this meets the objectives<br>**ISO/IEC 27001, Annex A.5.27 Learning from information security incidents:** Calculate the average resolution time of information security incidents from a sample taken by the auditor | |

| | | | | |
|---|---|---|---|---|
| *No. 78* | *No. 78* | 3. Confirmative Evidence | Changed from:<br>**ISO/IEC 27001, Annex A.13.1.3 Segregation in networks:** Report from an external consultant showing that the information services, users, and information system groups are segregated on the network<br>**ISO/IEC 27001, Annex A.18.1.1 Identification of applicable legislation and contractual requirements:** Letter from an attorney external to the organization that confirms the various legislations to which the organization must comply to<br><br>To:<br>**ISO/IEC 27001, Annex A.8.22 Segregation of networks:** Report from an external consultant showing that the information services, users, and information system groups are segregated on the network<br>**ISO/IEC 27001, Annex A.5.31 Legal, statutory, regulatory and contractual requirements:** Letter from an attorney external to the organization that confirms the various legislations to which the organization must comply to | |

| | | | | |
|---|---|---|---|---|
| *No. 79* | *No. 79* | 4. Technical Evidence | **Changed from:**<br>• ISO/IEC 27001, Annex A.13.1.2 Security of network services: The auditor's observation notes on the configuration of firewalls in place to ensure the security of the connection to network services in accordance with policies and procedures on the security of network connections of the audited organization<br>• ISO/IEC 27001, Annex A.14.1.3 Protecting application services transactions: Result of transaction simulation tests in a payroll system to validate if the deductions are calculated in conformity with the financial policies of the organization<br><br>**To:**<br>**ISO/IEC 27001, Annex A.8.21 Security of network services:** The auditor's observation notes on the configuration of firewalls in place to ensure the security of the connection to network services in accordance with policies and procedures on the security of network connections of the audited organization<br>**ISO/IEC 27001, Annex A.8.26 Application security requirements:** Result of transaction simulation tests in a payroll system to validate if the deductions are calculated in conformity with the financial policies of the organization | |

| | | | | |
|---|---|---|---|---|
| *No. 80* | *No.80* | 5. Analytical Evidence | **Changed from:**<br>• ISO/IEC 27001, Annex A.9.2.6 Removal or adjustment of access rights: Analysis of the results of the access rights removal procedure on a sample of users having left the organization<br>• ISO/IEC 27001, Annex A.16.1.2 Reporting information security events: Analysis of the results of a sample of event tickets related to information security incidents<br><br>**To:**<br>• ISO/IEC 27001, Annex A.5.18 Access rights: Analysis of the results of the access rights removal procedure on a sample of users having left the organization<br>• ISO/IEC 27001, Annex A.6.8 Information security event reporting: Analysis of the results of a sample of event tickets related to information security incidents | |
| *No. 81* | *No. 81* | 6. Documentary Evidence | **Changed from:**<br>Annex A.13.2.4 Confidentiality or nondisclosure agreements<br>**To:**<br>Annex A.6.6 Confidentiality or non-disclosure agreements<br><br>**Changed from:**<br>Annex A.12.3.1 Information backup<br>**To:**<br>Annex A.8.13 Information backup | |

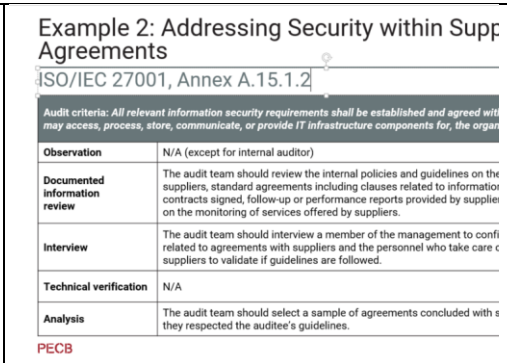
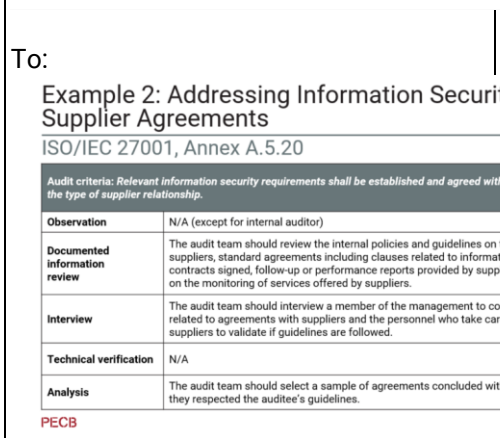
| | | | | |
|---|---|---|---|---|
| *No. 82* | *No. 82* | 7. Verbal Evidence | **Changed from:**<br>Annex A.6.1.1<br>**To:**<br>Annex A.5.2<br><br>**Changed from:**<br>A.6.1.4<br>**To:**<br>Annex A.5.6 | |
| *No. 85* | *No. 85* | Reliability of Audit Evidence | Notes page:<br><br>**Changed from** "Annex A 12.2" **to** "Annex A.8.7 *Protection against malware* | |
| *No.86* | *No.86* | Quiz 7 | **Question 4:**<br>**Changed from:** A.9.2.6 Removal or adjustment of access rights<br><br>**To:** A.5.18 A*ccess rights* | |
| *No. 139* | *No. 139* | Requirements on Documented Information | Notes page:<br>**Changed from:** 114 controls **to:** 93 controls | |
| *No. 140* | *No. 140* | Slide Notes Extension** | **Notes page:**<br><br>**Changed from:**<br>Logs of user activities, exceptions, and security events (Annex A.8.15)<br><br>**To:**<br>Logging (Annex A.8.15) | |
| *No.151* | *No.151* | Scenario-based<br>Quiz 2 | **Changed from:**<br>Annex A 5.1.1 *Policies for information security*<br><br>**To**<br>Annex A.5.1 *Policies for information security* | |

| ***Day 3:*** | | | | |
|---|---|---|---|---|
| ***Slide Number*** | | ***Slide Description:*** | ***Modifications:*** | ***Comments*** |
| *Current Version* | *Previous version* | | | |
| *No. 74* | *No. 74* | Examples of Frequent Analysis | Changed from:<br>  <br>To:<br>  <br>Notes page:<br><br>Changed from:<br>Examples of frequent analysis done during an ISO/IEC 27001 audit include:<br>• **Clause 7.2 and 7.3 Competence and awareness of employees:** | |

| | | | | |
|---|---|---|---|---|
| | | | Verifying a sample of employees to determine if they have been adequately trained and made aware of their role within the information security management system<br>• **Annex A.5.1.1 Distribution and understanding of the information security policy:** Verifying a sample of employees to determine if they have received and are made aware of the information security policy<br>• **Annex A.6.1.1 Assignment of responsibilities:** Verifying a sample of employees to determine if they know their roles and responsibilities related to the information security management system<br>• **Annex A.8.1.2 Ownership of assets:** Verifying a sample of asset owners to determine if they are aware of their responsibility and the asset(s) under their custody<br>• **Annex A.12.2.1 Protection against malware present on workstations:** Verifying a sample of computers to check for the presence of installed and properly-configured software that protect against malicious codes<br>• **Annex A.9 Controls related to access control:** Verifying a | |

| | | | | |
|---|---|---|---|---|
| | | | sample of requests for access rights to validate if the requests comply with the procedures in place<br>• **Annex A.16 Controls related to incident management:** Verifying a sample of incident reports to validate if their treatment complies with the incident management procedure<br>**To:**<br>Examples of frequent analysis done during an ISO/IEC 27001 audit include:<br>• **Clause 7.2 and 7.3 Competence and awareness of employees:** Verifying a sample of employees to determine if they have been adequately trained and made aware of their role within the information security management system<br>• **Annex A.5.1 Policies for information security:** Verifying a sample of employees to determine if they are aware of the policies for information security<br>• **Annex A.5.2 Information security roles and responsibilities:** Verifying a sample of employees to determine whether employees are aware of their roles and responsibilities related to information security<br>• **Annex A.5.9 Inventory of information and other** | |

| | | | | |
|---|---|---|---|---|
| | | | **associated assets:** Verifying a sample of asset owners to determine if they are aware of their responsibility and the asset(s) under their custody<br>• **Annex A.8.7 Protection against malware:** Verifying a sample of computers to check for the presence of installed and properly-configured software that protect against malicious codes<br>• **Annex A.5.15 Access control:** Verifying a sample of requests for access rights to validate if the requests comply with the procedures in place<br>• **Annex A.5.26 Response to information security incidents:** Verifying a sample of incident reports to validate if their treatment complies with the incident management procedure | |
| *No. 101* | *No. 101* | Example 2: Addressing Information Security within Supplier Agreements | Changed from: | |

| | | | | |
|---|---|---|---|---|
| | | |  <br>To:<br>  |
| *No. 102* | *No. 102* | Example 3: Information Backup | Subtitle: Changed to A.8.13<br><br>Audit criteria has been updated based on 27001 Amendment 1. | |
| *No. 103* | *No. 103* | Example 4: User registration and de-registration | Control A.9.2.1 has been changed to A.5.16.<br><br>In addition, the text in the slide has been changed. | |
| *No. 104* | *No. 104* | Example 5: Management of Technical Vulnerabilities | The subtitle has been updated. | |

| | | | | |
|---|---|---|---|---|
| | | | The audit criteria has been updated based on 27001 Amendment 1. | |
| *No. 105* | *No. 105* | Example 6: Information Security Event Reporting | Title: Updated the name of the control Subtitle: Number of control has been changed.<br><br>Slide: Audit criteria has been updated. | |

| ***Day 4:*** | | | | |
|---|---|---|---|---|
| ***Slide Number*** | | ***Slide Description:*** | ***Modifications:*** | ***Comments*** |
| *Current Version* | *Previous version* | | | |
| *No. 9* | *No. 9* | Minor Nonconformity | Notes page:<br>Audit criteria and the control number from Annex A have been updated in the first example. | |
| *No. 11* | *No. 11* | Major Nonconformity | The text has been changed from:<br>1. **Description of the detected nonconformity:** The internal users of the organization are not all aware of the security risks related to the use of mobile computing, and there is no formal procedure in place to ensure the protection of mobile communication devices (Blackberry and iPhone). In a sample of 25 mobile communication devices (15 Blackberry and 10 iPhone), only 5 devices had an activated authentication mechanism.<br>Audit criteria: *A policy and supporting security measures shall* | |

| | | | | |
|---|---|---|---|---|
| | | | *be adopted to manage the risks introduced by using mobile devices (ISO/IEC 27001, Annex A.6.2.1)*<br><br>To:<br>1. **Description of the detected nonconformity:** The internal users of the organization are not all aware of the security risks related to the use of user endpoint devices, and there is no formal procedure in place to ensure the protection of mobile communication devices (Blackberry and iPhone). In a sample of 25 mobile communication devices (15 Blackberry and 10 iPhone), only 5 devices had an activated authentication mechanism.<br>Audit criteria: *Information stored on, processed by or accessible via user endpoint devices shall be protected (ISO/IEC 27001, Annex A.8.1)* | |
| *No. 17* | *No. 17* | Drafting a Nonconformity Report | Changed from: **Clause number:** A.8.1.1<br><br>To: **Clause number** A.5.9<br><br>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.*<br>To: **Audit criteria:** *An inventory of information and other associated assets,* | |

| | | | | |
|---|---|---|---|---|
| | | | *including owners, shall be developed and maintained.* | |
| *No. 25* | *No. 25* | Work Document — Example 1 | The number and the name of the clause has been updated. | |
| *No. 26* | *No. 26* | Work Document — Example 2 | The control number and description have been changed. | |
| *No. 32* | *No. 32* | Document the Quality Review | Changed from : **G**<br>To :**7.5.2 Creating and updating**<br><br>Changed from : **A.11.1.2 Physical entry controls**<br>To : **A.7.2 Physical entry**<br><br>Changed from : **A.12.1.2 Change management**<br><br>To: **A.8.32 Change management** | |
| *No.61* | *No.61* | Action Plans | Changed from :<br>**Process:** Information security aspects of business continuity management<br>**Clause number:** A.17.1<br><br>To :<br>**Process:** Information security during disruption<br>**Clause number:** A.5.29 | |
| | | | | |
| | | | | |

| ***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: All supporting materials have been updated to reflect the changes made in the training course.*

**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.<br>Minor technical modifications.<br>Name of the form changed from “Change Log” to “Training Course Change Log”<br>Removed EPG from the list of “Other Materials” | 2021-02-01 |