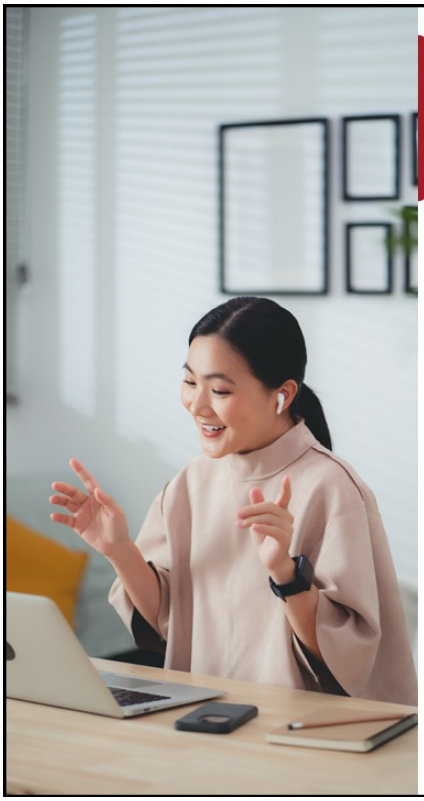
Day 2

ISO/IEC 27001:2022 Foundation

Accredited by ANAB

Version 7.0

Document number: ISMSFDD2V7.0

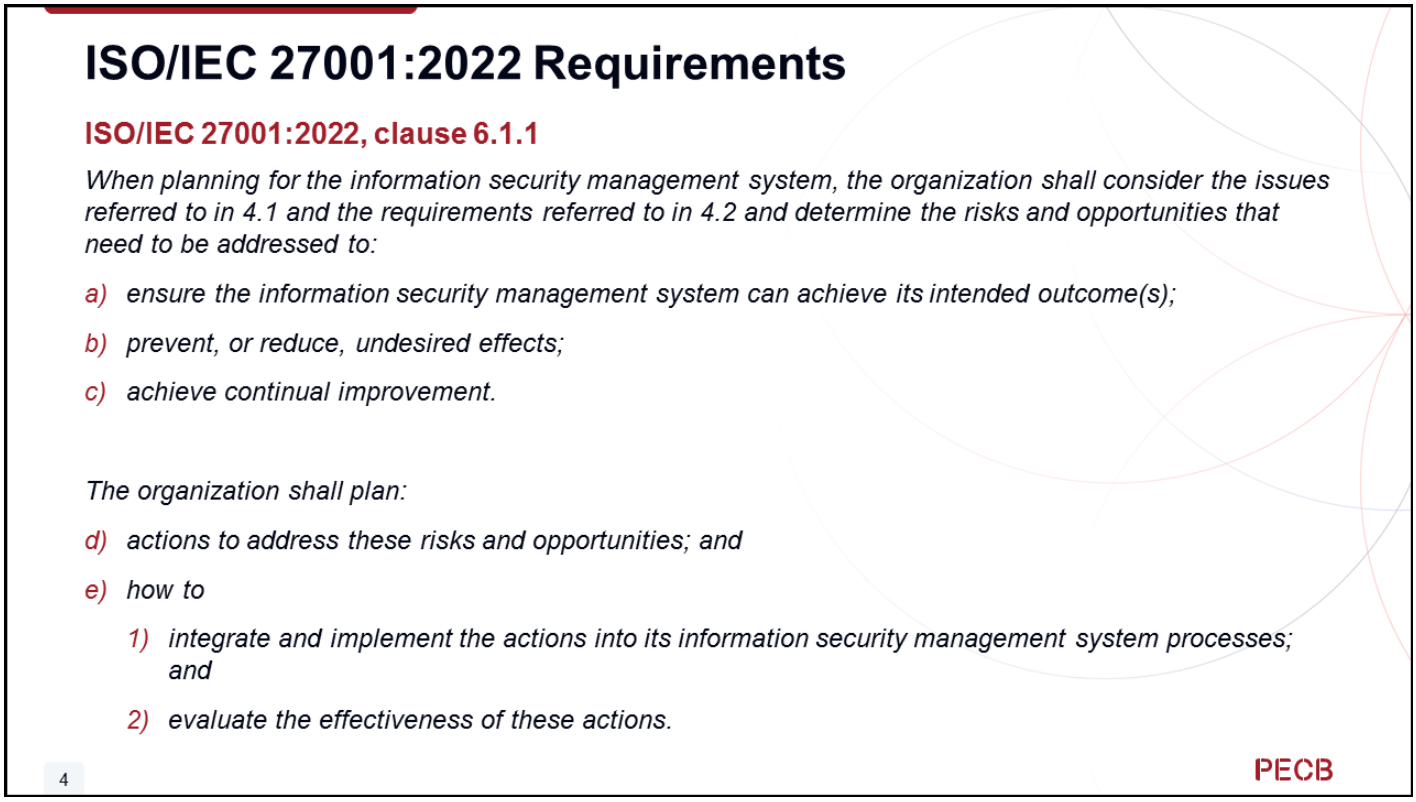


Day 2 Agenda

Section 7	Planning
Section 8	Support
Section 9	Operation
Section 10	Performance evaluation
Section 11	Improvement
Section 12	Information security controls
Section 13	Closing of the training course

PECB

This section provides information that will help the participant gain knowledge on the risk management process, including risk identification, risk estimation, risk evaluation, and risk treatment.



An organization wishing to comply with ISO/IEC 27001:2022 shall at least:

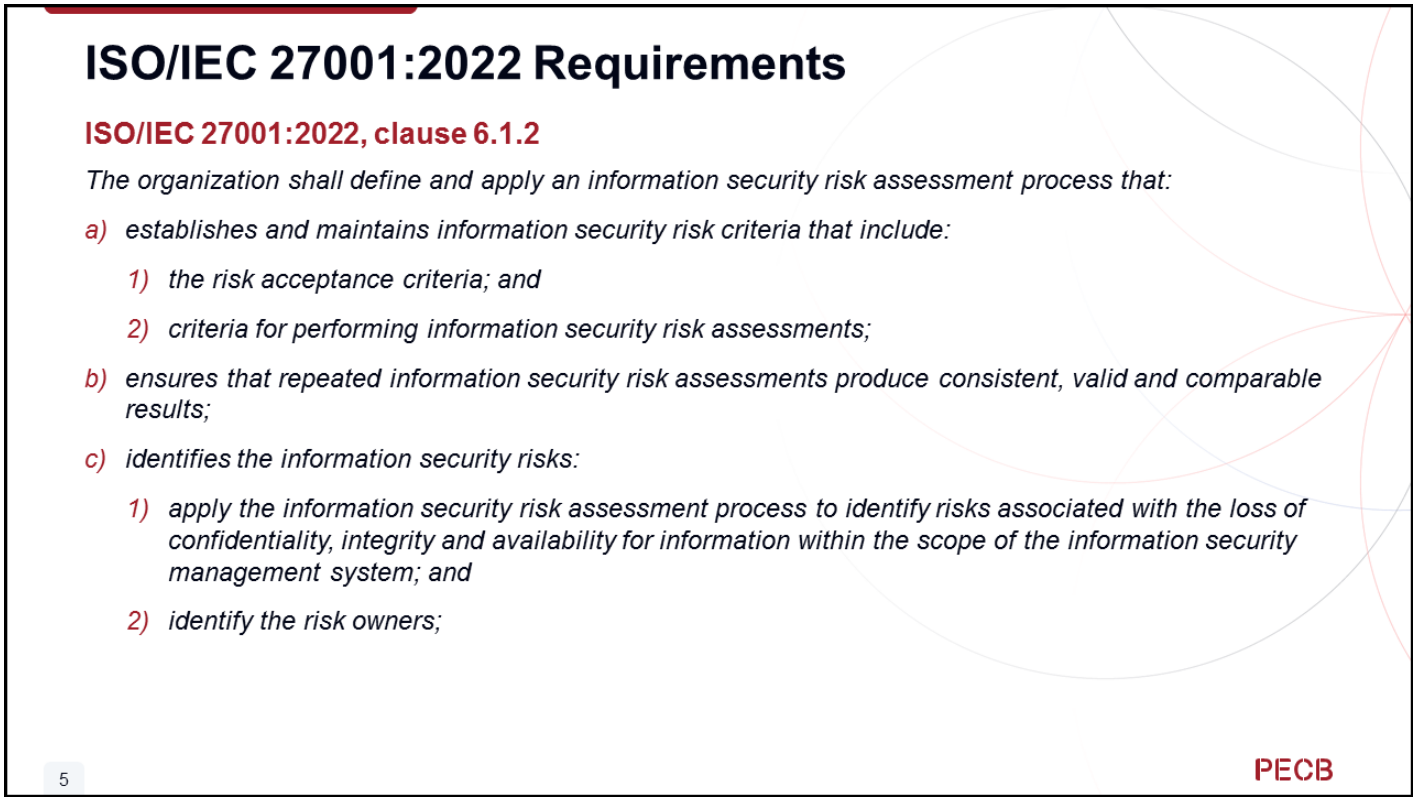
1. Select and define a risk assessment methodology
2. Demonstrate that the selected methodology will provide comparable and reproducible results
3. Define criteria for accepting risks and identify acceptable levels of risk

ISO/IEC 27003, clause 6.1.1 General

The subdivision of requirements for addressing risks can be explained as follows:

- *it encourages compatibility with other management systems standards for those organizations that have integrated management systems for different aspects like quality, environment and information security;*
- *it requires that the organization defines and applies complete and detailed processes for information security risk assessment and treatment; and*
- *it emphasizes that information security risk management is the core element of an ISMS.*

NOTE: The term "risk" is defined as the "effect of uncertainty on objectives".



ISO/IEC 27003, clause 6.1.2 Information security risk assessment

Guidance on establishing risk criteria (6.1.2 a))

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with top management's risk preferences and risk perceptions on one hand and should allow for a feasible and appropriate risk management process on the other hand.

After establishing criteria for assessing consequences and likelihoods of information security risks, the organization should also establish a method for combining them in order to determine a level of risk. Consequences and likelihoods may be expressed in a qualitative, quantitative or semi-quantitative manner.

Risk acceptance criteria relates to risk assessment (in its evaluation phase, when the organization should understand if a risk is acceptable or not), and risk treatment activities (when the organization should understand if the proposed risk treatment is sufficient to reach an acceptable level of risk).

Guidance on producing consistent, valid and comparable assessment results (6.1.2 b))

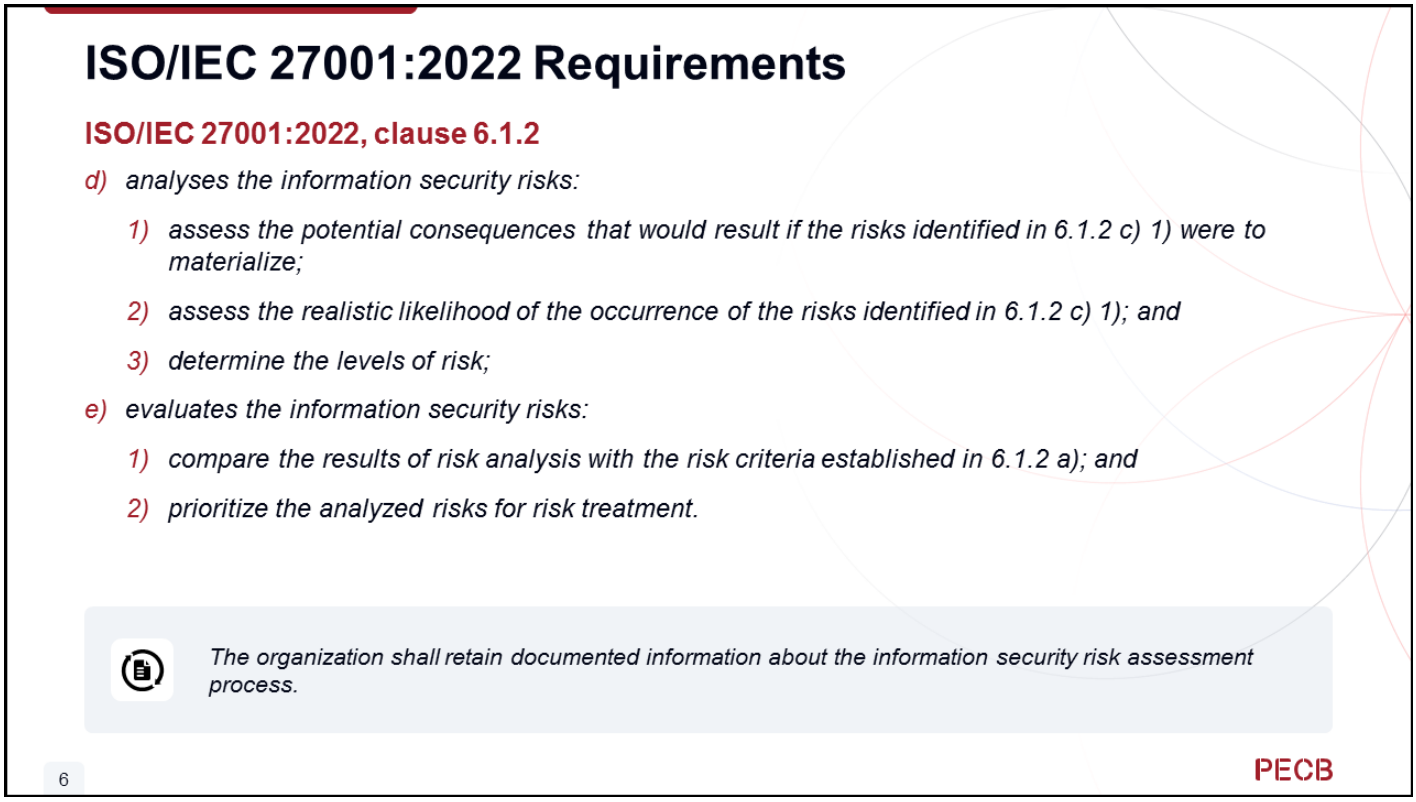
The risk assessment process should be based on methods and tools designed in sufficient detail so that it leads to consistent, valid and comparable results. Whatever the chosen method, the information security risk assessment process should ensure that:

- *all risks, at the needed level of detail, are considered;*
- *its results are consistent and reproducible (i.e. the identification of risks, their analysis and their evaluation can be understood by a third party and results are the same when different persons assess the risks in the same context); and*
- *the results of repeated risk assessments are comparable (i.e. it is possible to understand if the levels of risk are increased or decreased).*

Guidance on identification of information security risks (6.1.2 c))

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of risk sources, events, their causes and their potential consequences. The aim of risk identification is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or

delay the achievement of information security objectives.



ISO/IEC 27003, clause 6.1.2 Information security risk assessment

Guidance on analysis of the information security risks (6.1.2 d))

Risk analysis has the objective to determine the level of the risk.

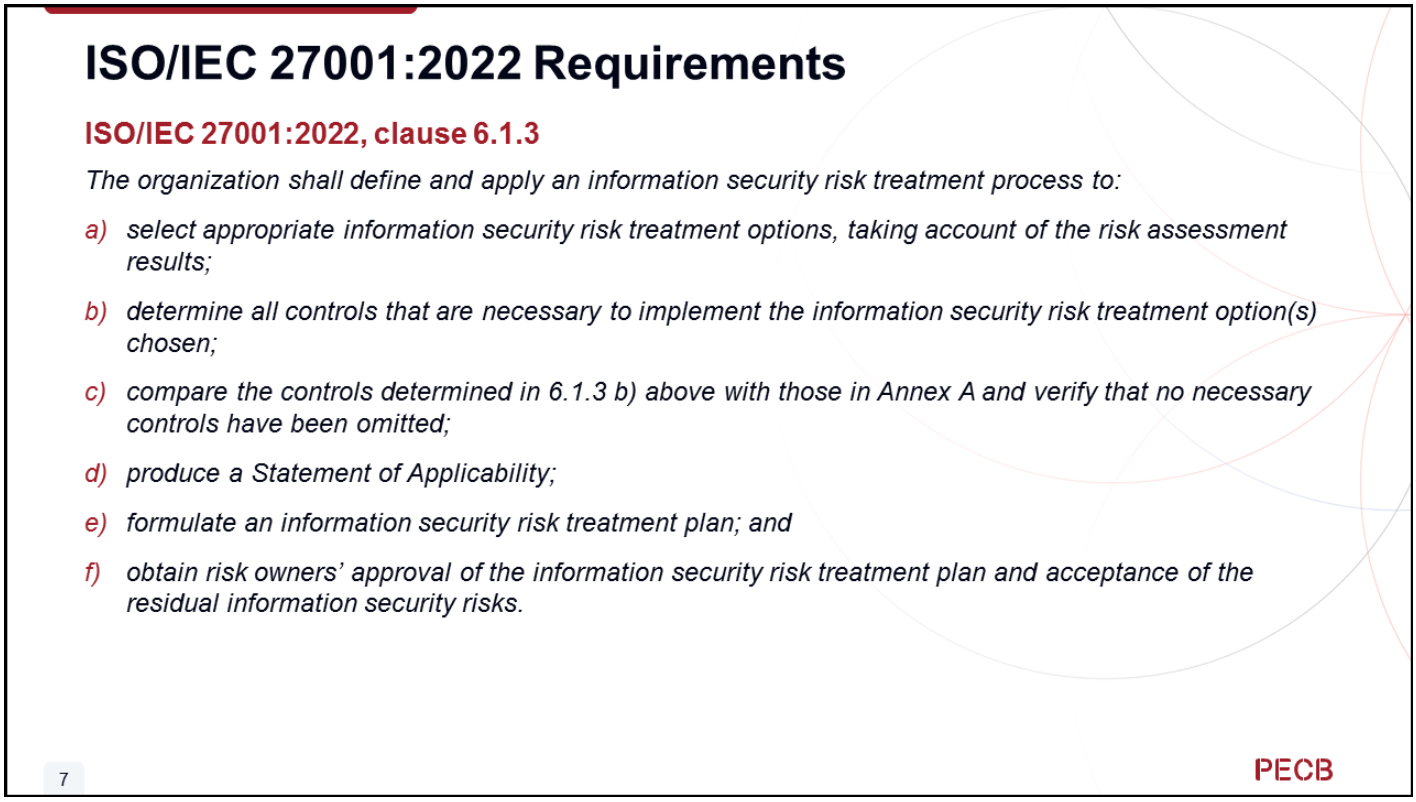
ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001 requires that for each identified risk the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of those consequences occurring to determine a level of risk.

Techniques for risk analysis based on consequences and likelihood can be:

1. *qualitative, using a scale of qualifying attributes (e.g. high, medium, low);*
2. *quantitative, using a scale with numerical values (e.g. monetary cost, frequency or probability of occurrence); or*
3. *semi-quantitative, using qualitative scales with assigned values.*

Guidance on evaluation of the information security risks (6.1.2 e))

Evaluation of analyzed risks involves using the organization's decision making processes to compare the assessed level of risk for each risk with the pre-determined acceptance criteria in order to determine the risk treatment options.



ISO/IEC 27003, clause 6.1.3 Information security risk treatment

Guidance on information security risk treatment options (6.1.3 a))

Risk treatment options are:

a. *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or by removing the risk source (e.g. closing an e-commerce portal);*
b. *taking additional risk or increasing risk in order to pursue a business opportunity (e.g. opening an e-commerce portal);*
c. *modifying the risk by changing the likelihood (e.g. reducing vulnerabilities) or the consequences (e.g. diversifying assets) or both;*
d. *sharing the risk with other parties by insurance, sub-contracting or risk financing; and*
e. *retaining the risk based on the risk acceptance criteria or by informed decision (e.g. maintaining the existing e-commerce portal as it is).*

Guidance on determining necessary controls (6.1.3 b))

Special attention should be given to the determination of the necessary information security controls. Any control should be determined based on information security risks previously assessed. If an organization has a poor information security risk assessment, it has a poor foundation for its choice of information security controls.

Slide Notes Extension

ISO/IEC 27003, clause 6.1.3 Information security risk treatment (cont'd)

Guidance on producing a Statement of Applicability (SoA) (6.1.3 d))

The SoA contains:

- *all necessary controls and, for each control:*
  - *the justification for the control's inclusion; and*
  - *whether the control is implemented or not (e.g. fully implemented, in progress, not yet started); and*
- *the justification for excluding any of the controls in ISO/IEC 27001, Annex A.*

Guidance on formulating an information security risk treatment plan (6.1.3 e))

ISO/IEC 27001 does not specify a structure or content for the information security risk treatment plan. However, the plan should be formulated from the outputs of 6.1.3 a) to c). Thus the plan should document for each treated risk:

- *selected treatment option(s);*
- *necessary control(s); and*
- *implementation status.*

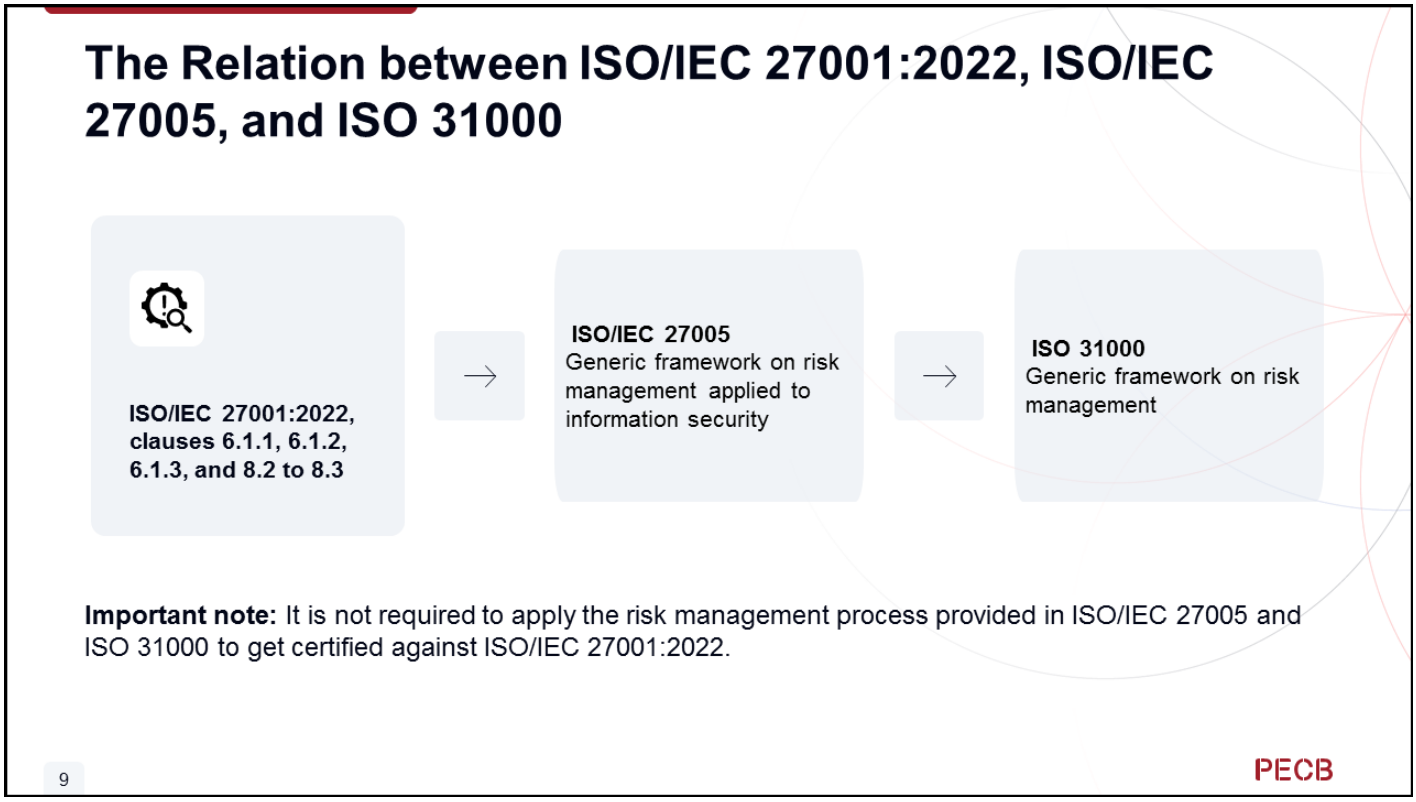
Other useful content can include:

- *risk owner(s); and*
- *expected residual risk after the implementation of actions.*

Guidance on obtaining risk owners' approval (6.1.3 f))

When the information security risk treatment plan is formulated, the organization should obtain the authorization from the risk owners. Such authorization should be based on defined risk acceptance criteria or justified concession if there is any deviance from them.

Through its management processes the organization should record the risk owner's acceptance of the residual risk and management approval of the plan.



Based on the ISO 31000 framework, the ISO/IEC 27005 standard explains in detail how to conduct risk assessment and risk treatment in the context of information security. This is the implementation of the PDCA cycle (Plan, Do, Check, Act) for risk management as it is used in all standards of management systems. In this case, it can be easily connected to the corresponding clauses of ISO/IEC 27001:2022 on risk management (clauses 6.1.2 and 6.1.3), ultimately leading to the certification of the organization.

ISO/IEC 27005, Introduction

This document provides guidance on:

- *implementation of the information security risk requirements specified in ISO/IEC 27001;*
- *essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;*
- *actions that address risks related to information security;*
- *implementation of risk management guidance in ISO 31000 in the context of information security.*

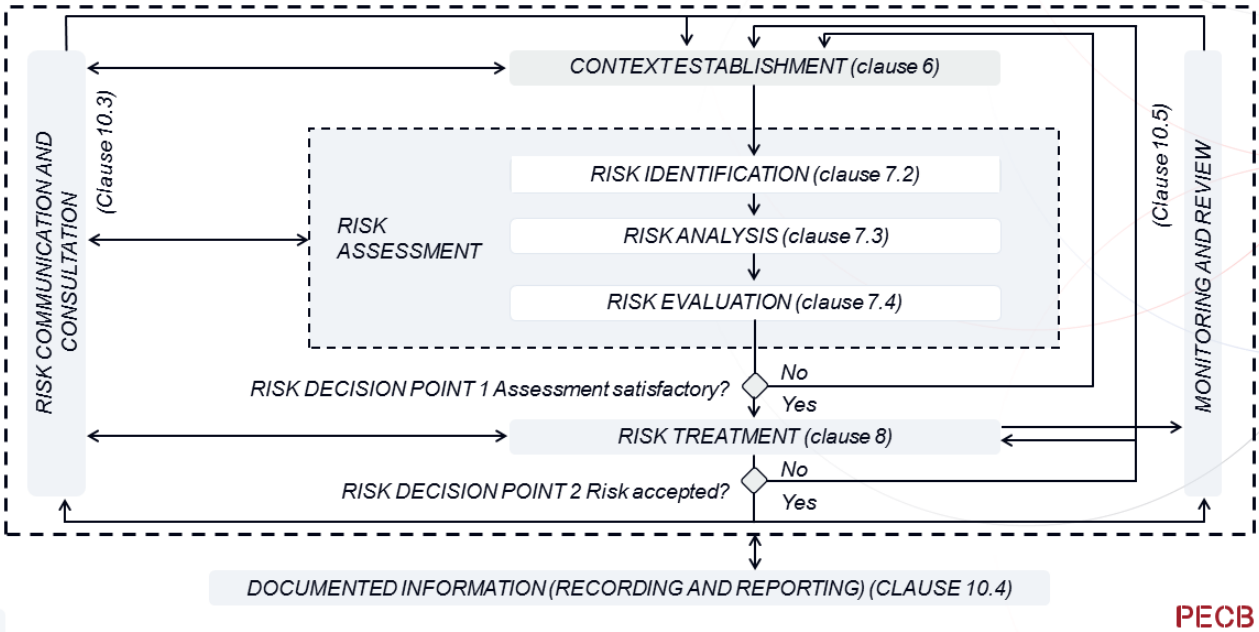
This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

- *organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;*
- *persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);*
- *organizations that intend to improve their information security risk management process.*

The Risk Management Process

ISO/IEC 27005, Figure 1

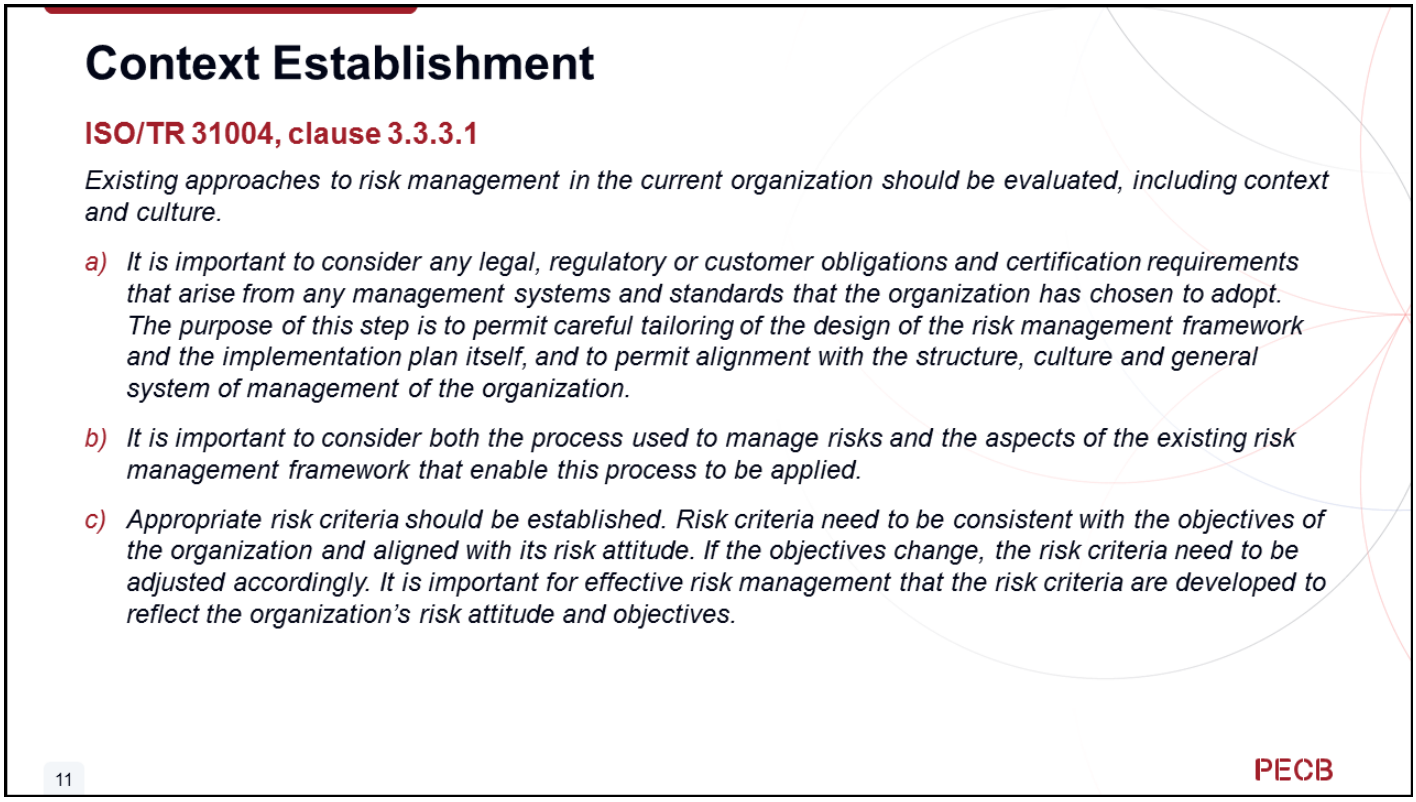


10

PECB

As illustrated in the figure, the risk management process should be iterative for risk assessment and risk treatment activities. If the risk assessment activities have provided sufficient evidence that the determined actions will reduce the risk to an acceptable level, the next step is to implement risk treatment options. However, if there is insufficient evidence to determine the risk level and if the risk treatment process appears to be unacceptable, a new iteration of risk assessment will be conducted on some or all the items of the application domain. If the risk treatment option is not satisfactory, but the context establishment and risk assessment are correct, a new iteration of risk treatment will be conducted; otherwise, a new iteration of context establishment will also have to be applied.

Whether the risk treatment is effective depends on the outcomes of the risk assessment. It is possible that risk treatment may not directly lead to an acceptable level of residual risk and, if that is the case, a new iteration of risk assessment should be undertaken.

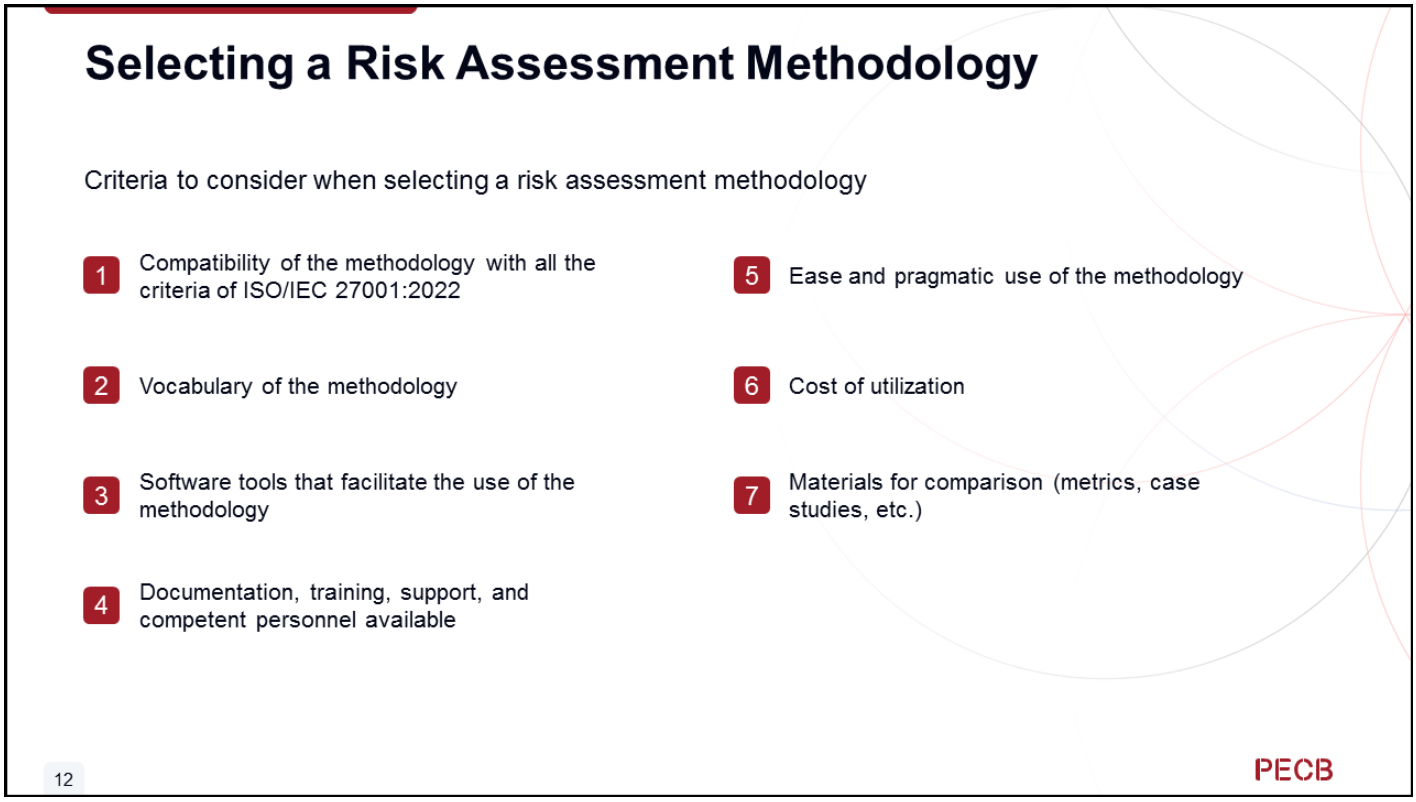


ISO/TR 31004, clause 3.3.3.2

On the basis of the evaluations described in 3.3.3.1, the organization should decide which aspects of the current risk management approach:

a. *could continue to be used in future (possibly extended to other types of decision making);*
b. *need amendment or enhancement;*
c. *no longer add value and should be discontinued.*

The organization should develop, document and communicate how it will be managing risk. The scale and content of the organization's internal standards, guidelines and models related to risk management should reflect organizational culture and context.

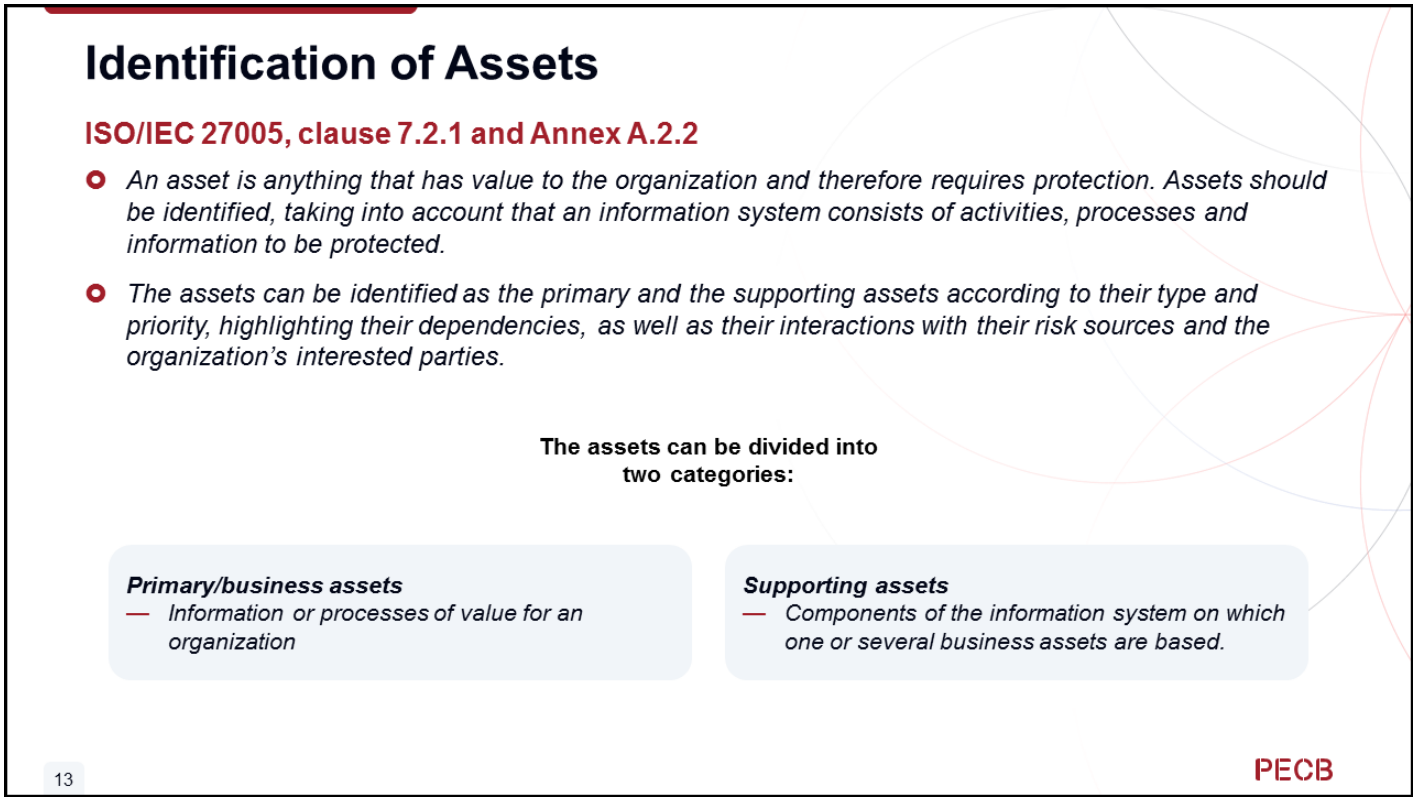


Any method of risk assessment that meets the minimum criteria of ISO/IEC 27001:2022 is acceptable, even a method developed in-house (provided that it can produce comparable and reproducible results).

Any risk analysis at least should consider the evaluation criteria established by ISO/IEC 27001:2022. The actions taken should produce desirable effects, prevent and reduce undesirable effects, and improve the organization's processes. In addition, the risk analysis should allow for the selection of the objective criteria for determining a level of acceptable risk.

When selecting a risk assessment methodology, you should ask:

- Have the potential impacts been identified?
- Is the probability of the occurrence of a potential impact evaluated?
- Can someone else use the same data and reach the same result?
- Can the process be repeated and give consistent results over time?
- Does the process take into account the analysis of the impact of changes?



ISO/IEC 27005, Annex A.2.2 Assets (cont'd)

The primary/business assets are often used in the event-based approach (identification of events and their consequences on business assets).

The supporting assets are often used in the asset-based approach (identification and analysis of vulnerabilities and threats on these assets) and in the risk treatment process (specification of the asset(s) to which each control should be applied).

Business and supporting assets are related, therefore risk sources identified for supporting assets can impact business assets.

For this reason, it is important to identify the relationships between the assets, and to understand their value to the organization. Misjudging the asset value can lead to a misjudgment of the consequences related to the risk but can also affect the understanding of the likelihood of threats under consideration.

Identification of Threats

ISO/IEC 27005, clause 7.2.1

A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information.

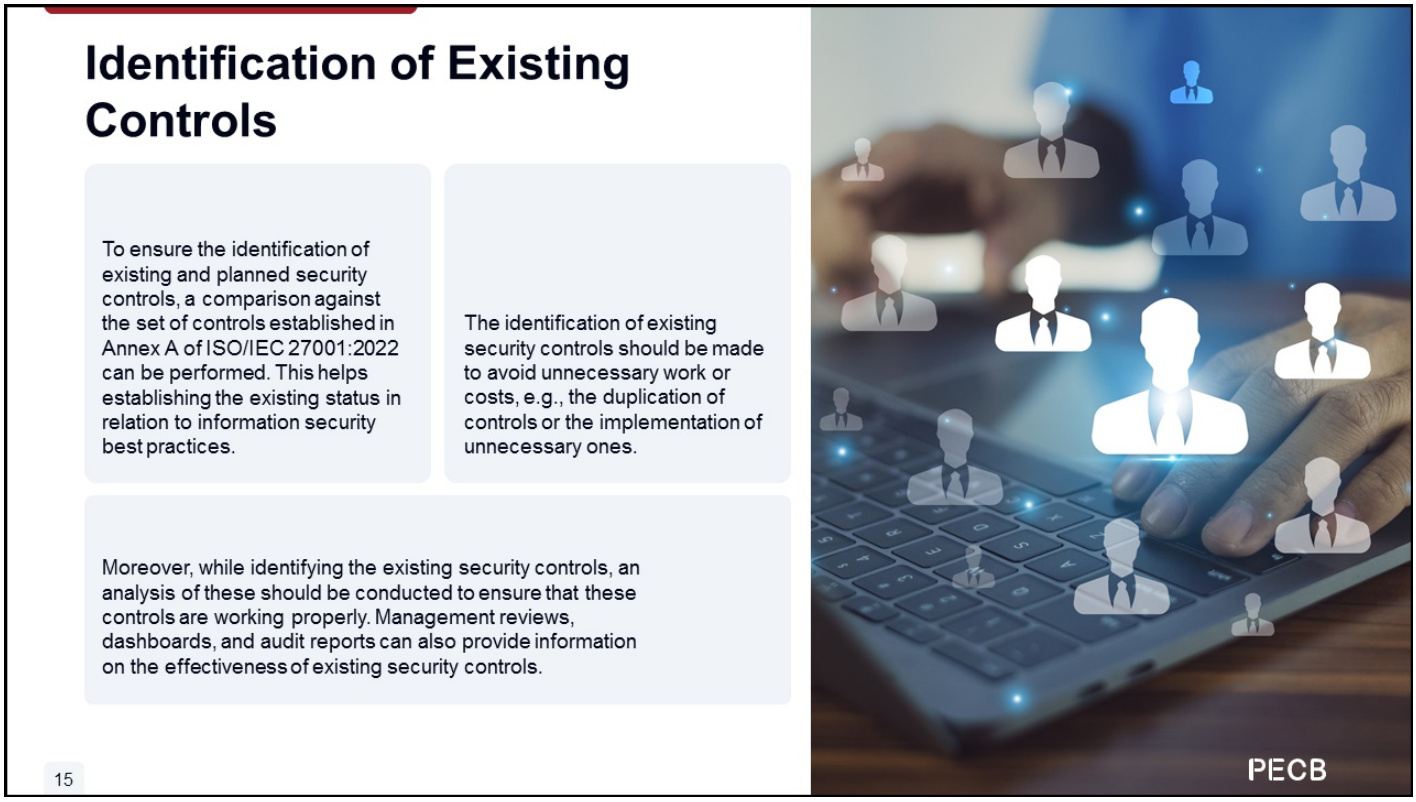
- Identification of threats enables organizations to make better decisions related to risk treatment options and activities.
- The list of threats is not exhaustive. New threats may appear instantaneously due to trends in technology and the evolving capabilities of threat agents.

14

PECB

ISO/IEC 27005, clause 7.2.1 Identifying and describing information security risks (cont'd)

The asset-based approach can identify asset-specific threats and vulnerabilities and allows the organization to determine specific risk treatment on a detailed level.

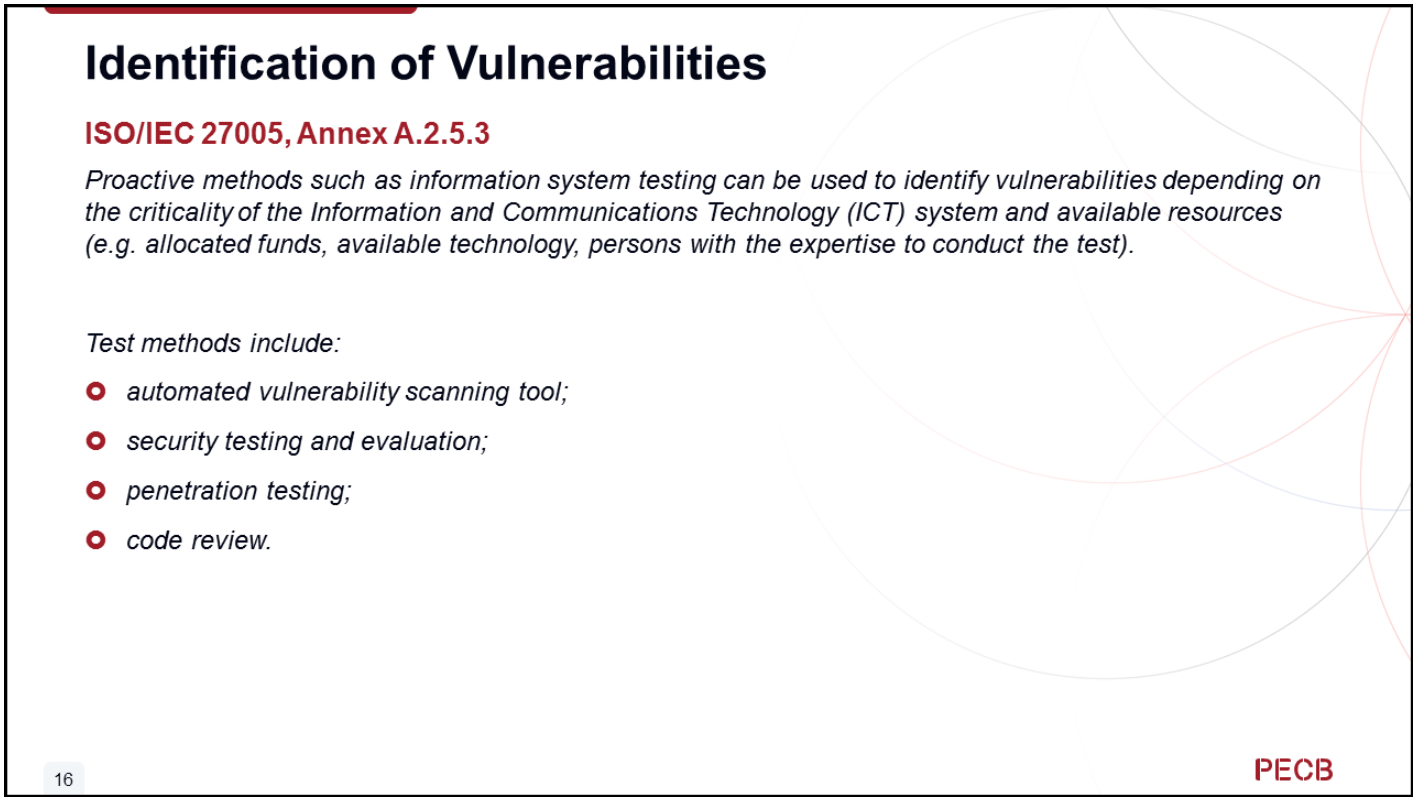


ISO/IEC 27005, clause 7.2.1 Identifying and describing information security risks

Management of information security risks should not be constrained by arbitrary or restrictive views of how risks should be structured, grouped, aggregated, split or described. Risks can appear to overlap or be subsets or specific instances of other risks. However, controls for individual risks should be considered and identified separately from wider risks or aggregated risks for the purposes of risk treatment.

In addition to considering the security controls already in place, the organization should also examine any controls that are planned to be implemented.

When the existing and planned controls are analyzed, they can be identified as ineffective or appropriate. If the control is not justified or does not address a risk, it should be rechecked to determine if it should be removed, replaced by another more appropriate control, or whether it should still remain in place, considering that its removal could trigger considerable costs.



ISO/IEC 27005, Annex A.2.5.3 Methods for assessment of technical vulnerabilities (cont'd)

An automated vulnerability-scanning tool is used to scan a group of hosts or a network for known vulnerable services [e.g. system allows anonymous File Transfer Protocol (FTP), Sendmail relaying]. However, some of the potential vulnerabilities identified by the automated scanning tool do not necessarily represent real vulnerabilities in the context of the system environment (e.g. some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements). Some of the vulnerabilities flagged by the automated scanning software can actually not be vulnerable for a particular site but can be configured that way because their environment requires it. This test method can therefore produce false positives.

Security testing and evaluation (STE) is another technique that can be used in identifying ICT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g. test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the ICT system are secured. Penetration testing, when used in the risk assessment process, can be used to assess an ICT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the ICT system from the viewpoint of a threat source and to identify potential failures in the ICT system protection schemes.

Code review is the most thorough (but also most expensive) way of vulnerability assessment.

The results of these types of security testing help identify a system's vulnerabilities.

Assessment of Potential Consequences

ISO/IEC 27005, clause 7.3.2

Failure to adequately preserve the security of information can lead to loss of its confidentiality, integrity or availability. Loss of confidentiality, integrity or availability can have further consequences for the organization and its objectives. Consequence analysis can be performed bottom up from the information security consequences by considering what can happen if there is a loss of confidentiality, integrity or availability of the information in question. Typically, the risk owner can estimate the consequence if the event occurs.

The following elements should be taken into consideration:

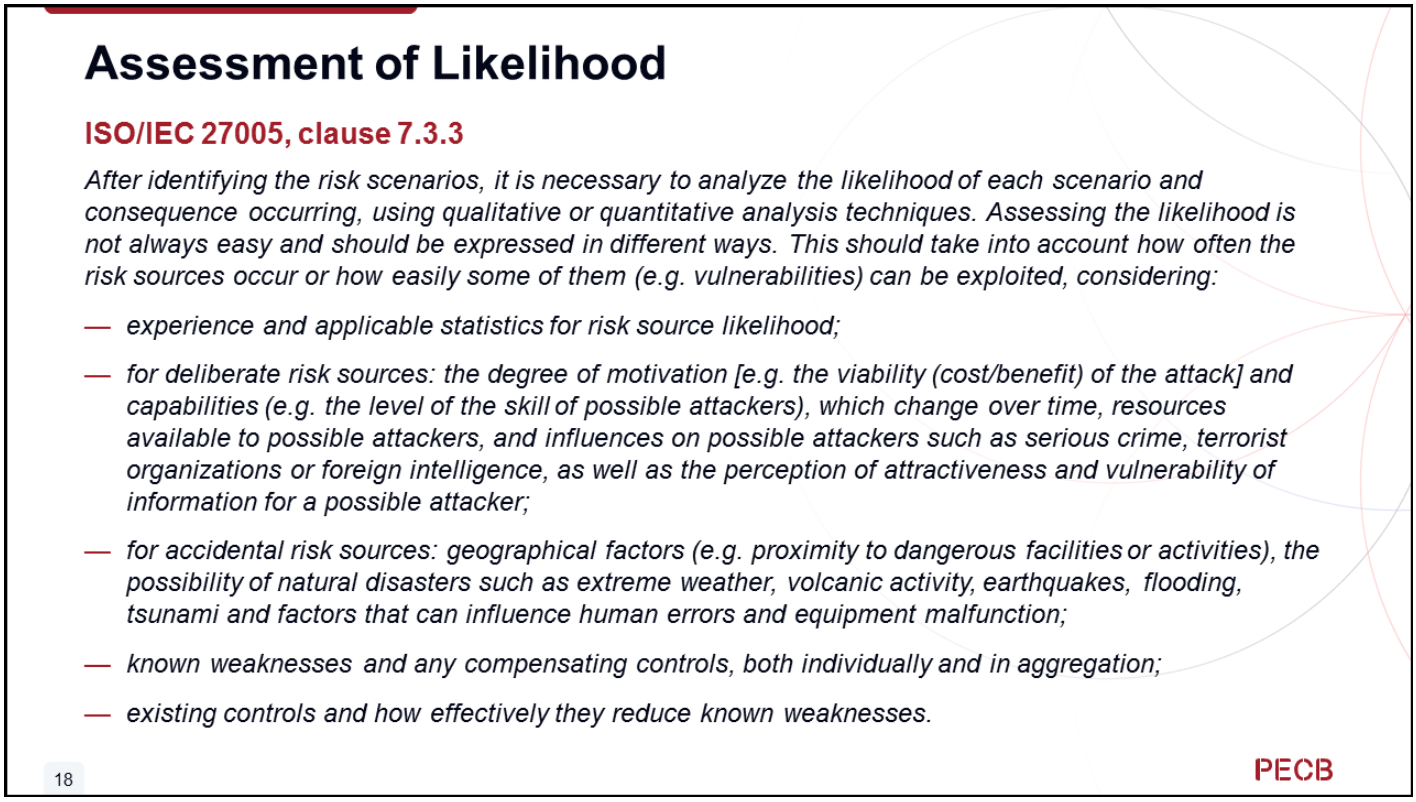
- *estimation (or measure based on experience) of the losses (time or data) due to the event as result of interrupting or disturbing operations;*
- *estimation/perception of severity of the consequence (e.g. expressed in money);*
- *recovery costs depending on whether recovery can be done internally (by the risk owner team), or there is a need to call an external entity.*

17

PECB

The consequence of an incident scenario is determined by using the impact criteria defined during the context establishment phase. An impact may derive from one or more aspects. Consequences on assets can be calculated on the basis of financial securities or qualitative scales. These effects may be temporary or permanent, as is the case with the destruction of an asset.

The consequences of the occurrence of an incident may be evaluated differently depending on the involvement of interested parties in risk assessment. The significant impacts on the organization should be documented accordingly.



ISO/IEC 27005, clause 7.3.3 Assessing likelihood (cont'd)

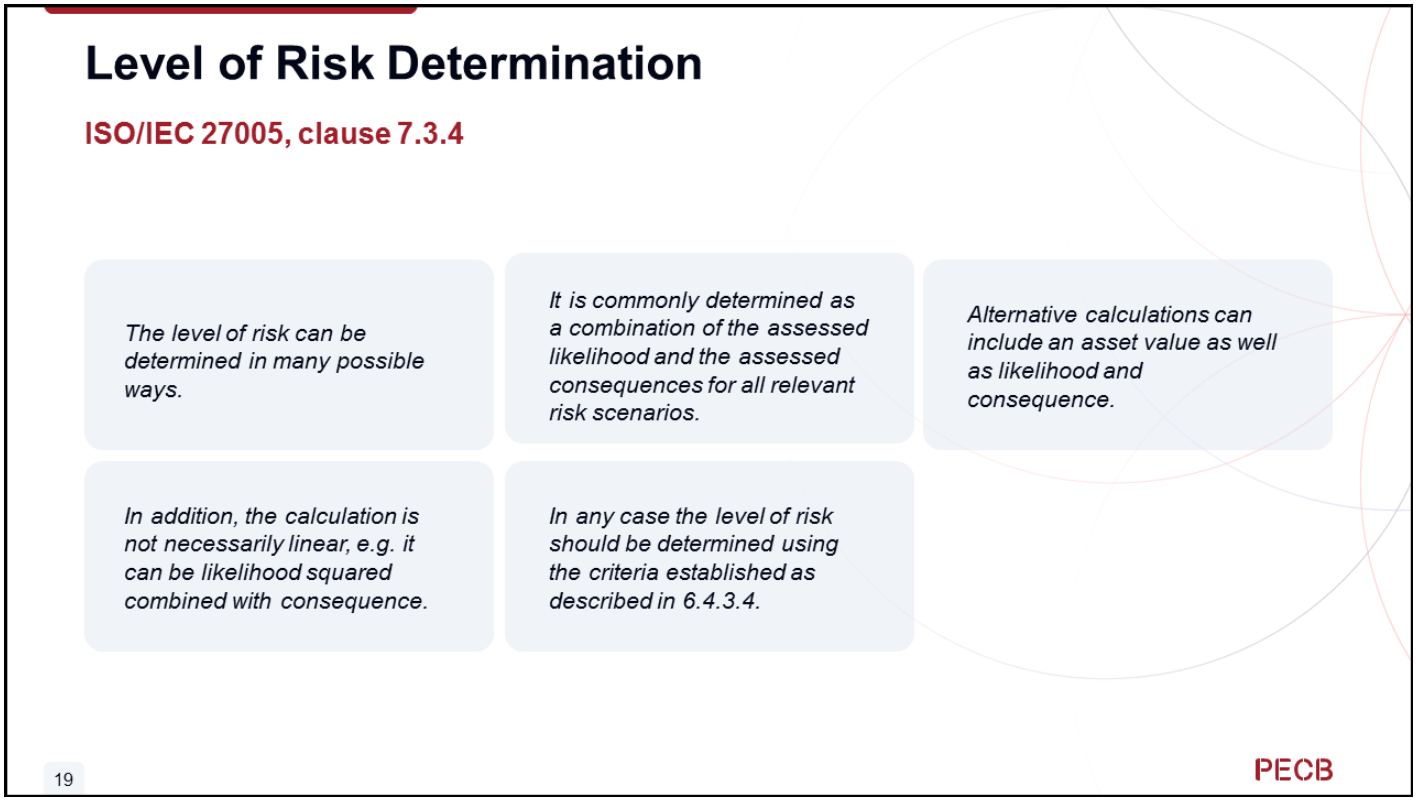
Estimation of likelihood is intrinsically uncertain, not only because it considers things that have not yet happened and are therefore not fully known, but also because likelihood is a statistical measure and is not directly representative of individual events. The three basic sources of assessment uncertainty are:

- *personal uncertainty originating in the judgement of the assessor, which derives from variability in the mental heuristics of decision making;*
- *methodological uncertainty, which derives from the use of tools that inevitably model events simplistically;*
- *systemic uncertainty about the anticipated event itself, which derives from insufficient knowledge (in particular, if evidence is limited or a risk source changes with time).*

To increase the reliability of estimating likelihood, organizations should consider using:

a. *team assessments rather than individual assessments;*
b. *external sources, such as information security breach reports;*
c. *scales with range and resolution appropriate to the organization's approach;*
d. *unambiguous categories, such as "once a year", rather than "infrequent".*

When assessing the likelihood of events, it is important to recognize the difference between independent and dependent events. The likelihood of events that depend on each other is conditioned by the relationship between them (e.g. a second event can be inevitable if a first event occurs) so that separate assessment of both their likelihoods is not necessary. The likelihood of relevant independent events are all essential contributors to the likelihood of a consequence to which they contribute.



Numerical estimation

If the organization possesses data on past or current incidents, especially past incidents, such data can be used to estimate future risks. Nonetheless, other methods should also be used to make such estimates.

Despite the fact that data on past incidents can be useful, they are not necessarily as helpful when assessing the risks that emerge from new activities. The purpose of assessing the risks that emerge from new activities is to identify incidents with a high level of risk, which have not caused any incidents yet. In this way, potential incidents can be prevented from occurring.

It is possible to calculate the probabilities of potential incidents by using external data. For example, past data on road accidents can be used to calculate road transport risks associated with those employees who travel by car. These statistics are used to calculate the probability of more serious, but also very rare, incidents. However, such calculations are not always possible.

Example of a Qualitative Approach for Level of Risk Determination

ISO/IEC 27005, Table A.3

Likelihood	Consequence				
	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low

20

PECB

ISO/IEC 27005, Annex A.1.1.2.3 Level of risk

The utility of qualitative scales and the consistency of risk assessments that derive from them depend entirely on the consistency with which the category labels are interpreted by all interested parties.

The levels of any qualitative scale should be unambiguous, its increments should be clearly defined, the qualitative descriptions for each level should be expressed in objective language and the categories should not overlap with each other.

Evaluation of Levels of Risk Based on Risk Evaluation Criteria

ISO 31000, clause 6.4.4

The purpose of risk evaluation is to support decisions.

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

21

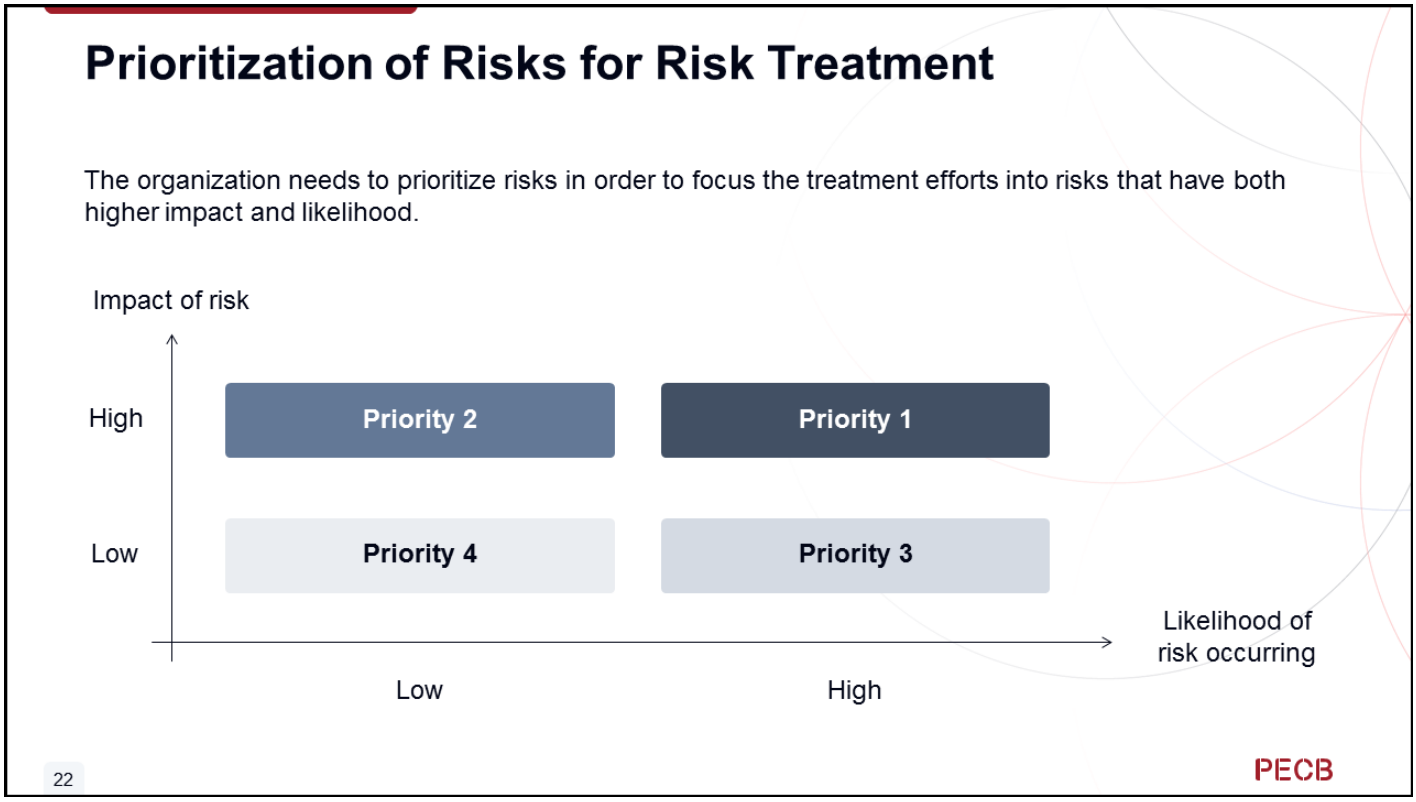
PECB

ISO/IEC 27005, clause 7.4.1 Comparing the results of risk analysis with the risk criteria

Risk evaluation decisions should be based on the comparison of assessed risk with defined acceptance criteria, ideally taking into account the degree of confidence in the assessment. In some cases, such as the frequent occurrence of relatively low consequence events, it can be helpful to consider their cumulative effect over some timescale of interest, rather than the risk of each event considered individually, as this can provide a more realistic representation of overall risks.

There can be uncertainties in defining the boundary between those risks that require treatment and those that do not. Under certain circumstances, using a single level as the acceptable level of risk that divides risks that require treatment from those which do not is not always appropriate. In some cases, it can be more effective to include an element of flexibility into the criteria by incorporating additional parameters such as cost and effectiveness of possible controls.

The levels of risk can be validated based on consensus among risk owners and business and technical specialists. It is important that risk owners have a good understanding of the risks they are accountable for that accords with the results of objective assessment. Consequently, any disparity between assessed levels of risk and those perceived by risk owners should be investigated to determine which better approximates to reality.



Risk prioritization is a commonly used process for identifying risks that matter and have an impact on the organization. Risk prioritization also supports the decision-making process by considering possible responses to various risks. Once the potential incident scenarios have been established, the criteria for the classification of risk in terms of priority should be defined.

The zero value of risk does not exist. Nonetheless, it is possible to define a threshold, below which the organization accepts to not engage in any activity that reduces the level of risk.

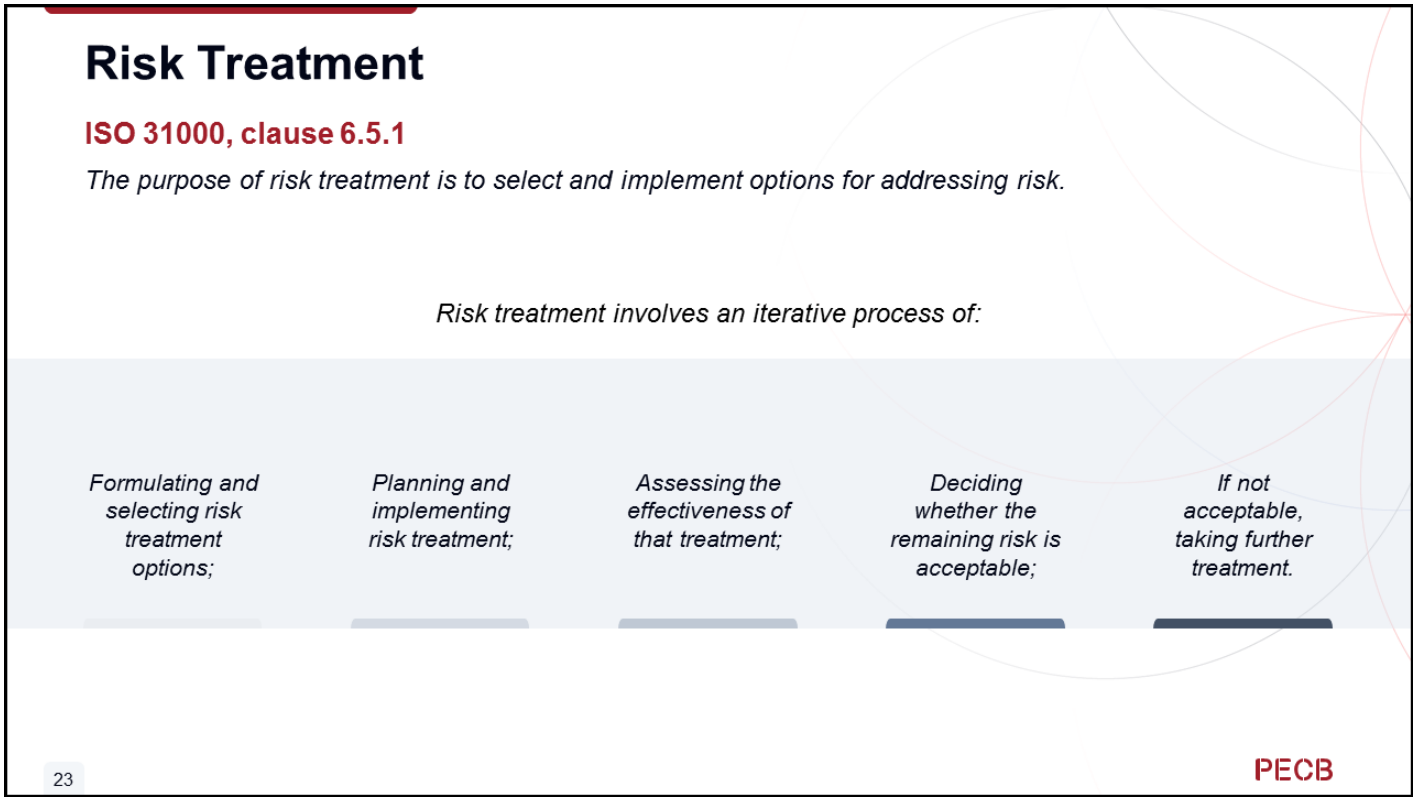
At the other end of the scale, there is a threshold beyond which risk is unacceptable, and as such, everything must be done to eliminate the risk source or reduce the risk.

ISO/IEC 27005, clause 7.4.2 Prioritizing the analyzed risks for risk treatment

Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding about the next step to take. Those should refer to:

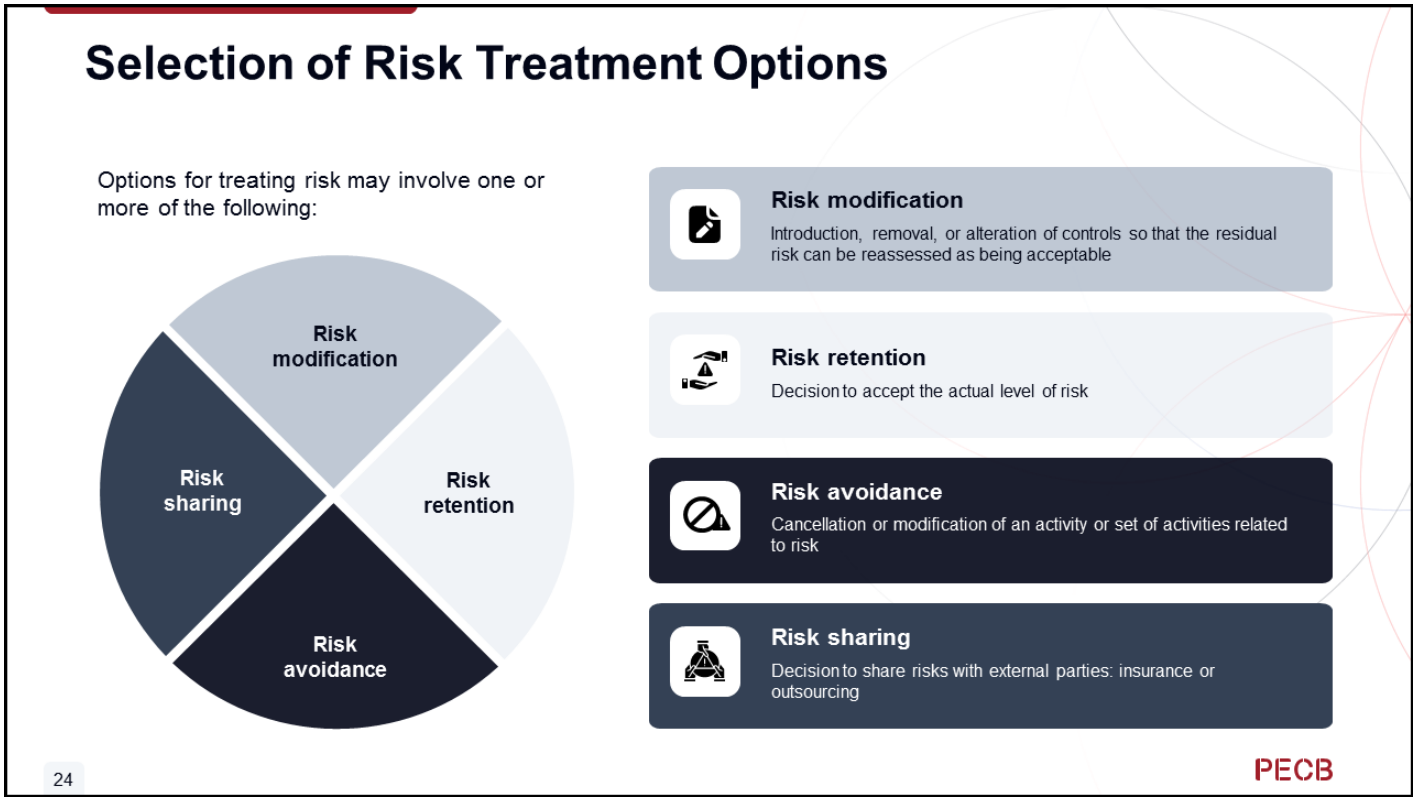
- *whether a risk treatment is required;*
- *priorities for risk treatment considering assessed levels of risks.*

Risk criteria used to prioritize risks should consider the objectives of the organization, contractual, legal and regulatory requirements and the views of relevant interested parties. Prioritization as taken in the risk evaluation activity are mainly based on the acceptance criteria.



It is preferable to initially focus the effort on the treatment of high-level risks and then gradually proceed with the treatment of low-level risks.

Selecting the best risk treatment option means that the costs associated with implementing such risk treatment options do not exceed the benefits of implementing them. The costs should at least be the same as the benefits. When conducting such a cost-benefit analysis, the organization's context should be taken into account, as well.



ISO/IEC 27005, clause 8.2 Selecting appropriate information security risk treatment options

Several options for risk treatment include:

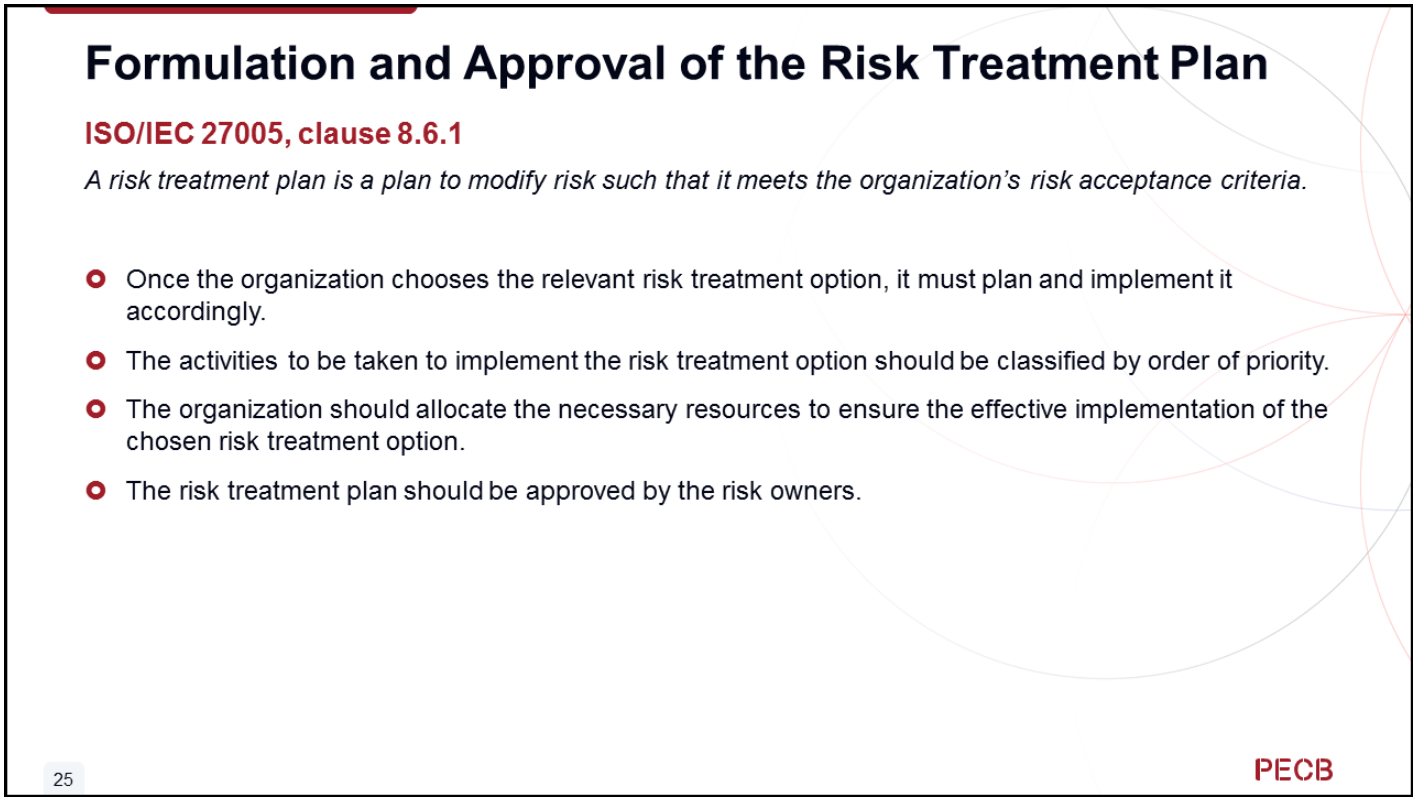
- *risk avoidance, by deciding not to start or continue with the activity that gives rise to the risk;*
- *risk modification, by changing the likelihood of the occurrence of an event or a consequence or changing the severity of the consequence;*
- *risk retention, by informed choice;*
- *risk sharing, by splitting responsibilities with other parties, either internally or externally (e.g. sharing the consequences via insurance);*

EXAMPLE 1: An example of risk avoidance is an office location situated in a flood-zone, where there is the potential of a flood and resultant damages to the office and restrictions to the availability of and/or access to the office. The relevant physical controls can prove insufficient to reduce this risk, in which case, the treatment option of risk avoidance can be the best available option. This can involve closing or stopping operation of that office.

EXAMPLE 2: Another example of risk avoidance is choosing not to collect certain information from individuals so that it is not necessary for the organization to manage, store and transmit the information in its information systems.

In the case of risk sharing, at least one control is required to modify the likelihood or consequence, butthe organization delegates the responsibility of implementing the control to another party.

Risk treatment options should be selected based on the outcome of the risk assessment, the expected costs for implementing these options and the expected benefits from these options, both individually and in the context of other controls. Risk treatment should be prioritized according to levels of risk as defined, time constraints and necessary sequence of implementations, and risk evaluation outcomes established in 7.4. While choosing the option, it can be considered how a particular risk is perceived by affected parties, and the most appropriate ways of communicating risk to these parties.



ISO/IEC 27005, clause 8.6.1 Formulation of the risk treatment plan (cont'd)

The purpose of this activity is to create plan(s) for treating specific sets of the risks that are on the list of prioritized risks. There are two possible interpretations of the term "plan" in the context of risk treatment. The first is a project plan, i.e. a plan to implement the organization's necessary controls. The second is a design plan, i.e. the plan that not only identifies necessary controls but also describes how the controls interact with their environment and each other to modify risks. In practice, both can be used.

Every risk that needs treatment should be treated in one of the risk treatment plans. An organization can choose to have several risk treatment plans, which together implement all required aspects of risk treatment.

While creating the risk treatment plan, organizations should consider the following:

- *priorities in relation with the level of risk and urgency of treatment;*
- *whether different types of controls (preventive, detective, corrective) or their composition are applicable;*
- *whether it is necessary to wait for a control to be settled before starting to implement a new one on the same asset;*
- *whether there is a delay between the time the control is implemented and the moment where it is fully effective and operational.*

For each treated risk the treatment plan should include the following information:

- *the rationale for selection of the treatment options, including the expected benefits to be gained;*
- *those who are accountable and responsible for approving and implementing the plan;*
- *the proposed actions;*
- *the resources required, including contingencies;*
- *the performance indicators;*
- *the constraints;*
- *the required reporting and monitoring;*
- *when actions are expected to be undertaken and completed;*
- *implementation status.*

Slide Notes Extension

ISO/IEC 27005, clause 8.6.1 Formulation of the risk treatment plan (cont'd)

The risk treatment plan actions should be ranked by priority in relation with the level of risk and urgency of treatment. The higher the level of risk, and in some cases the frequency of risk occurrence, the sooner the control is to be implemented.

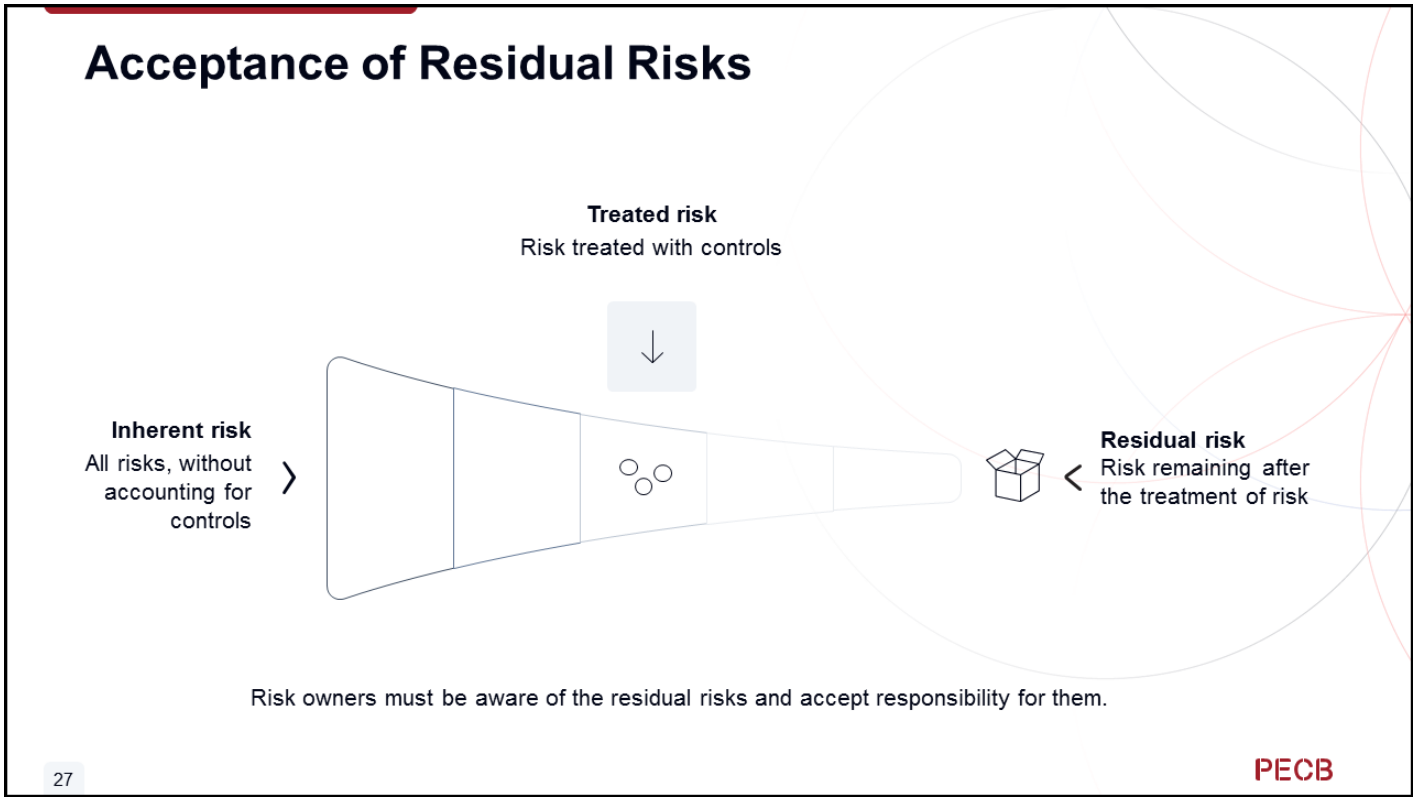
For each listed risk within the risk treatment plan, detailed implementation information should be tracked and can include but is not limited to:

- *names of risk owners and persons responsible for the implementation;*
- *implementation dates or timelines;*
- *control activities planned to test the implementation result;*
- *implementation status;*
- *cost level (investment, operation).*

ISO/IEC 27005, clause 8.6.2 Approval by risk owners

The information security risk treatment plan should be approved by the risk owners once it is formulated. Risk owners should also decide on the acceptance of residual information security risks. This decision should be based on defined risk acceptance criteria.

The results of the risk assessment, the risk treatment plan and the remaining risks should be understandable to the risk owners so that they can discharge their accountabilities properly.



After the implementation of a risk treatment plan, there are always residual risks. **The value of risk reduction following risk treatment should be evaluated, calculated, and documented.** Residual risks can be difficult to evaluate, but an estimation should at least be made to ensure that the value of residual risks is within the organization's risk acceptance criteria. The organization also must put in place residual risk surveillance mechanisms.

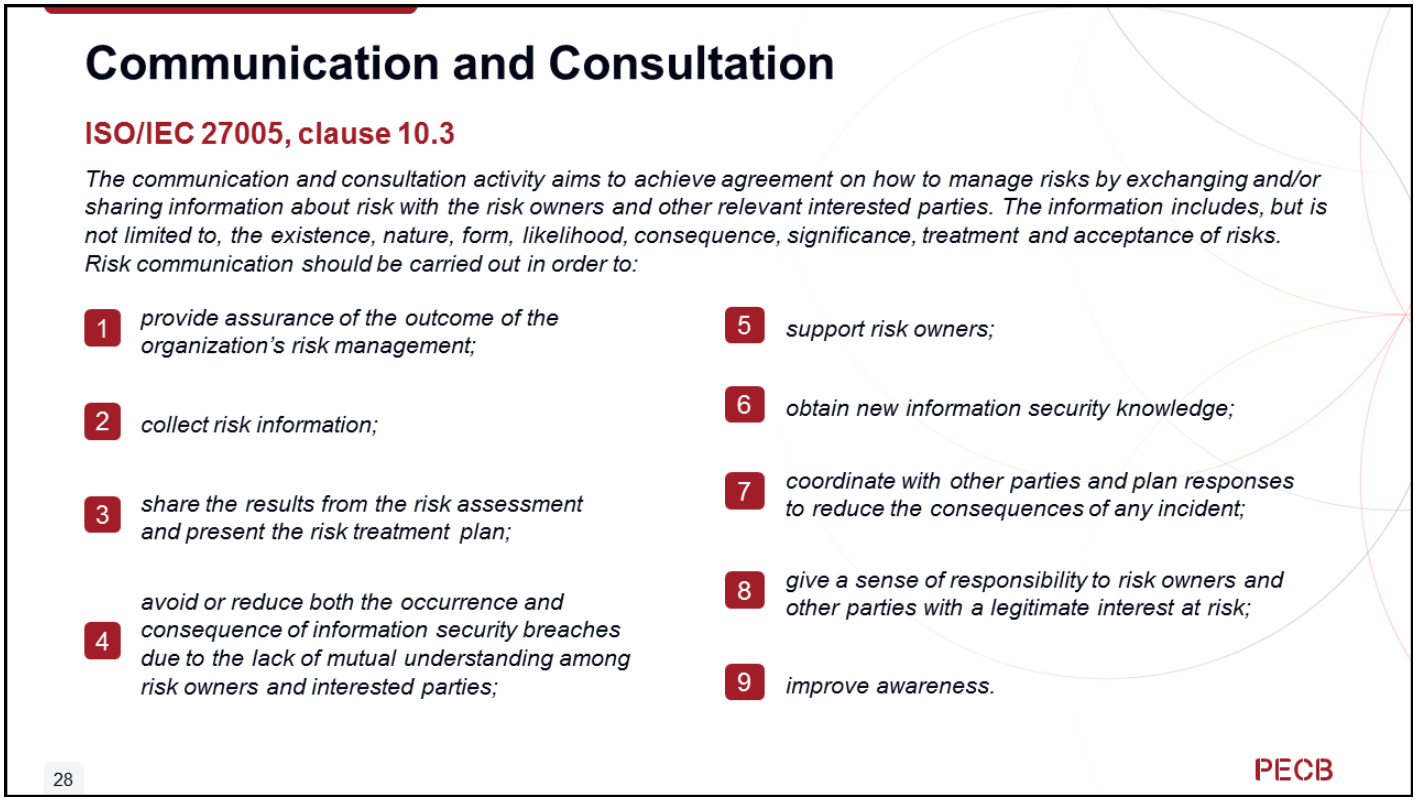
If the residual risk is considered as unacceptable after the controls have been implemented, a decision must be made to treat the risk completely. One alternative could be to identify other risk treatment options such as sharing the risk (insurance or outsourcing), which would reduce the risk to an acceptable level. Another option could be to accept the risk (on purpose). Even though it is best practice to completely eliminate risks that exceed the organization's risk acceptance criteria, it is not always possible to reduce all risks to an acceptable level. **In all circumstances, residual risks must be understood, accepted, and approved by management.**

ISO/IEC 27005, clause 8.6.3 Acceptance of the residual information security risks

Risk acceptance can involve a process to achieve endorsements of treatments prior to a final risk acceptance decision. It is important for risk owners to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval. Depending on the risk assessment process and risk acceptance criteria, this can require a manager with a higher level of authority than the risk owner to agree to the risk acceptance.

It can take some time to implement a plan to treat assessed risks. Risk criteria can allow levels of risk to exceed a desired threshold to a defined extent if there is a plan in place to reduce that risk in an acceptable time. Risk acceptance decisions can take into account timeframes in risk treatment plans and whether or not risk treatment implementation progress is in line with what is planned.

Some risks can vary over time (regardless of whether this change is due to implementation of a risk treatment plan). Risk acceptance criteria can consider this and have risk acceptance thresholds that depend on the length of time that an organization can be exposed to an assessed risk.



Good communication and consultation requires honest talks and meetings with all the relevant interested parties so that all their needs are identified and fulfilled.

To achieve desirable results, it is important to firstly develop a communication strategy and then implement it.

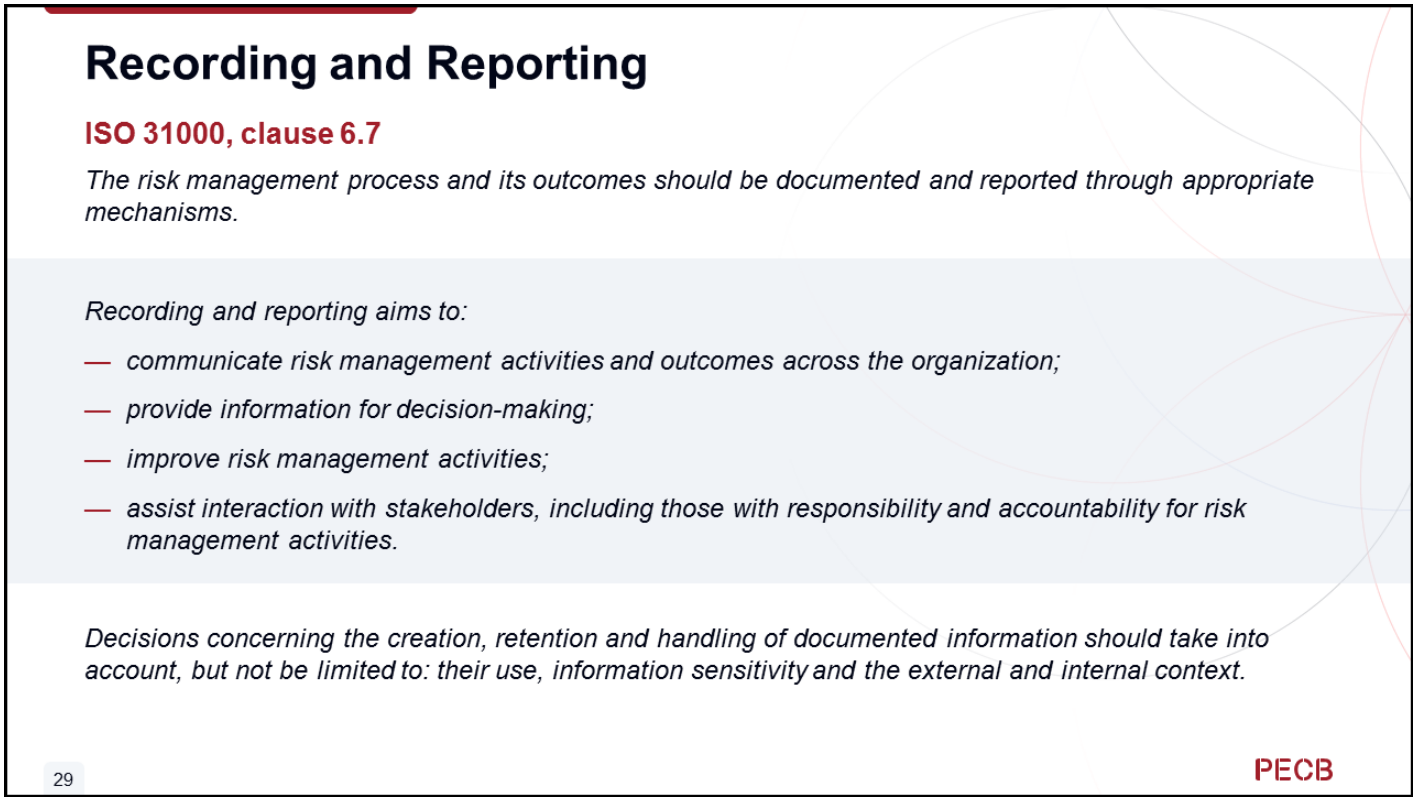
The second important part is consultation. The risk manager is considered as an internal consultant or coach that helps less experienced employees in acquiring the necessary expertise in risk management so as to achieve risk optimization objectives.

ISO/IEC 27005, clause 10.3 Communication and consultation (cont'd)

ISO/IEC 27001:2022, 6.1.2 c) 2), requires that owners of the information security risks be identified. Risk ownership can be deliberately confused or concealed. Even when risk owners can be identified, they can be reluctant to acknowledge that they are responsible for the risks that they own, and obtaining their participation in the risk management process can be difficult. There should be a defined communication procedure for informing those concerned about risk ownership.

ISO/IEC 27001:2022, 6.1.3 f), requires the risk owners to approve the risk treatment plan(s) and to decide on the acceptance of residual risks. Communication between risk owners and staff responsible for the implementation of the ISMS is an important activity. There should be an agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners, and perhaps other interested parties and decision-makers. The information includes, but is not limited to, the existence, nature, form, likelihood, significance, treatment and acceptance of risks. Communication should be bi-directional.

An organization should develop risk communication plans for normal operations as well as for emergencies. The risk communication and consultation activity should be performed continually.



ISO/IEC 27005, clause 10.4.1 General

ISO/IEC 27001 specifies requirements for organizations to retain documented information concerning the risk assessment process and results; the risk treatment process and results.

ISO/IEC 27005, clause 10.4.2 Documented information about processes

Documented information about the information security risk assessment process should contain:

a. *a definition of the risk criteria (including the risk acceptance criteria and the criteria for performing information security risk assessments);*
b. *reasoning for the consistency, validity and comparability of results;*
c. *a description of the risk identification method (including the identification of risk owners);*
d. *a description of the method for analyzing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk);*
e. *a description of the method for comparing the results with the risk criteria and the prioritization of risks for risk treatment.*

Documented information about the information security risk treatment process should contain descriptions of:

- *the method for selecting appropriate information security risk treatment options;*
- *the method for determining necessary controls;*
- *how ISO/IEC 27001:2022, Annex A, is used to determine that necessary controls have not been inadvertently overlooked;*
- *how risk treatment plans are produced;*
- *how risk owners' approval is obtained.*

Slide Notes Extension

ISO/IEC 27005, clause 10.4.3 Documented information about results

As organizations are required to perform risk assessments at planned intervals or when significant changes are proposed or occur, there should at least be evidence of a schedule, and risk assessments being performed in accordance with that schedule. If a change is proposed, or has occurred, then there should be evidence of the performance of an associated risk assessment. Otherwise, the organization should explain why the change is significant or not.

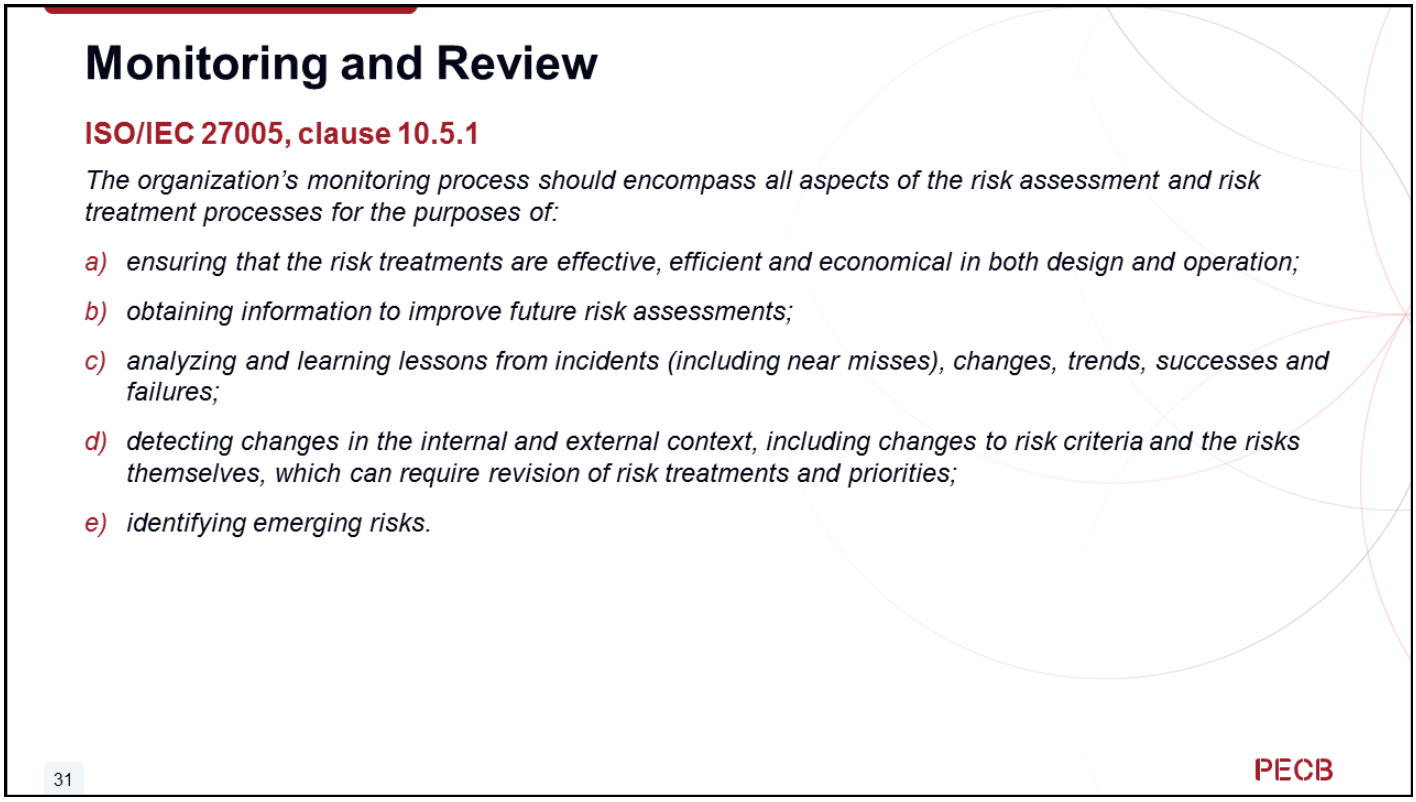
Documented information about the information security risk assessment results should contain:

a. *the identified risks, their consequence and likelihood;*
b. *the identity of the risk owner(s);*
c. *the results of applying the risk acceptance criteria;*
d. *the priority for risk treatment.*

Recording of the rationale for risk decisions is also recommended, in order to both learn from error in individual cases and facilitate continual improvement.

Documented information about the information security risk treatment results should contain:

- *identification of the necessary controls;*
- *where appropriate and available, evidence that these necessary controls act to modify risks, so as to meet the organization's risk acceptance criteria.*



ISO 31000, clause 6.6 Monitoring and review (cont'd)

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analyzing information, recording results and providing feedback.

The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

ISO/IEC 27005, clause 10.5.2 Monitoring and reviewing factors influencing risks

Risks are not static. Event scenarios, asset values, threats, vulnerabilities, likelihoods and consequences can change abruptly without any indication. Constant monitoring should be carried out to detect these changes. This can be supported by external services that provide information regarding new threats or vulnerabilities. Organizations should ensure the continual monitoring of relevant factors, such as:

a. *new sources of risk, including freshly reported vulnerabilities in IT;*
b. *new assets that have been included in the risk management scope;*
c. *necessary modification of asset values (e.g. due to changed business requirements);*
d. *identified vulnerabilities to determine those becoming exposed to new or re-emerging threats;*
e. *changes in patterns of use of existing or new technologies that can open up new possible opportunities for attack;*
f. *changes in laws and regulations;*
g. *changes in risk appetite and perceptions of what is now acceptable and what is no longer acceptable;*
h. *information security incidents, both inside and outside of the organization.*

Information Security Objectives

ISO/IEC 27001:2022, clause 6.2

The organization shall establish information security objectives at relevant functions and levels. The organization shall retain documented information on the information security objectives.

The information security objectives shall:

a) *be consistent with the information security policy;*

b) *be measurable (if practicable);*

c) *take into account applicable information security requirements, and results from risk assessment and risk treatment;*

d) *be communicated; and*

e) *be updated as appropriate.*

When planning how to achieve its information security objectives, the organization shall determine:

f) *what will be done;*

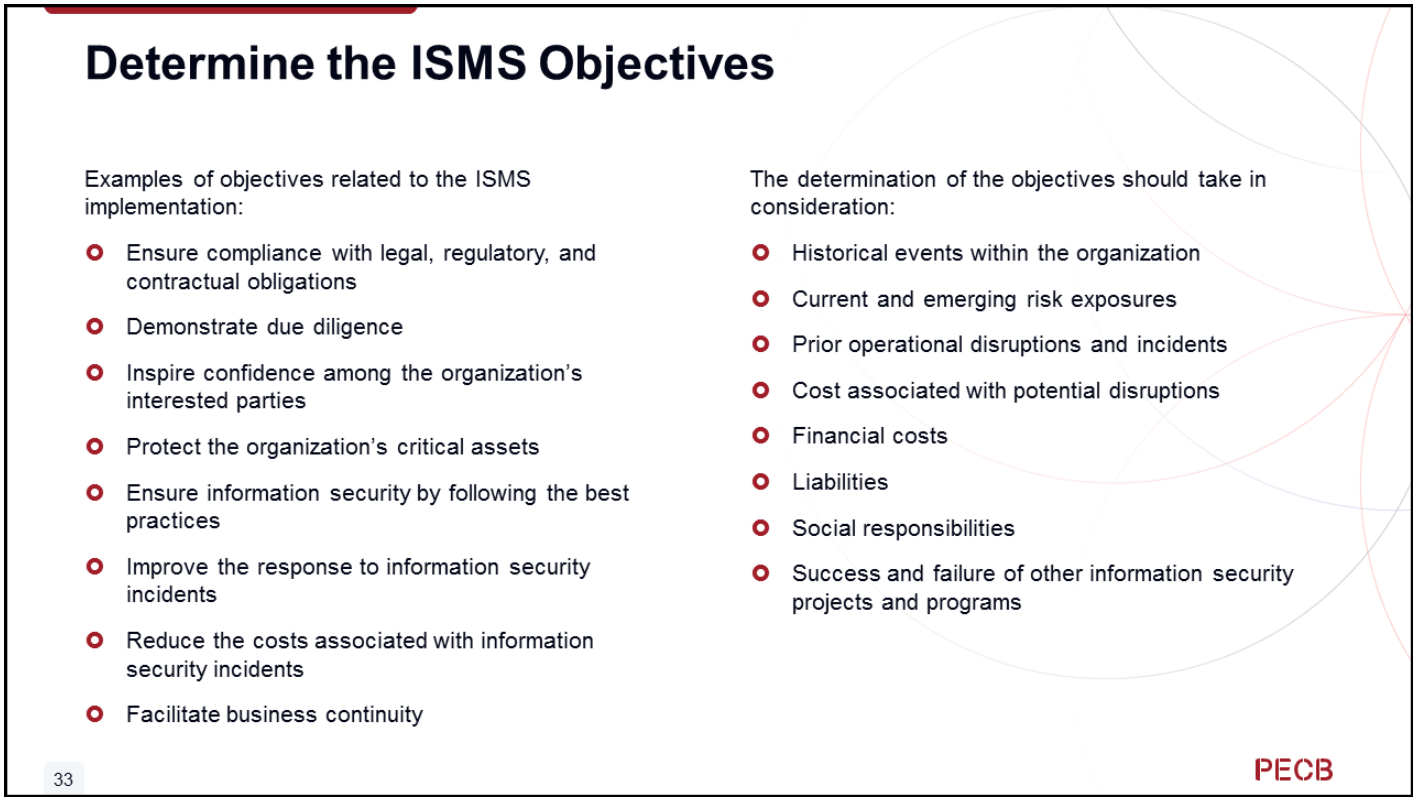
g) *what resources will be required;*

h) *who will be responsible;*

i) *when it will be completed; and*

j) *how the results will be evaluated.*

PECB



The determination of the objectives should take in consideration:

- Historical events within the organization
- Current and emerging risk exposures
- Prior operational disruptions and incidents
- Cost associated with potential disruptions
- Financial costs
- Liabilities
- Social responsibilities
- Success and failure of other information security projects and programs

Section 7 Summary

- ISO 31000 underlines the importance of integrating risk management in the organization's processes, activities, or systems.
- PECB risk management process includes the context establishment, risk assessment, risk treatment, risk acceptance, communication and consultation, recording and reporting, and monitoring and review.
- Risk assessment includes risk identification, analysis, and evaluation.
- Risk identification aims to find, recognize, and describe risks that might help or prevent an organization achieving its objectives.
- Risk analysis aims to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.
- Risk evaluation aims to compare the results of risk analysis with risk criteria to determine whether the risk or its magnitude is acceptable or tolerable.
- Risk treatment options include risk modification, risk retention, risk avoidance, and risk sharing.
- Risk acceptance is defined as the informed decision to take a particular risk.

Questions?

Quiz 4

Note: To complete Quiz 4, please go to the Quizzes Worksheet.

This section provides information that will help the participant gain knowledge on resource management, training, competence, awareness, communication, and ISMS documented information.

Resources

ISO/IEC 27001:2022, clause 7.1

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

36

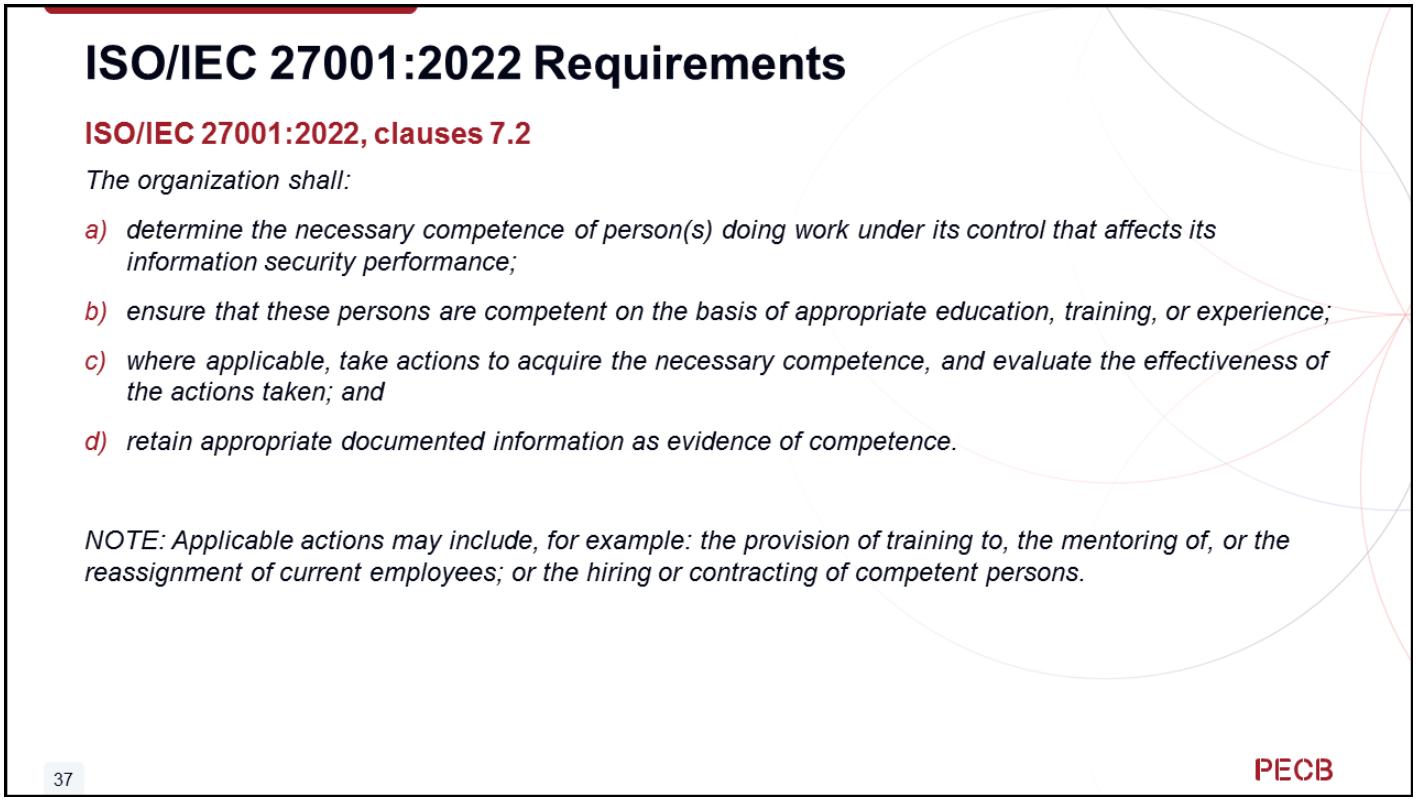
PECB

ISO/IEC 27003, clause 7.1 Resources

Resources are fundamental to perform any kind of activity. Categories of resources can include:

a. *persons to drive and operate the activities;*
b. *time to perform activities and time to allow results to settle down before making a new step;*
c. *financial resources to acquire, develop and implement what is needed;*
d. *information to support decisions, measure performance of actions, and improve knowledge; and*
e. *infrastructure and other means that can be acquired or built, such as technology, tools and materials, regardless of whether they are products of information technology or not.*

These resources are to be kept aligned with the needs of the ISMS and hence are to be adapted when required.



An organization wishing to conform to the requirements of ISO/IEC 27001:2022 should:

1. Identify the skills that its employees need to ensure the proper functioning of the ISMS
2. Provide a training program for the employees that are directly or indirectly involved in the implementation of the ISMS
3. Provide an awareness program on information security appropriate to the different interested parties
4. Provide a communication program to inform all interested parties about the ISMS and the changes that may affect them
5. Evaluate the effectiveness of the actions taken and keep records

ISO/IEC 27003, clause 7.2 Competence

Guidance

The organization should:

a. *determine the expected competence for each role within the ISMS and decide if it needs to be documented (e.g. in a job description);*
b. *assign the roles within the ISMS to persons with the required competence either by:*
    1. *identifying persons within the organization who have the competence (based e.g. on their education, experience, or certifications);*
    2. *planning and implementing actions to have persons within the organization obtain the competence (e.g. through provision of training, mentoring, reassignment of current employees); or*
    3. *engaging new persons who have the competence (e.g. through hiring or contracting);*
c. *evaluate the effectiveness of actions in b) above;*
d. *verify that the persons are competent for their roles; and*
e. *ensure that the competence evolves over time as necessary and that it meets expectations.*

ISO/IEC 27001:2022 Requirements

ISO/IEC 27001:2022, clause 7.3

Persons doing work under the organization's control shall be aware of:

- *the information security policy;*
- *their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and*
- *the implications of not conforming with the information security management system requirements.*

38

PECB

ISO/IEC 27003, clause 7.3 Awareness

The organization should:

a. *prepare a program with the specific messages focused on each audience (e.g. internal and external persons);*
b. *include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts;*
c. *prepare a plan to communicate messages at planned intervals;*
d. *verify the knowledge and understanding of messages both at the end of an awareness session and at random between sessions; and*
e. *verify whether persons act according to the communicated messages and use examples of 'good' and 'bad' behavior to reinforce the message.*

Ensure Resource Management

To ensure the maintenance and continual improvement of the information security management system, the organization must allocate sufficient resources for its operation.

Note: The allocation of resources for the operation of the ISMS depends on the business case.

39

PECB

ISO/IEC 27021, clause 5.9 Competence: Resource management

Intended outcome

Ensuring that appropriate resources are determined and provided in time for the establishment, implementation, maintenance and continual improvement of the ISMS

Knowledge required

- *Financial reporting and measurement*
- *Budget creation and management techniques*
- *Cost management and reduction techniques*
- *Time and materials management techniques*
- *Management review and corrective action processes*

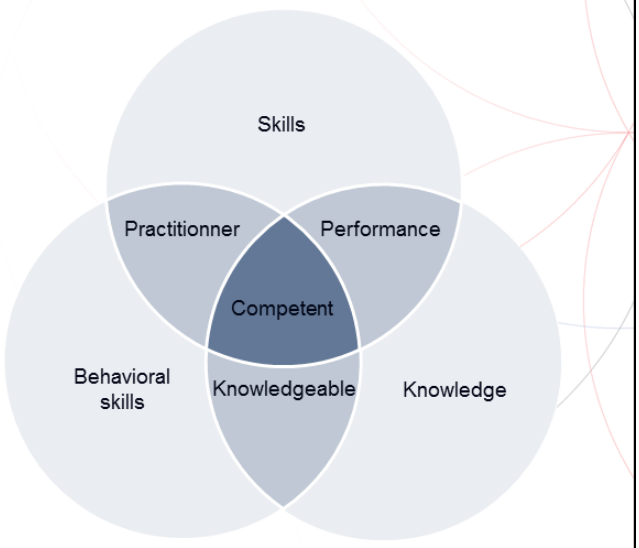
Skills required

- *Determine the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS*
- *Budget business elements including cost of implementation and operation of the ISMS*
- *Understand financial reporting, including cash flow and profit and loss*
- *Create business and investment cases*
- *State ROI (return on investment), ROSI (return on security investment) and other financial benefits*
- *Apply cost control and budget management techniques*
- *Provide appropriate resources in time in the right place*

Competence and People Development

ISO 9000, clause 3.10.4 and ISO 10015, clause 3.2

- ***Competence*** *– Ability to apply knowledge and skills to achieve intended results*
- ***People development*** *– Encouragement of employees to acquire new or advanced competence by creating learning and training opportunities with circumstances to deploy the outcomes that have been acquired*



40

PECB

A systematic and planned training program can help the organization increase its capability and conform to its information security objectives.

ISO 10015, clause 5.4.1

Teams, groups and individuals should be encouraged to engage in competence management and people development planning activities to increase engagement and ownership.

Training, Awareness, and Communication

Differences

1. **Training** – The aim of a training program is to help an individual acquire the knowledge, skills, and behavior required to meet specific requirements.

2. **Awareness** – The aim of an awareness session is to raise and promote awareness among the target audience regarding a concern and possibly a change in their approach and behavior.

3. **Communication** – The aim of communication is to inform the concerned parties about a given subject.

PECB

Awareness Program

An awareness program allows the organization to:

- Raise awareness regarding information security threats and how to protect from potential risks
- Ensure consistency in information security practices
- Contribute to the dissemination and implementation of its policies, guidelines, and procedures

42

PECB

The technological factor is one of the key parameters in the process of providing a functional management system. However, the “human” factor is equally important in ensuring its effectiveness. Humans can be as big a weakness as they are a strength. Thus, they require considerable attention. The staff should know and understand what their responsibilities are, how they can contribute to the effectiveness of the information security management system, and how they can positively affect the business.

An employee who is neither aware nor trained represents a potential risk.

Regarding the awareness of interested parties, the main objective of an awareness program is to reinforce or modify their behavior and attitudes and encourage them to adhere to the values of the organization.

Competence Management and People Development Activities

ISO 10015, clause 5.4.2

Competence management and people development activities at the team or group level should address:

a) *establishing and delivering team or group training programs;*

b) *developing and providing a range of targeted communications (e.g. newsletters, websites, e-learning);*

c) *attending external conferences, professional forums and networking events;*

d) *liaising with relevant professional or trade bodies;*

e) *providing support structures to share knowledge and skills;*

f) *recruiting to address specific gaps;*

g) *restructuring to utilize competence within the organization in a more effective and focused way.*

43

PECB

ISO 10015, clause 5.4.3

Developing activities at the individual level can include:

a. *individual learning program;*
b. *mentoring, coaching and supervision;*
c. *personal development plans;*
d. *formal study for qualifications;*
e. *attending external conferences, etc.;*
f. *training (in the role or function, classroom, online);*
g. *networking events.*

ISO 10015, clause 5.5.1

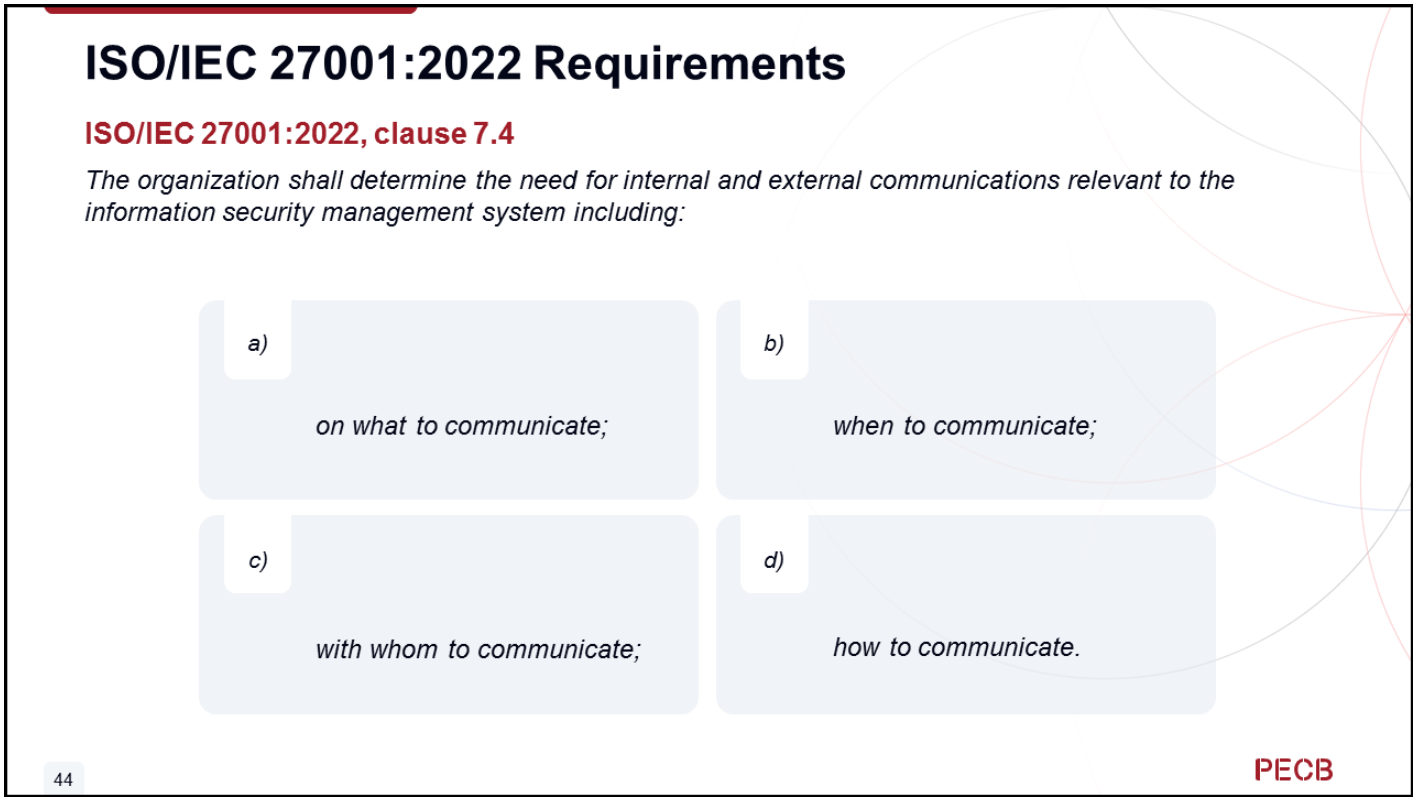
When implementing the development program, the organization should determine and identify the different roles and responsibilities. The organization is responsible for:

a. *determining who will deliver the development program;*
b. *agreeing the scope, purpose and target audience of the development program;*
c. *facilitating the development program by providing the resources required;*
d. *communicating the requirements of the program to relevant interested parties.*

ISO 10015, clause 5.5.2

Those delivering the people development program and its activities are responsible for:

a. *agreeing the people development program;*
b. *ensuring the people development program addresses the relevant competence gaps;*
c. *ensuring activities are suitable for the target audience;*
d. *managing and delivering all parts of the program to the agreed timelines;*
e. *ensuring monitoring and evaluation takes place as agreed.*



An organization wishing to conform to the requirements of ISO/IEC 27001:2022 should:

1. Identify the skills that employees need to ensure the proper functioning of the ISMS
2. Provide a training program for the employees that are involved directly or indirectly in the ISMS implementation
3. Provide an awareness program on information security appropriate to different interested parties
4. Provide a communication program to inform all interested parties about the ISMS and the changes that may affect them
5. Evaluate the effectiveness of actions taken and keep records

ISO/IEC 27003, clause 7.4 Communication

Guidance

Communication relies on processes, channels and protocols. These should be chosen to ensure the communicated message is integrally received, correctly understood and, when relevant, acted upon appropriately. Organizations should determine which content needs to be communicated, such as:

a. *plans and results of risk management to interested parties as needed and appropriate, in the identification, analysis, evaluation, and treatment of the risks;*
b. *information security objectives;*
c. *achieved information security objectives including those that can support their position in the market (e.g. ISO/IEC 27001 certificate granted; claiming conformance with personal data protection laws);*
d. *incidents or crises, where transparency is often key to preserve and increase trust and confidence in the organization's capability to manage its information security and deal with unexpected situations;*
e. *roles, responsibilities and authority;*
f. *information exchanged between functions and roles as required by the ISMS's processes;*
g. *changes to the ISMS;*
h. *other matters identified by reviewing the controls and processes within the scope of the ISMS;*
i. *matters (e.g. incident or crisis notification) that require communication to regulatory bodies or other interested parties; and*
j. *requests or other communications from external parties such as customers, potential customers, users of services and authorities.*

Slide Notes Extension

ISO/IEC 27003, clause 7.4 Communication (cont'd)

The organization should identify the requirements for communication on relevant issues:

k.*who is allowed to communicate externally and internally (e.g. in special cases such as a data breach), allocating to specific roles with the appropriate authority. For example, official communication officers can be defined with the appropriate authority. They could be a public relations officer for external communication and a security officer for internal communication;*

l.*the triggers or frequency of communication (e.g. for communication of an event, the trigger is the identification of the event);*

m.*the contents of messages for key interested parties (e.g. customers, regulators, general public, important internal users) based on high level impact scenarios. Communication can be more effective if based on messages prepared and pre-approved by an appropriate level of management as part of a communication plan, the incident response plan or the business continuity plan;*

n.*the intended recipients of the communication; in some cases, a list should be maintained (e.g. for communicating changes to services or crisis);*

o.*the communication means and channels. Communication should use dedicated means and channels, to make sure that the message is official and bears the appropriate authority. Communication channels should address any needs for the protection of the confidentiality and integrity of the information transmitted; and*

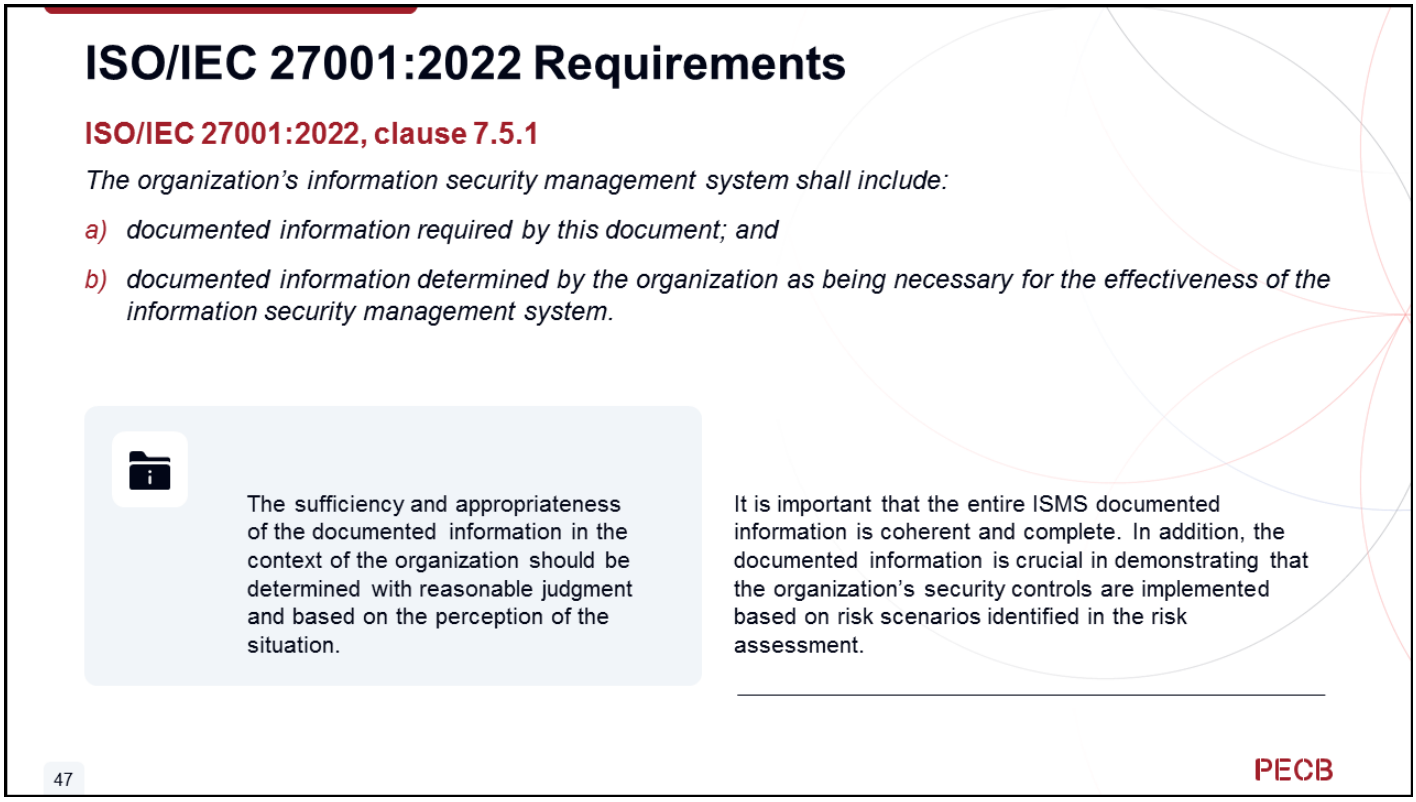
p.*the designed process and the method to ensure messages are sent and have been correctly received and understood.*

Communication should be classified and handled according to the organization's requirements.

Principles of an Efficient Communication Strategy

- **Transparency:** Properly communicate the processes, procedures, methods, data sources, and assumptions used to all interested parties, taking into account the confidentiality of information
- **Appropriateness:** Provide relevant information to interested parties, using formats, language, and media that meet their interests and needs, enabling them to participate fully
- **Credibility:** Conduct communication in an honest and fair manner, and provide information that is truthful, accurate, and substantive; develop information and data using recognized and reproducible methods and indicators
- **Responsiveness:** Respond to the queries and concerns of interested parties in a full and timely manner; make interested parties aware of how their queries and concerns have been addressed
- **Clarity:** Ensure that communication approaches and language are understandable to interested parties in order to avoid ambiguity

PECB



ISO/IEC 27001:2022, clause 7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a. *identification and description (e.g. a title, date, author, or reference number);*
b. *format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and*
c. *review and approval for suitability and adequacy.*

ISO/IEC 27001:2022, clause 7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a. *it is available and suitable for use, where and when it is needed; and*
b. *it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).*
    - *For the control of documented information, the organization shall address the following activities, as applicable:*
c. *distribution, access, retrieval and use;*
d. *storage and preservation, including the preservation of legibility;*
e. *control of changes (e.g. version control); and*
f. *retention and disposition.*

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

Slide Notes Extension

ISO/IEC 27003, clause 7.5.1 General

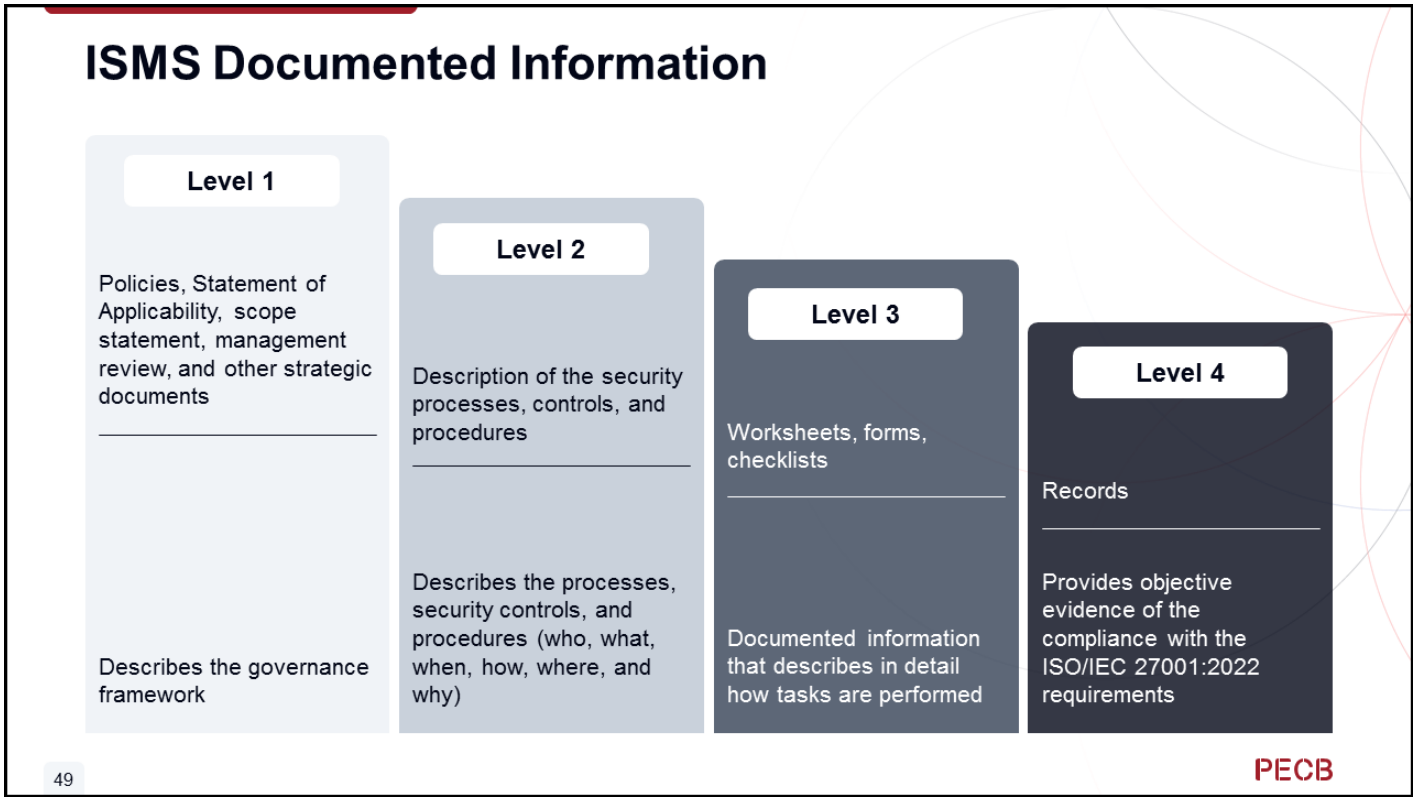
Explanation

Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls.

Guidance

Examples of documented information that can be determined by the organization to be necessary for ensuring effectiveness of its ISMS are:

- *the results of the context establishment;*
- *the roles, responsibilities and authorities;*
- *reports of the different phases of the risk management;*
- *resources determined and provided;*
- *the expected competence;*
- *plans and results of awareness activities;*
- *plans and results of communication activities;*
- *documented information of external origin that is necessary for the ISMS;*
- *process to control documented information;*
- *policies, rules and directives for directing and operating information security activities;*
- *processes and procedures used to implement, maintain and improve the ISMS and the overall information security status;*
- *action plans; and*
- *evidence of the results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).*



There is no mandatory requirement on how to document processes and security controls. This can be done using diagrams, textual descriptions, spreadsheets, etc.

Discussion questions:

1. Explain the difference between training, awareness, and communication.
2. What are the principles of an efficient communication strategy?
3. What are some of the main ISMS documented information?

Section 8 Summary

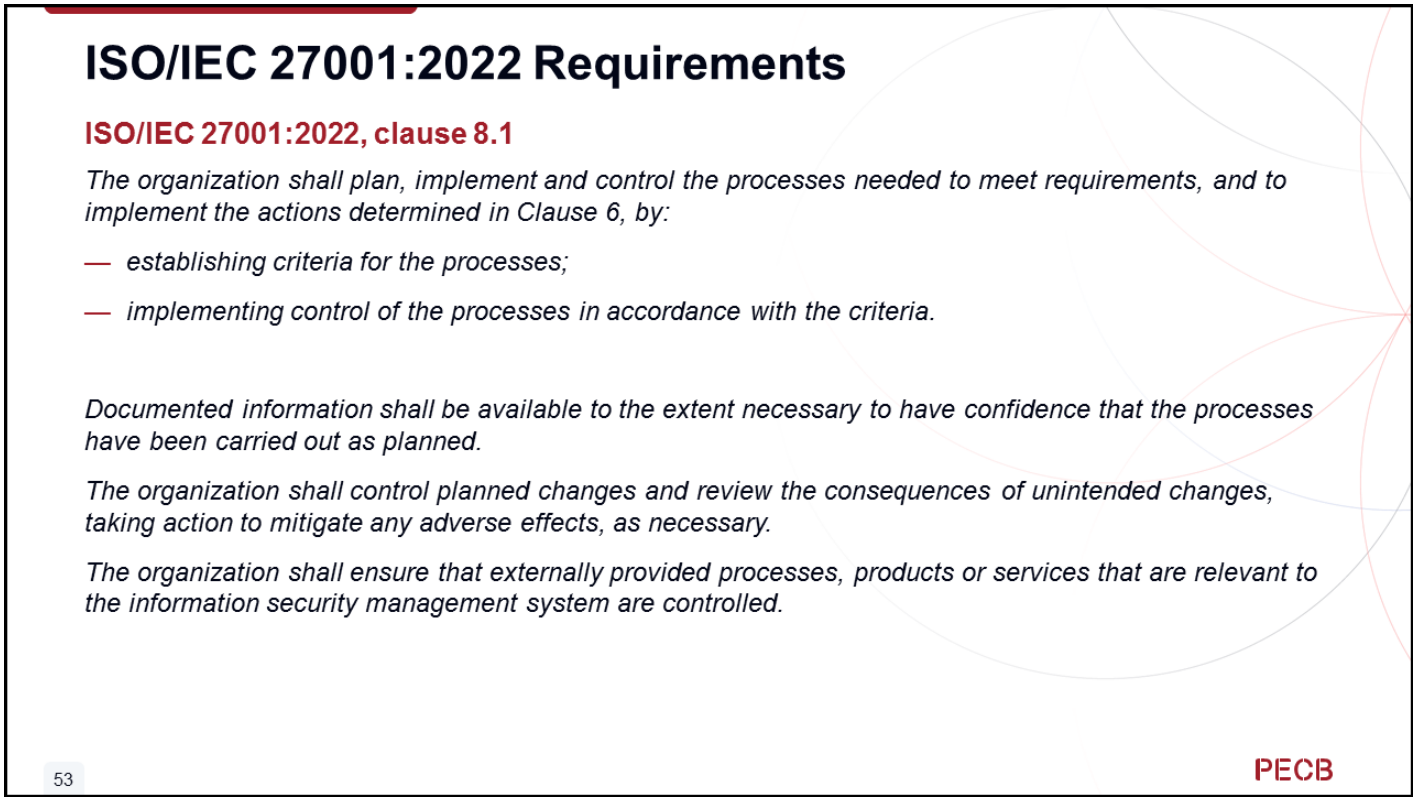
- The organization shall conduct competence development activities such as training and awareness programs for employees whose work affects the ISMS. Such regular activities help organizations conform to the information security objectives.
- Training programs are focused on the skills needed to be acquired, while the awareness programs are focused on changing habits.
- A communication program should provide a transparent, credible, clear, and appropriate communication.
- ISMS documented information is needed to comply with the ISO/IEC 27001:2022 requirements.
- Organizations should develop procedures for the control of documents and records.

Questions?

Quiz 5

Note: To complete Quiz 5, please go to the Quizzes Worksheet.

This section elaborates on operational planning, change management, and the difference between business continuity and disaster recovery.



An organization wishing to conform to the requirements of ISO/IEC 27001:2022 should:

1. Ensure the effective management of operations related to the ISMS
2. Ensure the provision of adequate resources for the effective operation of the ISMS

ISO/IEC 27003, clause 8.1 Operational planning and control

Processes to meet information security requirements include:

a. *ISMS processes (e.g. management review, internal audit); and*
b. *processes required for implementing the information security risk treatment plan.*

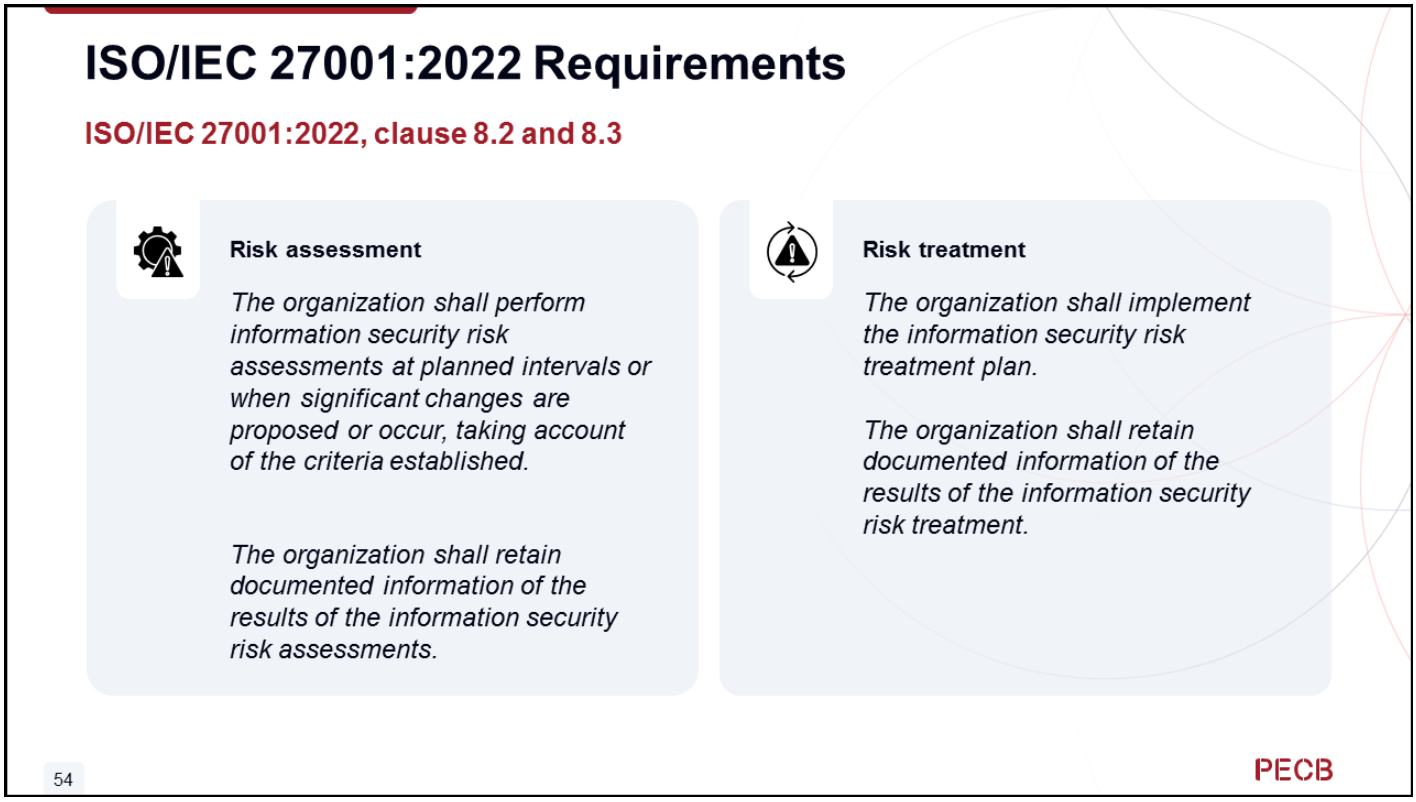
Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

a. *determine outsourced processes considering the information security risks related to the outsourcing; and*
b. *ensure that outsourced processes are controlled (i.e. planned, monitored and reviewed) in a manner that provides assurance that they operate as intended (also considering information security objectives and the information security risk treatment plan).*

If part of the organization's functions or processes are outsourced to suppliers, the organization should:

a. *determine all outsourcing relationships;*
b. *establish appropriate interfaces to the suppliers;*
c. *address information security related issues in the supplier agreements;*
d. *monitor and review the supplier services to ensure that they are operated as intended and associated information security risks meet the risk acceptance criteria of the organization; and*
e. *manage changes to the supplier services as necessary.*



ISO/IEC 27003, clause 8.2 Information security risk assessment

Guidance

Organizations should have a plan for conducting scheduled information security risk assessments.

When any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization should determine:

a. *which of these changes or incidents require an additional information security risk assessment; and*
b. *how these assessments are triggered.*

The level of detail of the risk identification should be refined step by step in further iterations of the information security risk assessment in the context of the continual improvement of the ISMS. A broad information security risk assessment should be performed at least once a year.

ISO/IEC 27003, clause 8.3 Information security risk treatment

Explanation

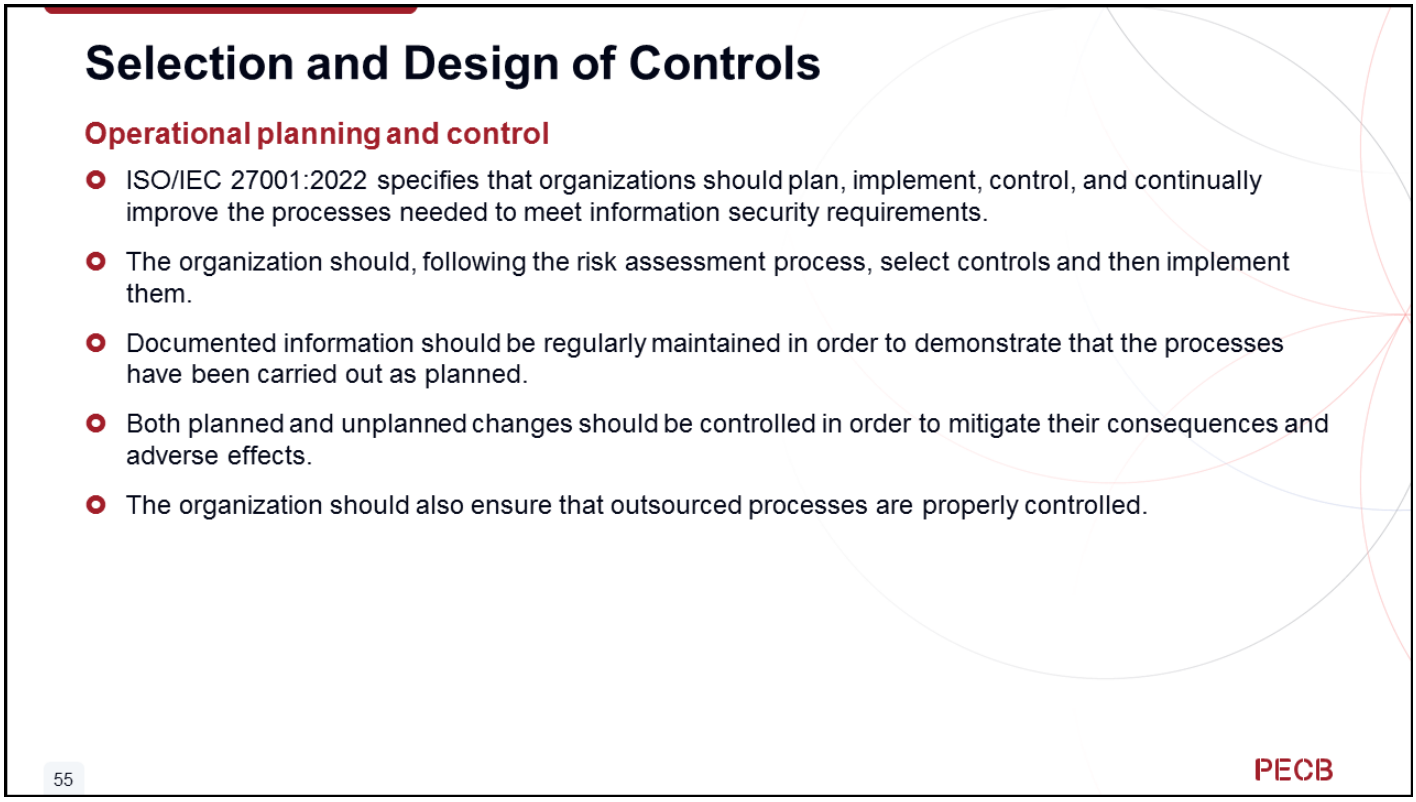
In order to treat information security risks, the organization needs to carry out the information security risk treatment process defined in 6.1.3. During operation of the ISMS, whenever the risk assessment is updated according to 8.2, the organization then applies the risk treatment according to 6.1.3 and updates the risk treatment plan. The updated risk treatment plan is again implemented.

The results of the information security risk treatment are retained in documented information as evidence that the process in 6.1.3 has been performed as defined.

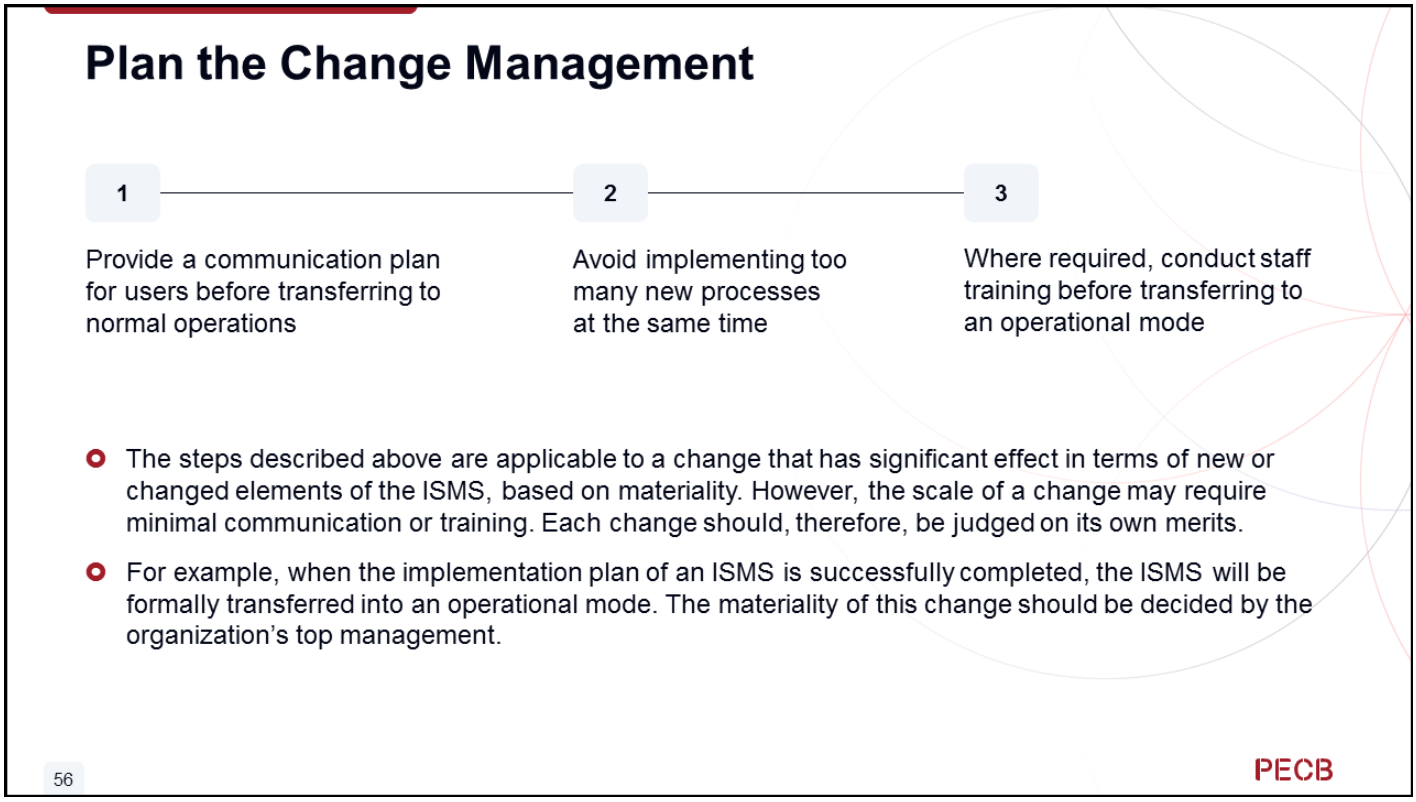
Guidance

The information security risk treatment process should be performed after each iteration of the information security assessment process in 8.2 or when the implementation of the risk treatment plan or parts of it fails.

The progress of implementation of the information security risk treatment plan should be driven and monitored by this activity.

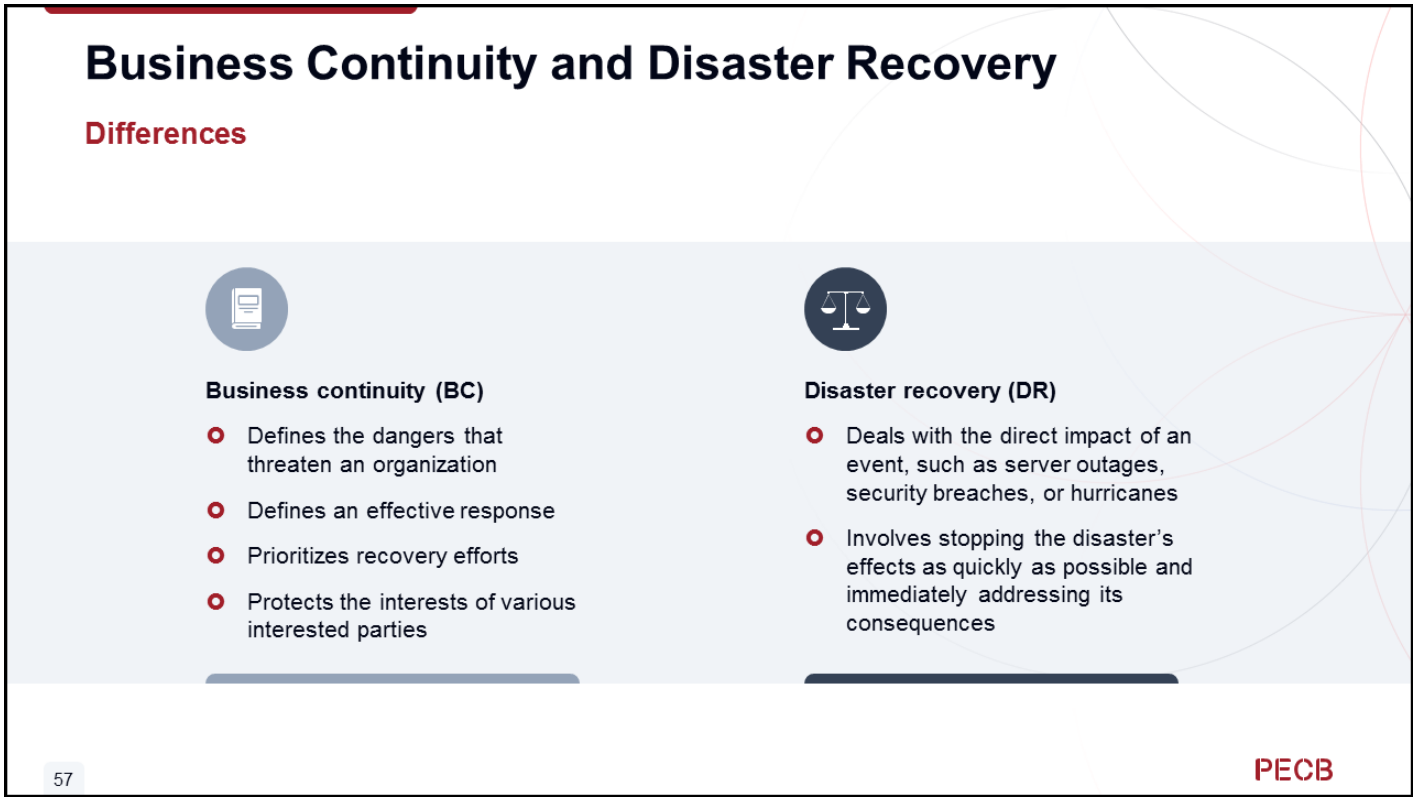


An organization wishing to comply with the requirements of ISO/IEC 27001:2022 shall, at least, implement security controls detailed in the risk treatment plan and those that have been declared applicable in the Statement of Applicability.



ISO/IEC 27001:2022, clause 6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.



At some time during the disaster recovery, business continuity activities begin to overlap. The three following questions, with a primarily focus on continuing businesses operations, are related to business continuity and disaster recovery maintenance cycle (BC/DR):

- Where to set up temporary systems?
- How to acquire replacement systems or parts?
- How to secure the new location?

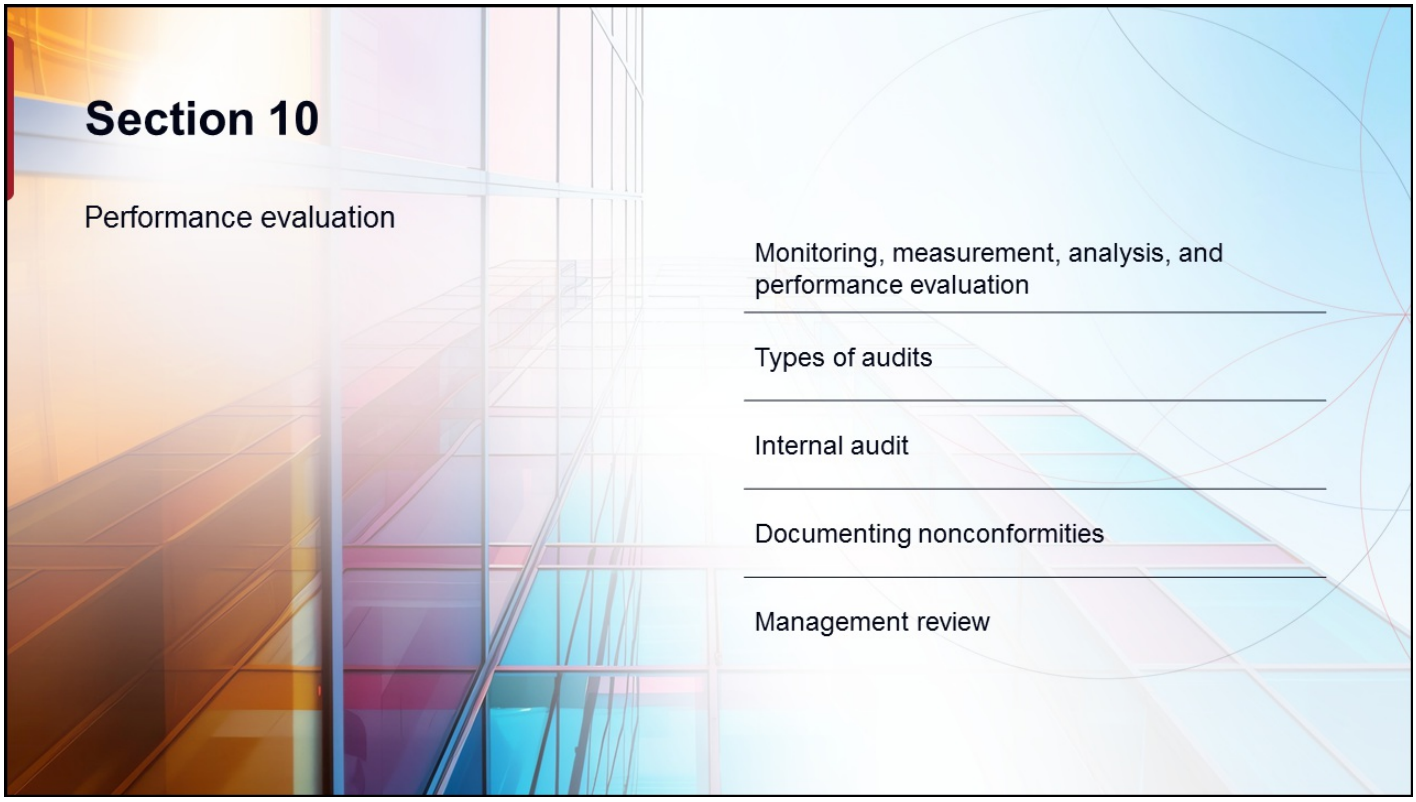
Example: Failover resilience

An organization decides to invest in a "failover" system, meaning that if the server that provides the organization with the data and applications that are used on a daily basis gets damaged and fails, another server will automatically replace the damaged server. Thus, the employees will be capable of immediately continuing their duties. This is considered as a resilience of the IT data, but is provided by a disaster recovery device. Even though disaster recovery is capable of existing on its own, it is an essential component in business continuity management, given that it offers the required resources that facilitate normal business operations.

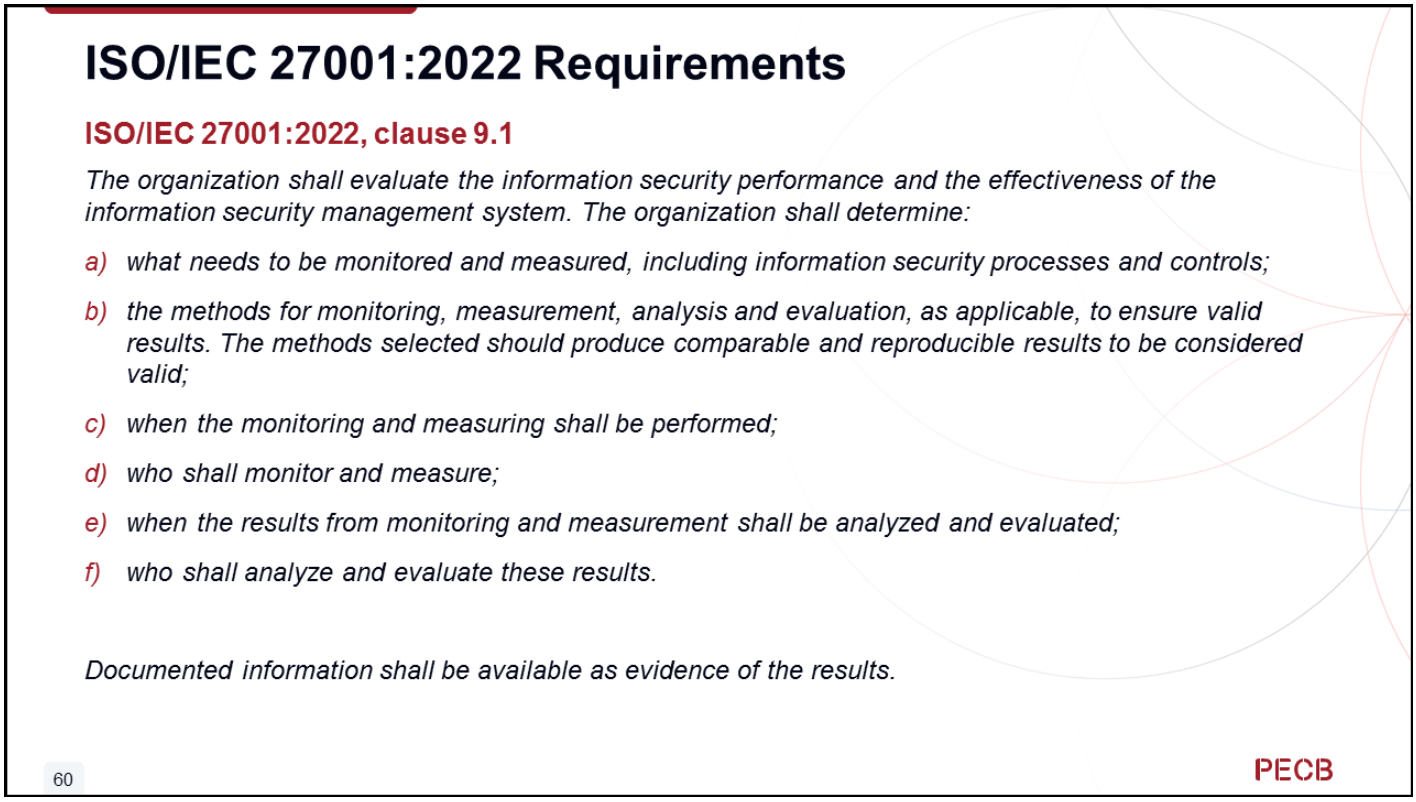
Section 9 Summary

- The key document that describes the control objectives and controls along with their applicability in the organization's ISMS is defined as the Statement of Applicability.
- An organization wishing to comply with the requirements of ISO/IEC 27001:2022 shall perform regular information security risk assessments and implement the information security risk treatment plan.
- According to ISO/IEC 27001:2022, an organization shall plan and implement changes in a planned manner.
- Business continuity defines the disruptions that threaten an organization's capability to deliver its services and products, provides an effective response, and protects the interests of involved parties.
- Disaster recovery deals with the direct impacts of an event.

Questions?



This section aims at providing the participants with information on performance evaluation processes including monitoring, measurement, analysis and evaluation, internal audit, and management review.



An organization wishing to comply with ISO/IEC 27001:2022 shall:

1. Determine what needs to be measured and monitored in the ISMS
2. Define the methods for monitoring, measurement, analysis, and evaluation
3. Gather the data for monitoring, measurement, analysis, and evaluation
4. Perform an analysis and evaluation of results

ISO/IEC 27003, clause 9.1 Monitoring, measurement, analysis and evaluation

A good practice is to define the 'information need' when planning the monitoring, measurement, analysis and evaluation. An information need is usually expressed as a high level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness. In other words, monitoring and measurement should be undertaken to achieve a defined information need.

Care should be taken when determining the attributes to be measured. It is impracticable, costly and counterproductive to measure too many, or the wrong attributes. Besides the costs of measuring, analyzing and evaluating numerous attributes, there is a possibility that key issues could be obscured or missed altogether.

There are two generic types of measurements:

h.*performance measurements*, *which express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls are implemented; and*

i.*effectiveness measurements*, *which express the effect that realization of the planned activities has on the organization's information security objectives.*

Monitoring, Measurement, Analysis, and Performance Evaluation

Measurement is the process of determining a value. Performance measurement can be defined as a systematic way of assessing an organization's current achievements against its objectives.

Monitoring – Process of determining the status of a system, a process, or an activity

Measurement – Process of determining a value

Analysis – Method of examining the nature of something or of determining its essential features and their relations

Performance evaluation – Process of determining measurable results

61

PECB

Performance measures are of little value per se, unless they are viewed within the context of organizational strategies and objectives. This holds true for management systems also, which cannot exist in a vacuum and must contribute to the objectives of the organization if they are to be effective. Measuring performance in this context should be a high priority on the agenda of individuals who are responsible for the implementation and maintenance of the management system.

Some of the advantages of monitoring, measurement, analysis, and evaluation are:

- Implementing a systematic control to ensure the realization of processes
- Identifying deviations on a timely manner and treating them accordingly
- Allowing the users of the ISMS to make decisions regarding process results
- Determining the effectiveness and efficiency of processes
- Identifying opportunities for continual improvement

Define What Needs to be Monitored and Measured

ISO/IEC 27004, clause 6.1

- *In order to determine what to monitor and measure, the organization should first consider what it wishes to achieve in evaluating information security performance and ISMS effectiveness. This can allow it to determine its information needs.*
- *Organizations should next decide what measures are needed to support each discrete information need and what data are required to derive the requisite measures. Hence, measurement should always correspond to the information needs of the organization.*

Examples of indicators to monitor:

- The extent to which the organization's information security objectives are met
- The critical processes, procedures, and functions
- Historical evidence of poor ISMS performance (e.g., nonconformities, near misses, false alarms, failures, incidents)
- Compliance with applicable legal and regulatory requirements, industry best practices
- Corrective and preventive actions used to treat nonconformities

62

PECB

A minimum number of meaningful performance measures are far more preferable than a plethora of measures that do not relate to organizational objectives. Many organizations use the SMART (Specific-Measurable-Attainable-Realistic-Timely) methodology when developing their performance measures.

- **Specific:** Clear and focused to avoid misconception
- **Measurable:** Can be quantified and compared to other data
- **Attainable:** Achievable, reasonable, and acceptable in a particular context
- **Realistic:** Fits into the organization's culture and is cost-effective within the available resources
- **Timely:** Achievable within the set time frame

No singular set of generic measures will be effective for all organizations, and may not even be effective for organizations in similar environments. The final mix of measures will be a product of operational, legislative, and cultural context.

There are a number of performance measurement levels ranging from strategic high-level measures to more specific operational-or program-level measures. It is crucial for an organization to measure the activities that truly matter, and not waste time and resources on measuring activities simply because they can be measured. In terms of efficiency, an organization needs meaningful measures that will indicate what is really happening so that it can decide to either let an activity continue or intervene to take corrective action. In terms of effectiveness, an organization needs measures to understand if the management system is aligned with the organization's needs and objectives.

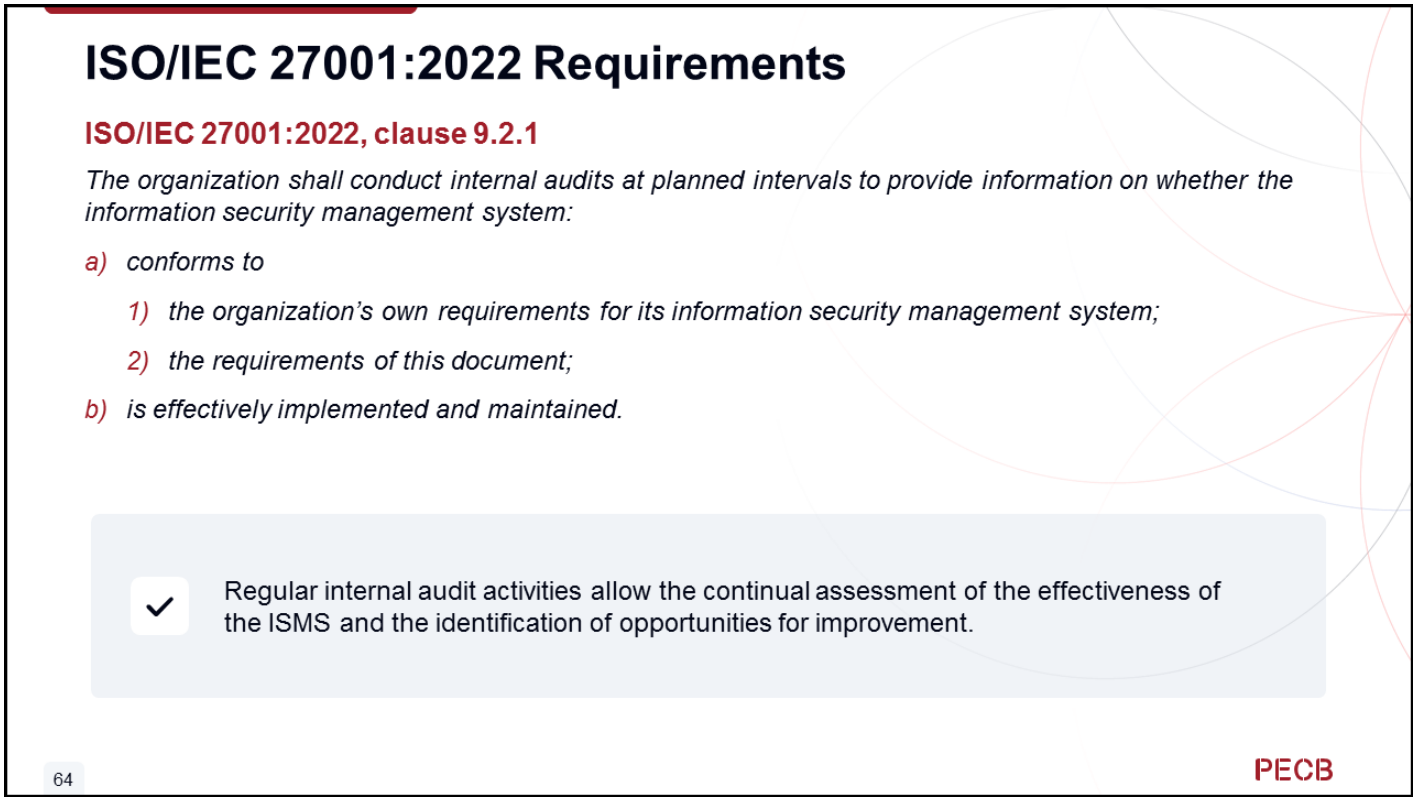
Determine the Frequency and Method of Monitoring and Measurement

How and when to monitor and measure?

Practices

- ISO/IEC 27001:2022 does not indicate how, nor how often, must monitoring and measurement be performed.
- It is up to the organization to determine how and how often to monitor or measure.
- It is best practice to use dashboards to record and report on monitoring and measurement activities with performance indicators.
- Dashboards should indicate actual performance vs. predetermined performance targets.

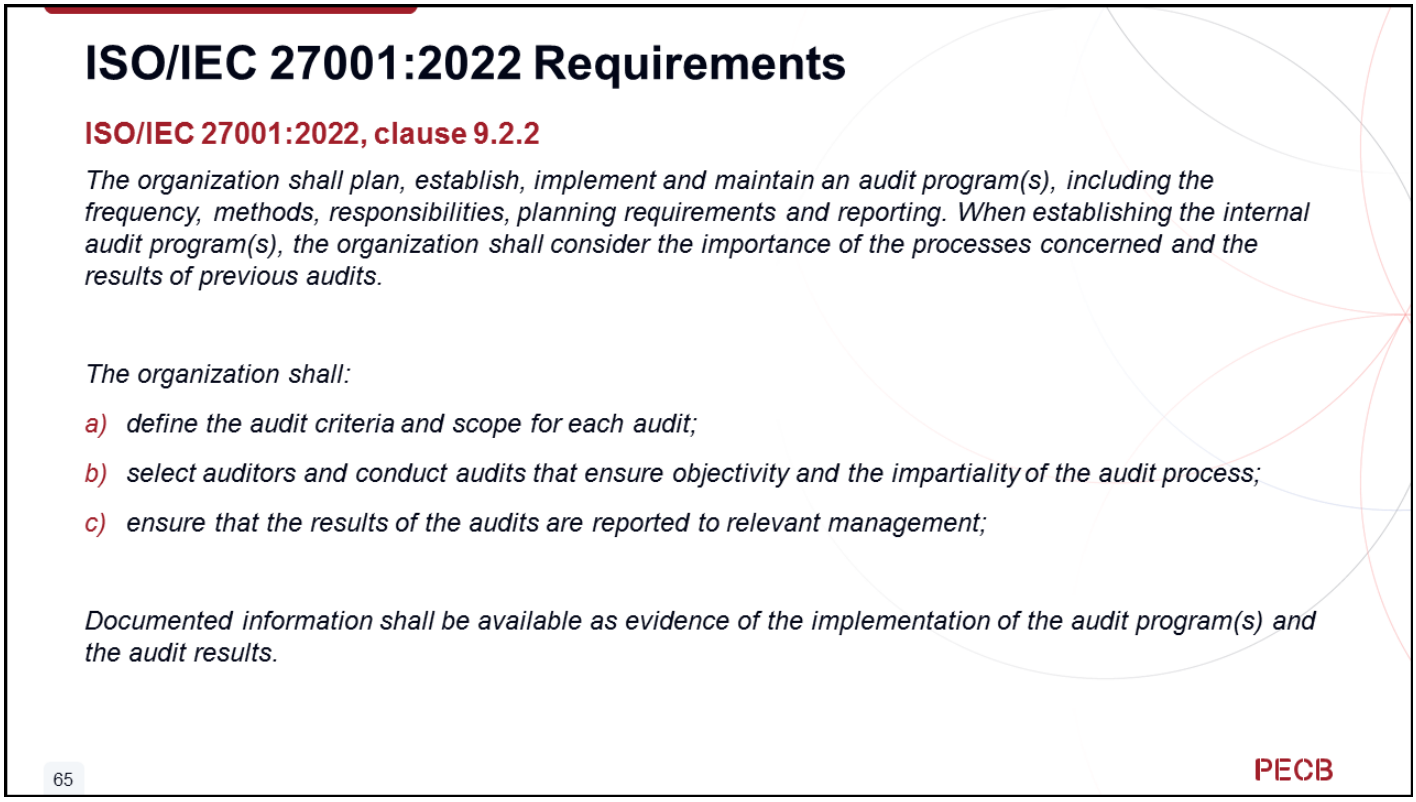
PECB



An organization wishing to comply with ISO/IEC 27001:2022 shall at least:

1. Conduct internal audits
2. Ensure the independence, objectivity, and impartiality of the audit function
3. Plan and perform audit activities

The objective of internal audits is to assess the extent to which an organization has fulfilled the requirements of the standard. Conducting internal audits regularly allows for the continual assessment of the effectiveness of the ISMS and the identification of opportunities for improvement.



ISO/IEC 27003, clause 9.2 Internal audit

Auditors also evaluate whether the ISMS is effectively implemented and maintained. An audit program describes the overall framework for a set of audits, planned for specific time frames and directed towards specific purposes. This is different from an audit plan, which describes the activities and arrangements for a specific audit. Audit criteria are a set of policies, procedures or requirements used as a reference against which audit evidence is compared, i.e. the audit criteria describe what the auditor expects to be in place.

If the outcome of the audit includes nonconformities, the auditee should prepare an action plan for each nonconformity to be agreed with the audit team leader. A follow-up action plan typically includes:

i.*description of the detected nonconformity;*

j.*description of the cause(s) of nonconformity;*

k.*description of short term correction and longer term corrective action to eliminate a detected nonconformity within a defined timeframe; and*

l.*the persons responsible for implementing the plan.*

Audit reports, with audit results, should be distributed to top management.

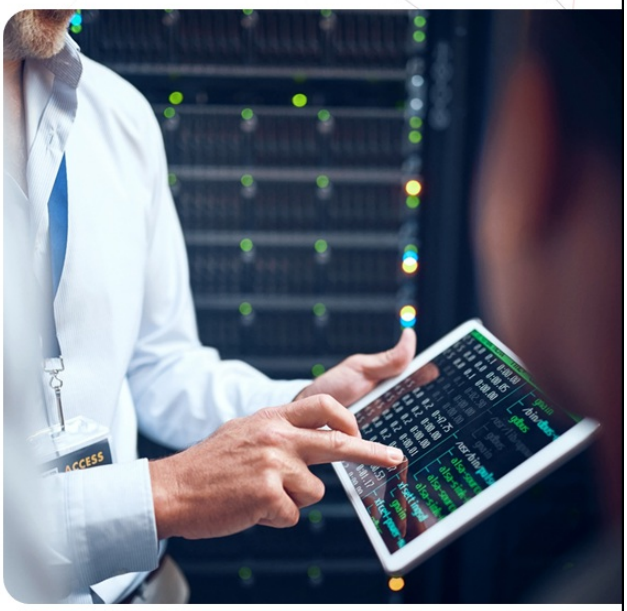
Results of the previous audits should be reviewed and the audit program adjusted to better manage areas experiencing higher risks due to nonconformity.

What Is an Audit?

ISO 19011, clause 3.1

Definition: *Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled*

Simply put, auditing means asking the auditee what they do and how they do it, in order to check whether the practices are in compliance with the organization's policies, procedures, and processes



66

PECB

An audit is an assessment based on evidence and facts. This assessment points out the strengths and weaknesses of the audited organization or the audited system. Audit results are then communicated to the management, who then undertake the required and appropriate measures. The same principles and techniques apply to management system audits.

- A **financial audit** determines whether an organization's accounting practices comply with legal requirements and recognized principles.
- An **administrative audit** determines the effectiveness of the overall administrative practices.
- An **information security** audit determines if the information assets are protected appropriately.

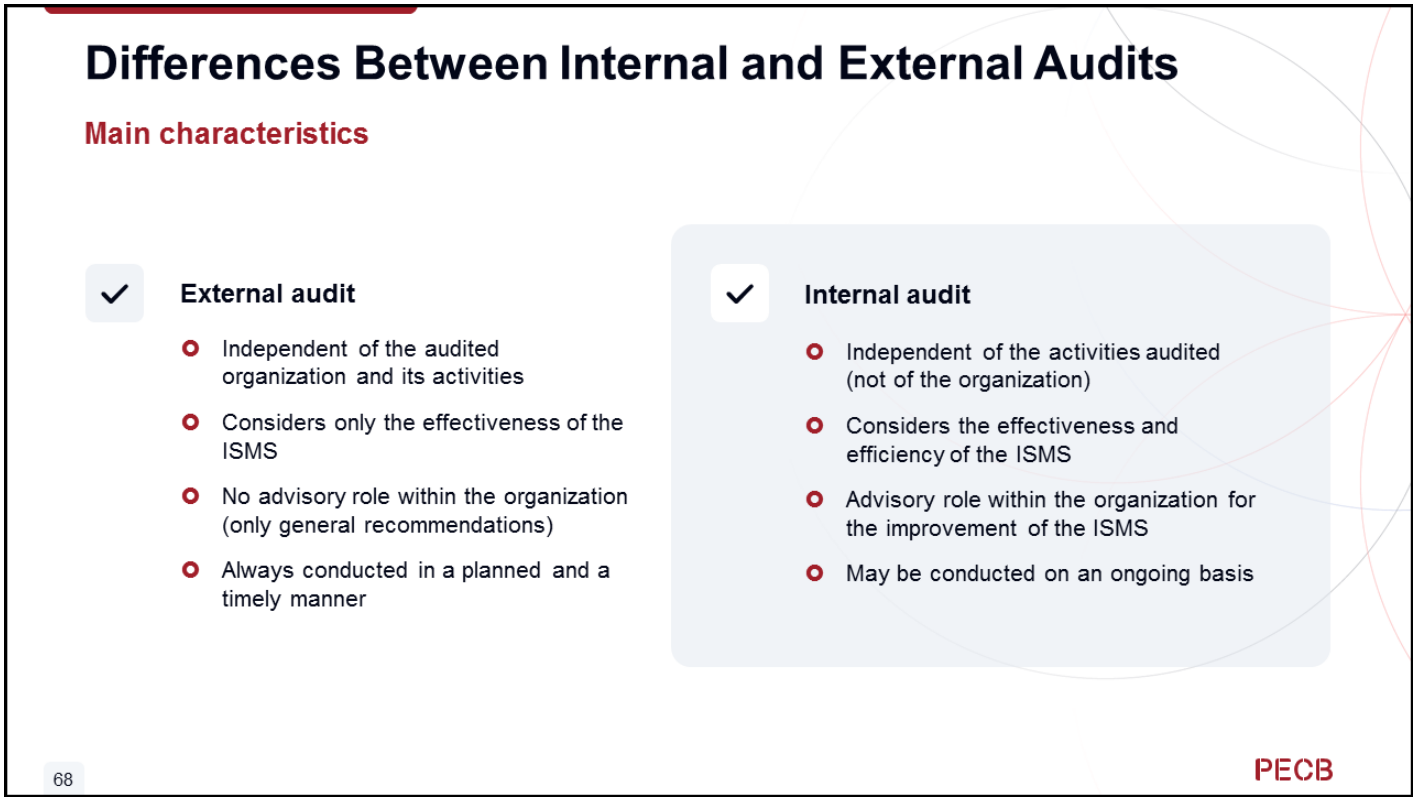
Internal audits:

The internal audit, also known as the **first party audit**, is an independent and objective activity that gives the organization an assurance on the level of control over operations, gives recommendations to improve operations, and contributes to creating added value. Internal audits are conducted by or for the organization itself for the purpose of management reviews and other internal needs. Independence must be demonstrated by the absence of responsibility in the activities to be audited.

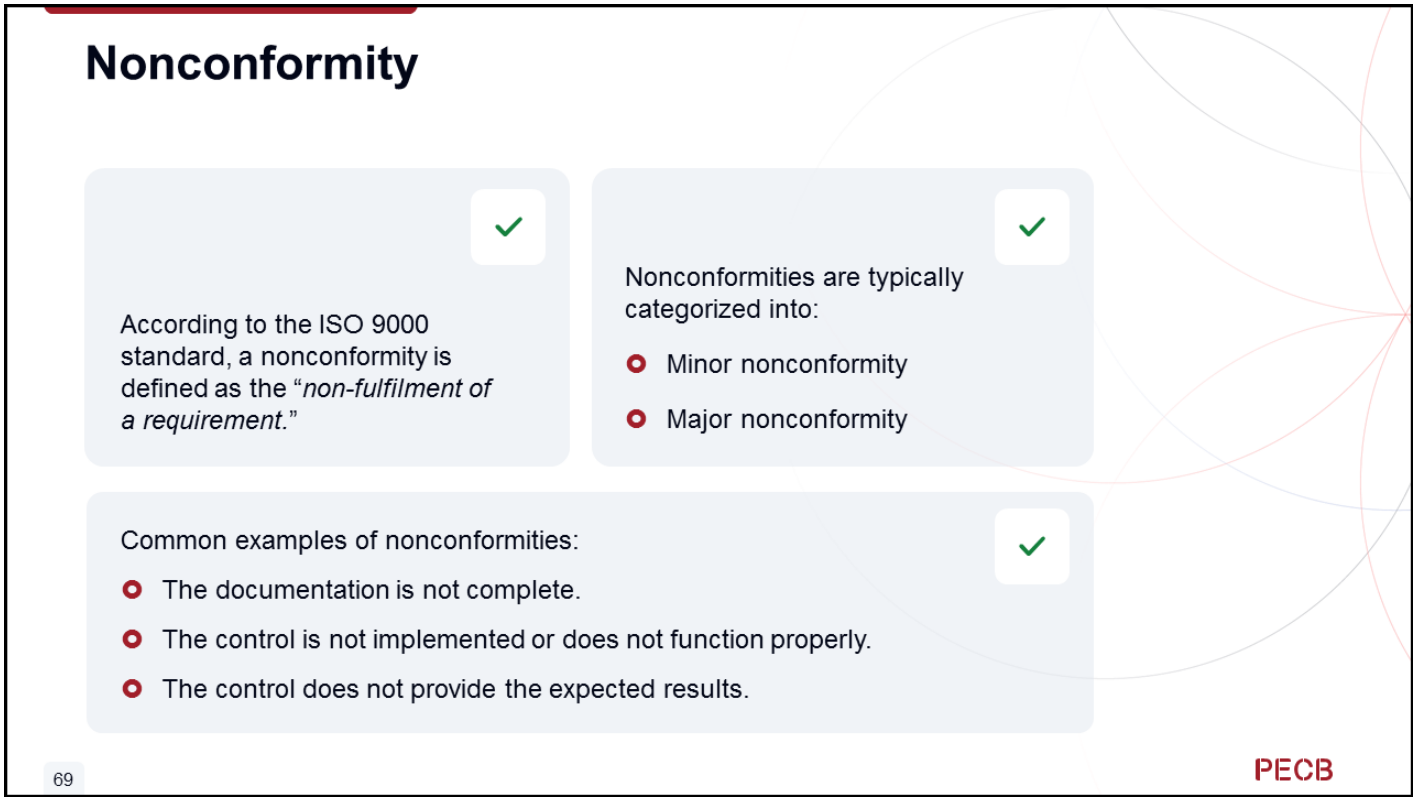
External audits include audits known as second and third party audits:

- **Second party audits** are conducted by parties that have an interest in the audited organization such as customers or other individuals acting on their behalf.
- **Third party audits** are conducted by external and independent audit organizations such as those providing certification and registration of conformity or governmental agencies.

Important note: Third party audits are performed by auditors who are external to and independent of the auditee.



Internal auditing is an independent, objective, and advisory activity designed to upgrade and improve the organization's functions. It also contributes to the objectives of the organization by providing a systematic and structured methodology to evaluate and improve the effectiveness of the risk management process, its control, and decision-making.



Requirements can originate from several sources; they can be specified in a standard, be part of an internal requirement of the organization, originate from a law or regulation, or be part of a contract signed with a client or partner.

ISO 9000, clause 3.6.9 Nonconformity

Non-fulfilment of a requirement

ISO 9000, clause 3.6.11 Conformity

Fulfilment of a requirement

Document the Nonconformities

Once the nonconformity has been identified, the auditor must document it. The recording of this nonconformity can be as simple as a description of the observation and the reference to the appropriate clause.

The adequate documentation of a nonconformity includes:

- Valid evidence supporting the findings
- Description of the requirements for which the nonconformity was detected (audit criteria)
- Nonconformity report

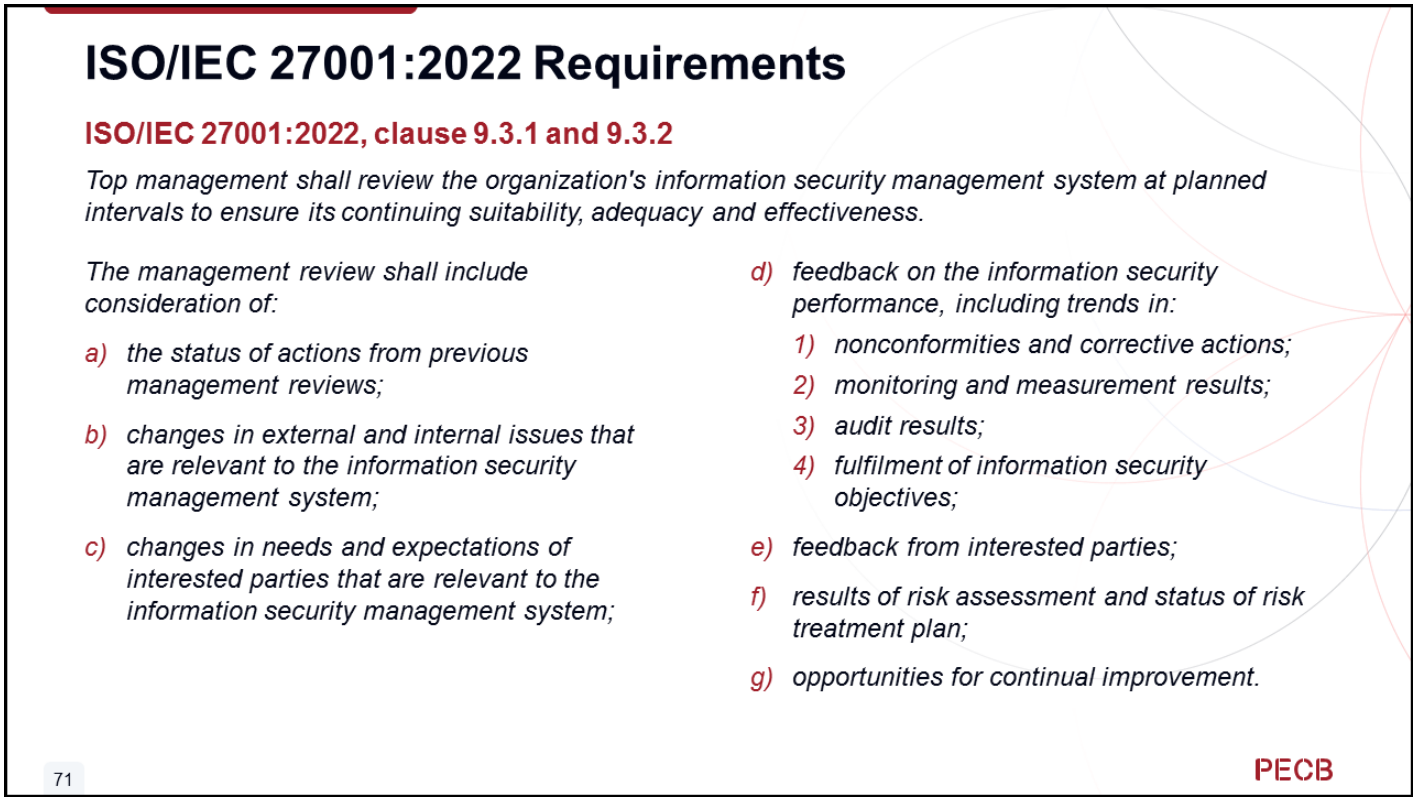
70

PECB

It is to be noted that ISO/IEC 27001:2022 contains several clauses that include more than one requirement. It is important that the auditor documents the specific conditions of the nonconformity (e.g., by writing the exact text and requirement associated to the audit criteria).

A nonconformity report should be:

- Explicit and related to an ISMS requirement
- Unambiguous, linguistically correct, and as concise as possible



ISO/IEC 27001:2022, clause 9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

An organization wishing to comply with ISO/IEC 27001:2022 shall at least perform regular management reviews at scheduled intervals and maintain records.

Management Review

Definition

A management review is a periodic review of the management system performed by the top management to analyze the system's continuing suitability, adequacy, and effectiveness.

Suitable

Results are achieved in the best possible way

Adequate

Outputs fulfill established criteria

Effective

The system fulfills the organization's needs

PECB

Prepare the Management Review

Management reviews must be conducted at planned intervals. They can be included in a management meeting and be a topic on the agenda.

It is good practice to send all documentation related to the management committee (audit report, results of reviews, action plans) before the review.

There is no specific requirement for frequency of management review meetings. The common practice is quarterly meetings. With annual meetings, the organization may not be able to prevent or resolve issues in a timely manner.

PECB

Section 10 Summary

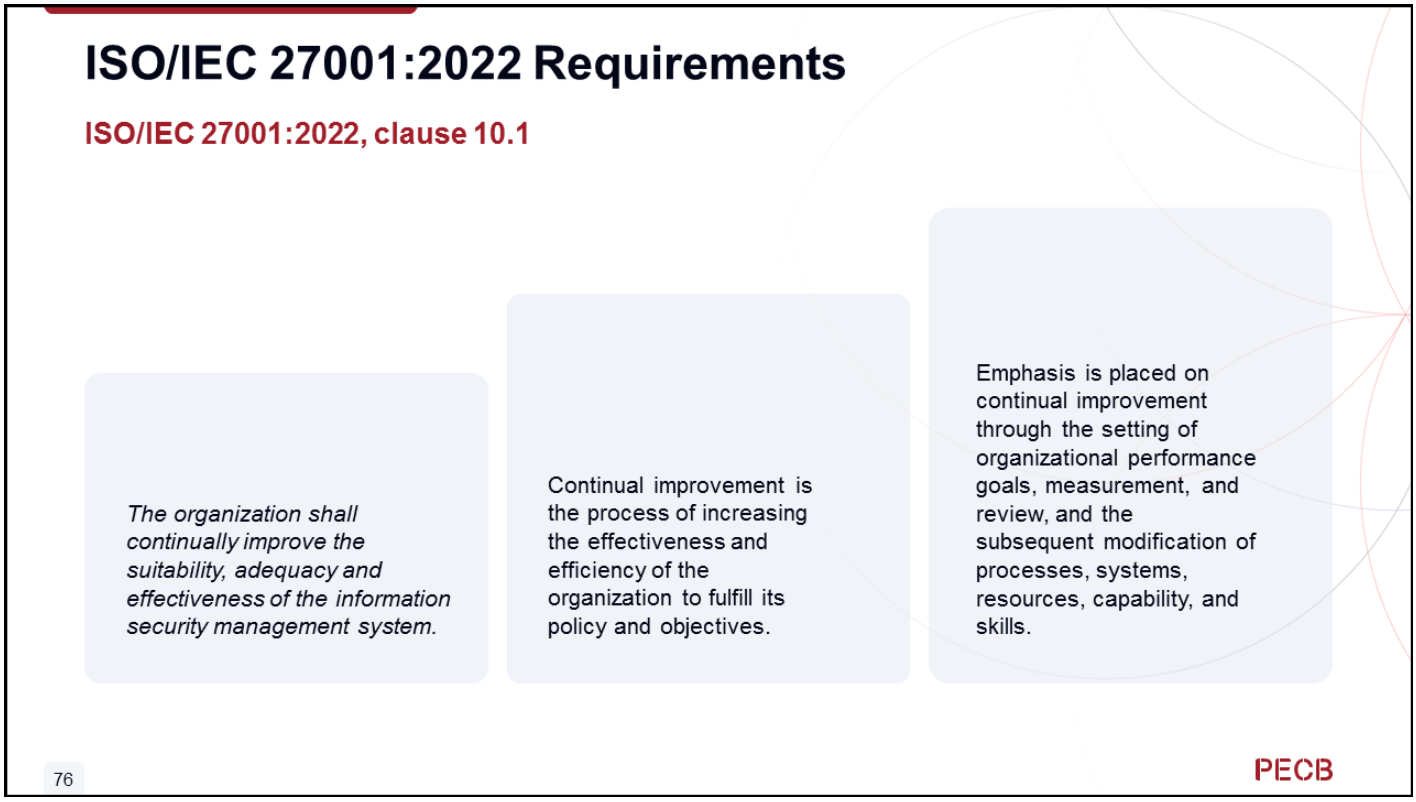
- Monitoring, measurement, analysis, and evaluation aim to improve the ISMS.
- The organization should determine how and how often to monitor or measure the ISMS.
- Internal audits help organizations evaluate if their ISMS is effectively implemented and maintained, as well as their compliance with the ISO/IEC 27001:2022 requirements.
- Internal audit is a type of audit where organizations audit their own systems.
- Management review is conducted by the top management to analyze the suitability, adequacy, and effectiveness of the information security management system.
- Management review should include, among others, information on audit results, nonconformities and corrective actions, review of new and ongoing actions, results of monitoring and measurement, risks assessment, and status of risk treatment plan.
- Management review must be conducted at planned intervals.

Questions?

Quiz 6

Note: To complete Quiz 6, please go to the Quizzes Worksheet.

This section provides information that will help the participant gain knowledge on corrective actions, action plans, and continual improvement.



An organization wishing to comply with ISO/IEC 27001:2022 shall at least:

1. Demonstrate that actions are taken to continually improve the effectiveness of the ISMS.
2. Define a process to review, evaluate, and treat nonconformities
3. Identify nonconformities and react effectively

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there should be at least one annual review of performance and a revision of processes, followed by the setting of revised performance objectives for the following period.

ISO/IEC 27003, clause 10.2 Continual improvement

Explanation

A systematic approach using continual improvement will lead to a more effective ISMS, which will improve the organization's information security. Information security management leads the organization's operational activities in order to avoid being too reactive, i.e. that most of the resources are used for finding problems and addressing these problems. The ISMS is working systematically through continual improvement so that the organization can have a more proactive approach. Top management can set objectives for continual improvement, e.g. through measurements of effectiveness, cost, or process maturity.

Guidance

Continual improvement of the ISMS should entail that the ISMS itself and all of its elements are assessed considering internal and external issues, requirements of the interested parties and results of performance evaluation. The assessment should include an analysis of:

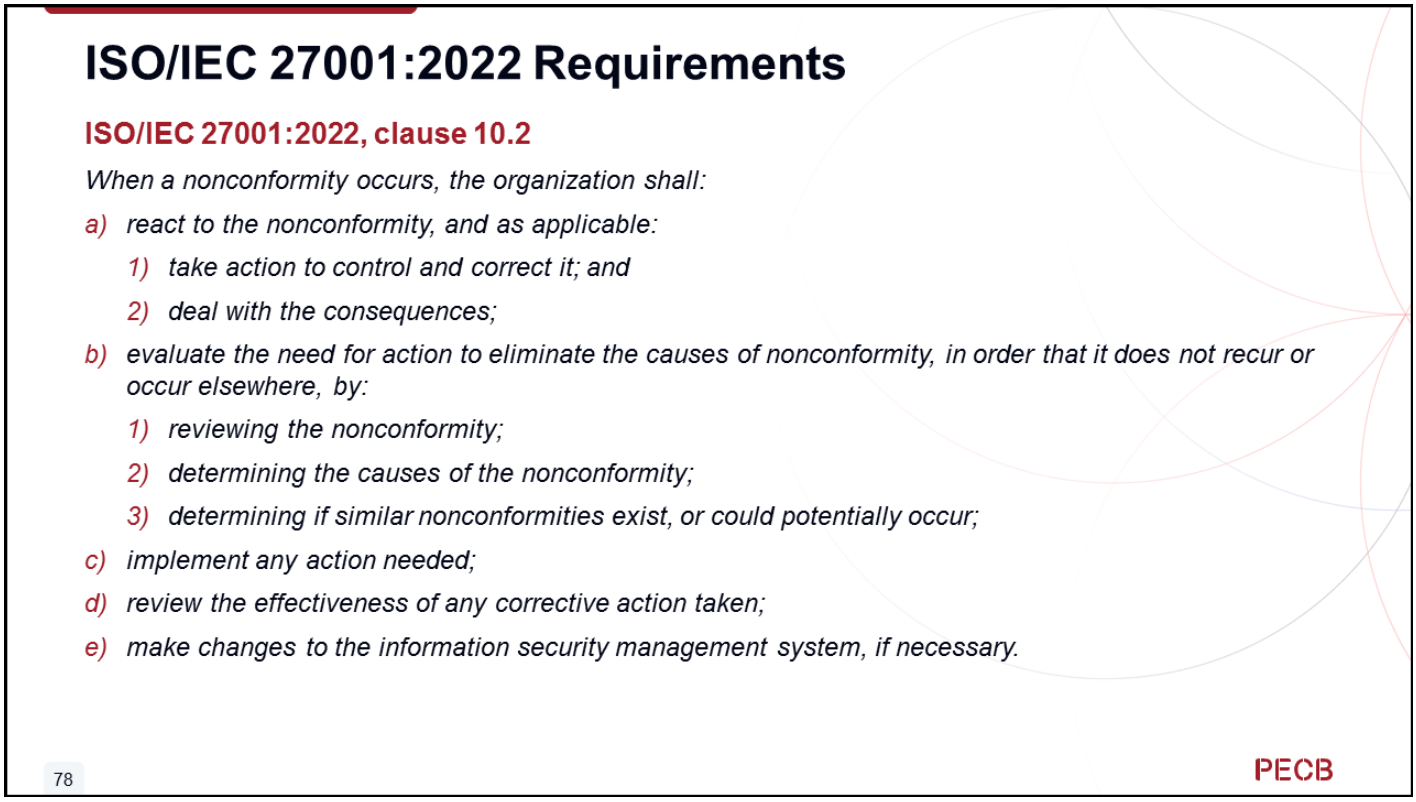
a. *suitability of the ISMS, considering if the external and internal issues, requirements of the interested parties, established information security objectives and identified information security risks are properly addressed through planning and implementation of the ISMS and information security controls;*
b. *adequacy of the ISMS, considering if the ISMS processes and information security controls are compatible with the organization's overall purposes, activities and processes; and*
c. *effectiveness of the ISMS, considering if the intended outcome(s) of the ISMS are achieved, the*

requirements of the interested parties are met, information security risks are managed to meet information security objectives, nonconformities are managed, while resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS are commensurate with those results.

The Benefits of Continual Improvement

- **Increased efficiency –** Continual improvement allows for increased productivity, since the changes may lead to long-term positive outputs.
- **Collaborative teams –** Working continuously together toward a common goal will help in building and reinforcing the existing relations of the team.
- **Increased customer satisfaction –** While organizations actively seek for ways to improve their management system, they indirectly reduce the number of errors.
- **Error reduction –** While organizations actively seek for ways to improve their management system, they indirectly increase the value and quality of the products and services they offer.

PECB



ISO/IEC 27001:2022, clause 10.2 Nonconformity and corrective action (cont'd)

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

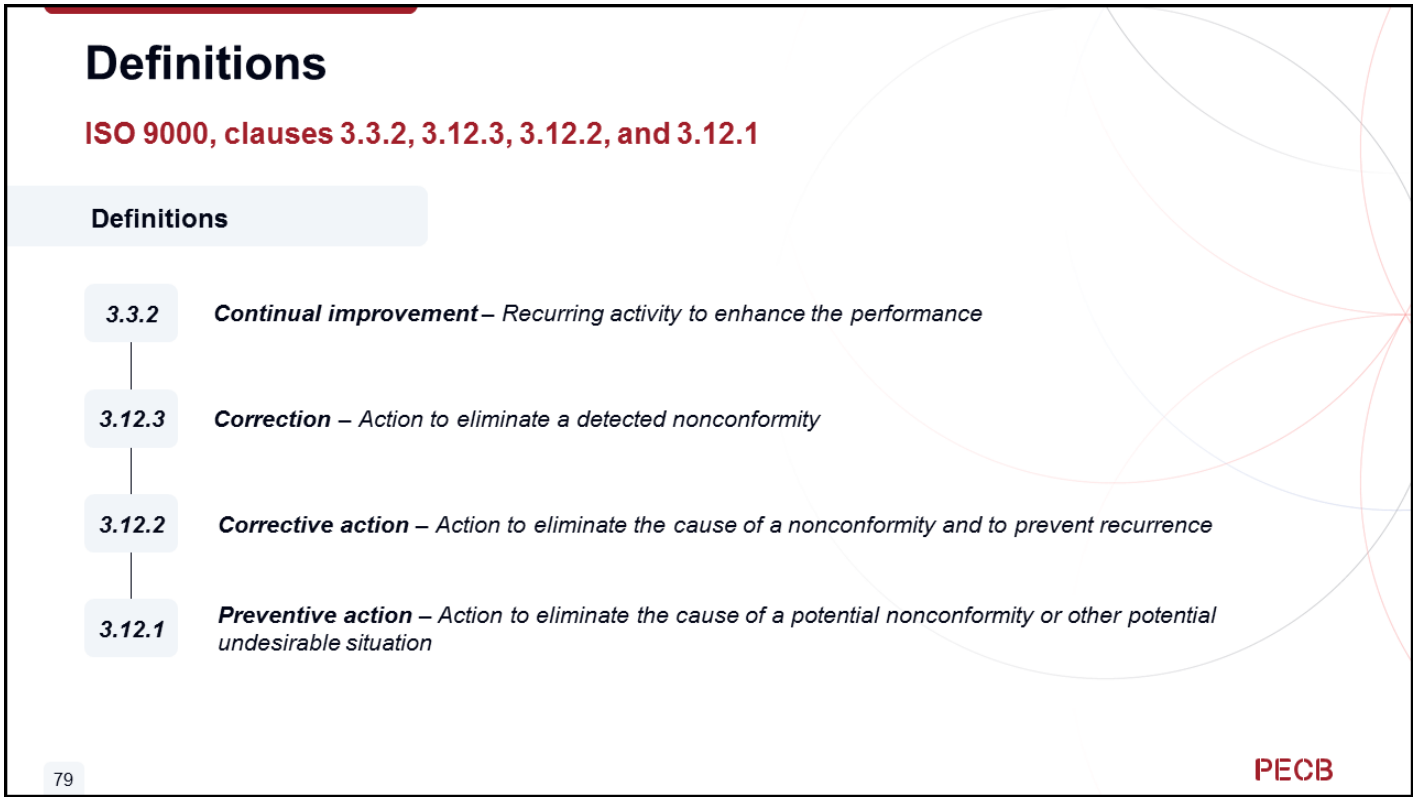
f.*the nature of the nonconformities and any subsequent actions taken,*

g.*the results of any corrective action.*

ISO/IEC 27003, clause 10.1 Nonconformity and corrective action

A nonconformity is a non-fulfilment of a requirement of the ISMS. Requirements are needs or expectations that are stated, implied or obligatory. There are several types of nonconformities such as:

a. *failure to fulfil a requirement (completely or partially) of ISO/IEC 27001 in the ISMS;*
b. *failure to correctly implement or conform to a requirement, rule or control stated by the ISMS; and*
c. *partial or total failure to comply with legal, contractual or agreed customer requirements.*
    - *Nonconformities canbe for example:*
d. *persons not behaving as expected by procedures and policies;*
e. *suppliers not providing agreed products or services;*
f. *projects not delivering expected outcomes; and*
g. *controls not operating according to design.*
    - *Nonconformities can be recognized by:*
h. *deficiencies of activities performed in the scope of the management system;*
i. *ineffective controls that are not remediated appropriately;*
j. *analysis of information security incidents, showing the non-fulfilment of a requirement of the ISMS;*
k. *complaints from customers;*
l. *alerts from users or suppliers;*
m. *monitoring and measurement results not meeting acceptance criteria; and*
n. *objectives not achieved.*



Notes on terminology:

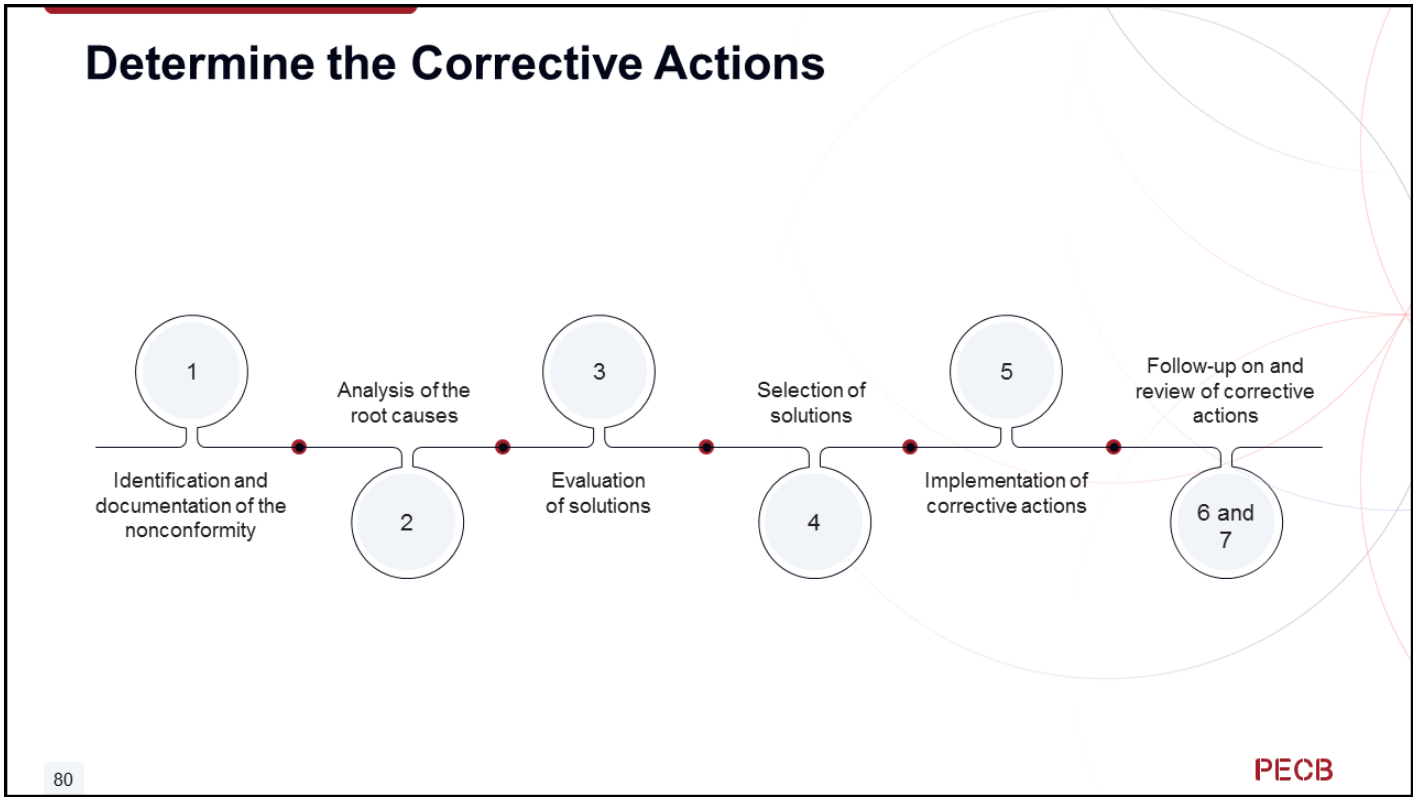
1. By definition, information security improvement is the part of information security management focused on increasing the ability to fulfill information security requirements. The requirements can be related to any aspect, including effectiveness, efficiency, or traceability.
2. The process of establishing objectives and finding opportunities for improvement is a continual process that uses audit findings and audit conclusions, analysis of data, management reviews, or other means. It generally leads to corrective action or preventive action.
3. Preventive action is taken to prevent occurrence, whereas corrective action is taken to prevent recurrence.
4. A correction can be made in conjunction with a corrective action.

ISO 9000, clause 3.7.11 Effectiveness

Extent to which planned activities are realized and planned results are achieved

ISO 9000, clause 3.7.10 Efficiency

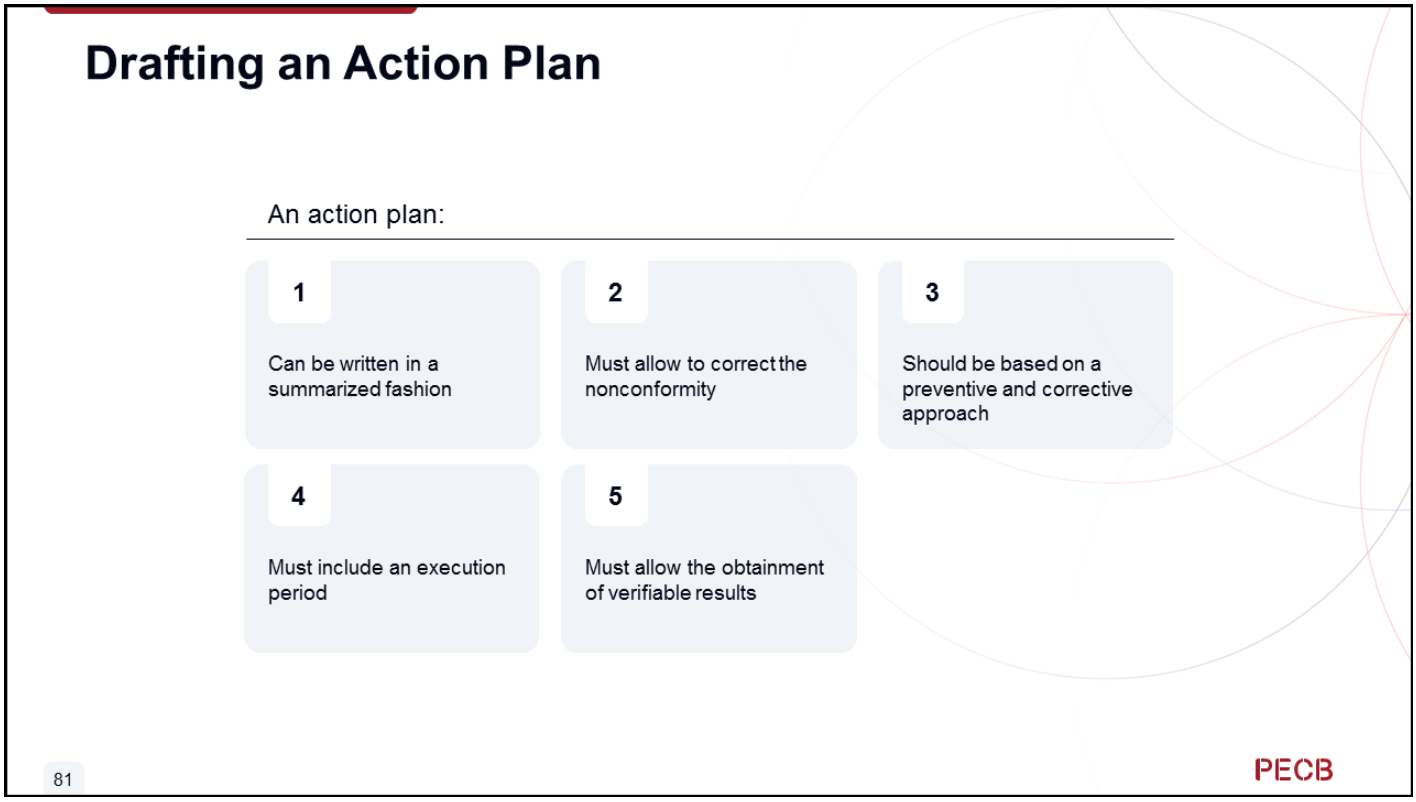
Relationship between the result achieved and the resources used



A corrective action is an action taken to **eliminate once and for all the root causes** of a nonconformity or of any other **existing** undesirable event, and to **prevent its recurrence**. A corrective action is, thus, a term that includes the reaction to a system problem process, to security incidents, to gaps in reaching objectives, to nonconformities, etc.

The corrective action process should include:

1. **Identification of the nonconformity:** The initial step in the process is to clearly define and document the nonconformity and analyze its impacts on the organization.
2. **Analysis of the root causes:** Determine the source of the nonconformity and analyze the root causes.
3. **Evaluation of solutions:** A list of possible corrective actions is elaborated. At this stage, if the problem is important, or if there is a considerably high probability that the problem will be repeated, temporary corrective actions can be set in place.
4. **Selection of solutions:** One or more corrective actions are selected to correct the situation and the contemplated improvement objectives are determined. The selected solution must correct the problem and should also contribute to the avoidance of the recurrence of similar situations.
5. **Implementation of corrective actions:** The corrective action plan approved is implemented and all the actions described in the plan are documented.
6. **Follow-up on corrective actions:** One must check that the new corrective controls are in place and effective. The follow-up is usually performed by the person responsible for the project and the audit department.
7. **Review of corrective actions:** To perform a review of the effectiveness of the corrective actions, it is periodically evaluated whether the organization has reached its security objectives using corrective actions, and if they remain effective over time.



Implementation dates must be realistic and based on the nonconformities observed and the costs of the corrective measures to be taken. The deadlines set must be reasonable.

Action Plans

Examples

1. A new system dedicated to the management of the client account data must be installed in the network to separate the confidential data from other databases (2nd quarter of 2019).

2. A new version of the security policy must be published to include legal and regulatory statements, as well as contract requirements (within 2 months).

3. The names of the persons to be contacted in case of disaster must be explicitly mentioned in the business continuity plan (immediately) and the procedures to contact these persons must be documented and communicated.

PECB

Discussion questions:

1. What is continual improvement?
2. Which are the benefits of continual improvement?
3. What should the corrective action process include?

Section 11 Summary

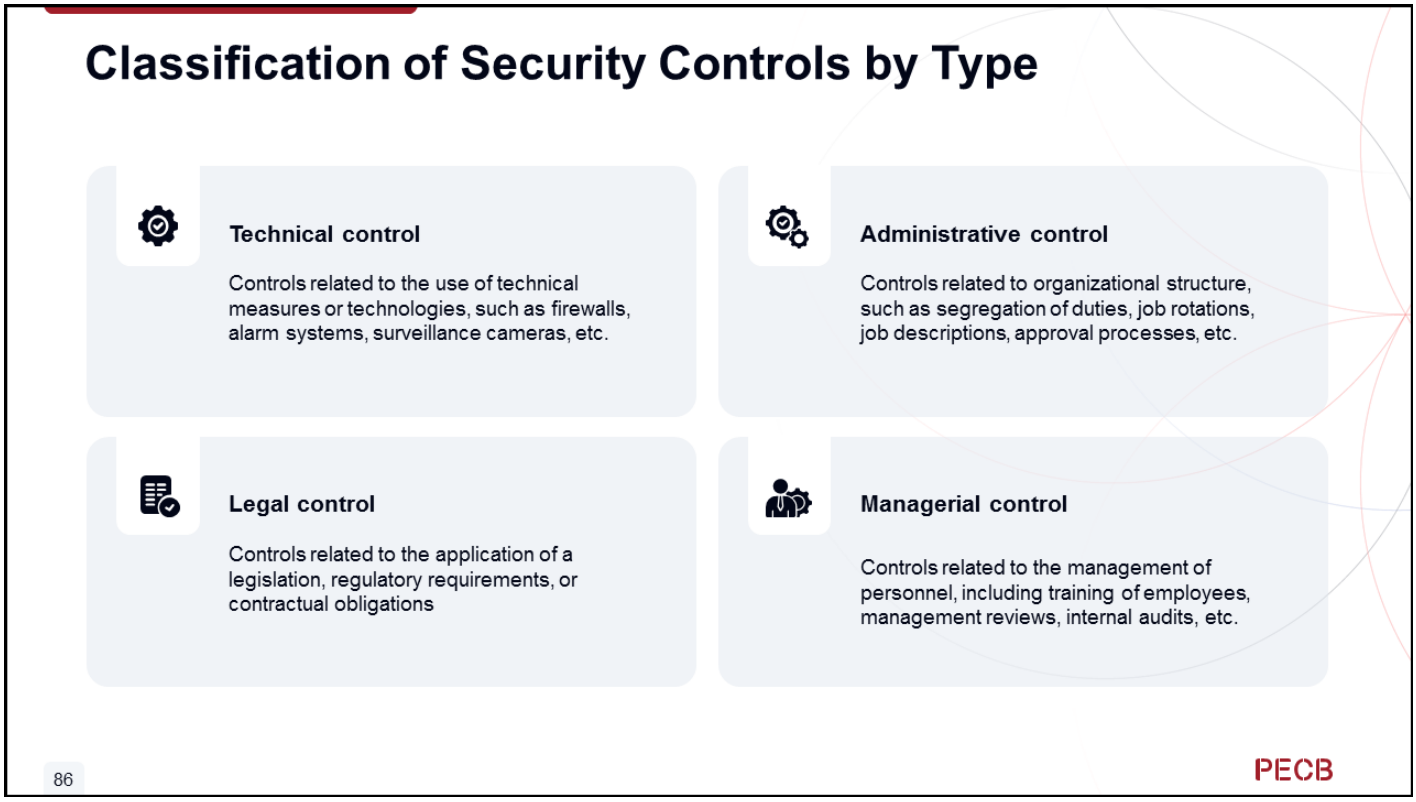
- Organizations should define a process to react effectively to nonconformities and review, evaluate, and treat them.
- The treatment of nonconformities requires defining a process to resolve them, determining the corrective and preventive actions, and drafting the action plan.
- Drafting an action plan should include the correction of nonconformities, the execution period, and the obtainment of verifiable results.
- Continual improvement helps organizations increase efficiency and customer satisfaction, reduce errors, and build teamwork.

Questions?

Quiz 7

Note: To complete Quiz 7, please go to the Quizzes Worksheet.

This section provides valuable information on the classification of security controls by type and function, and the controls of Annex A.



ISO/IEC 27000, clause 3.14 Control

Measure that is modifying risk

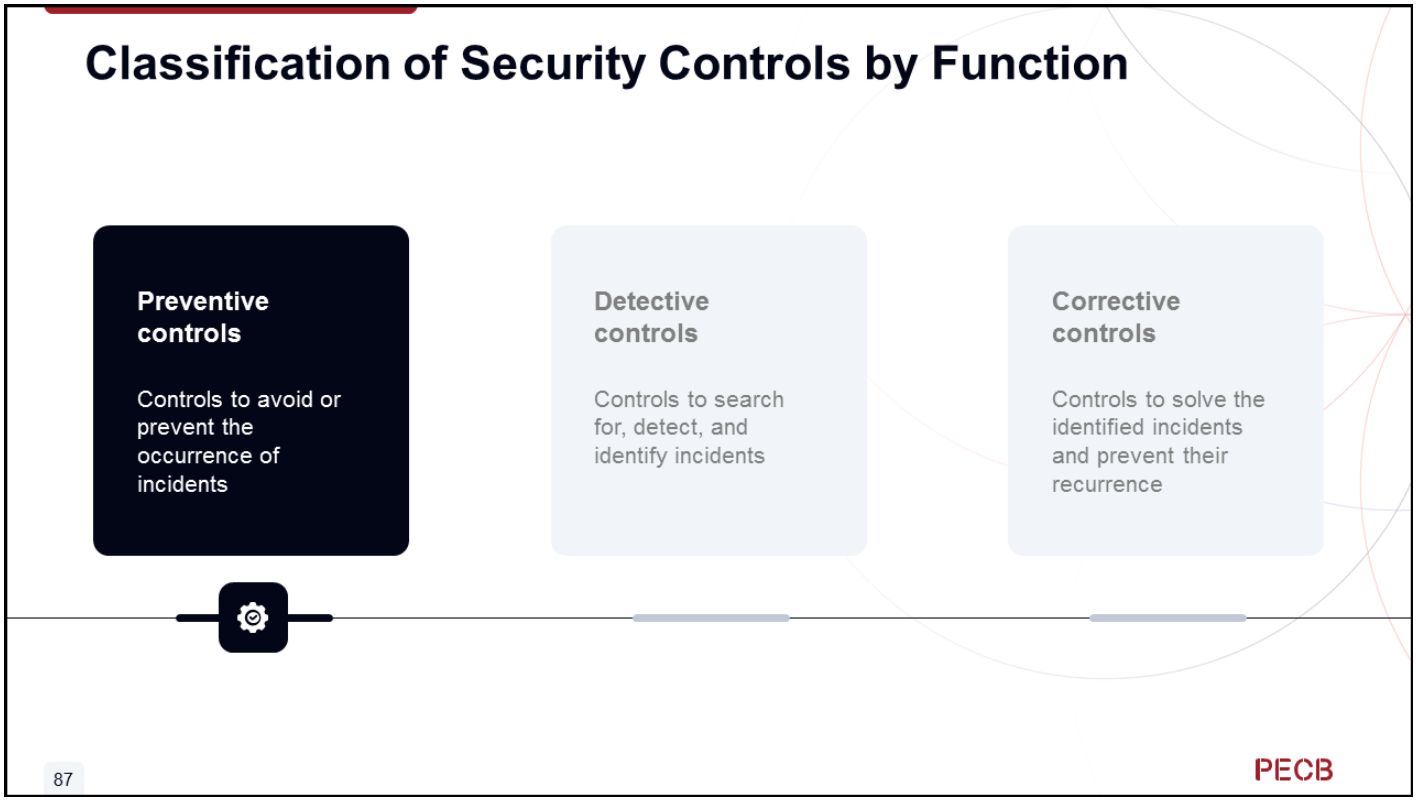
ISO/IEC 27000, clause 3.15 Control objective

Statement describing what is to be achieved as a result of implementing controls

Controls for information security include any process, policy, procedure, guideline, practice, or organizational structure that can be administrative, technical, managerial, or legal in nature, and that can modify information security risks.

Note:

- An administrative control is more related to the structure of the organization as a whole without being applied by a particular person, while a managerial control is to be applied by managers.
- The differences between the types of security controls are explained only for understanding. An organization does not need to determine the nature of the security controls it implements.



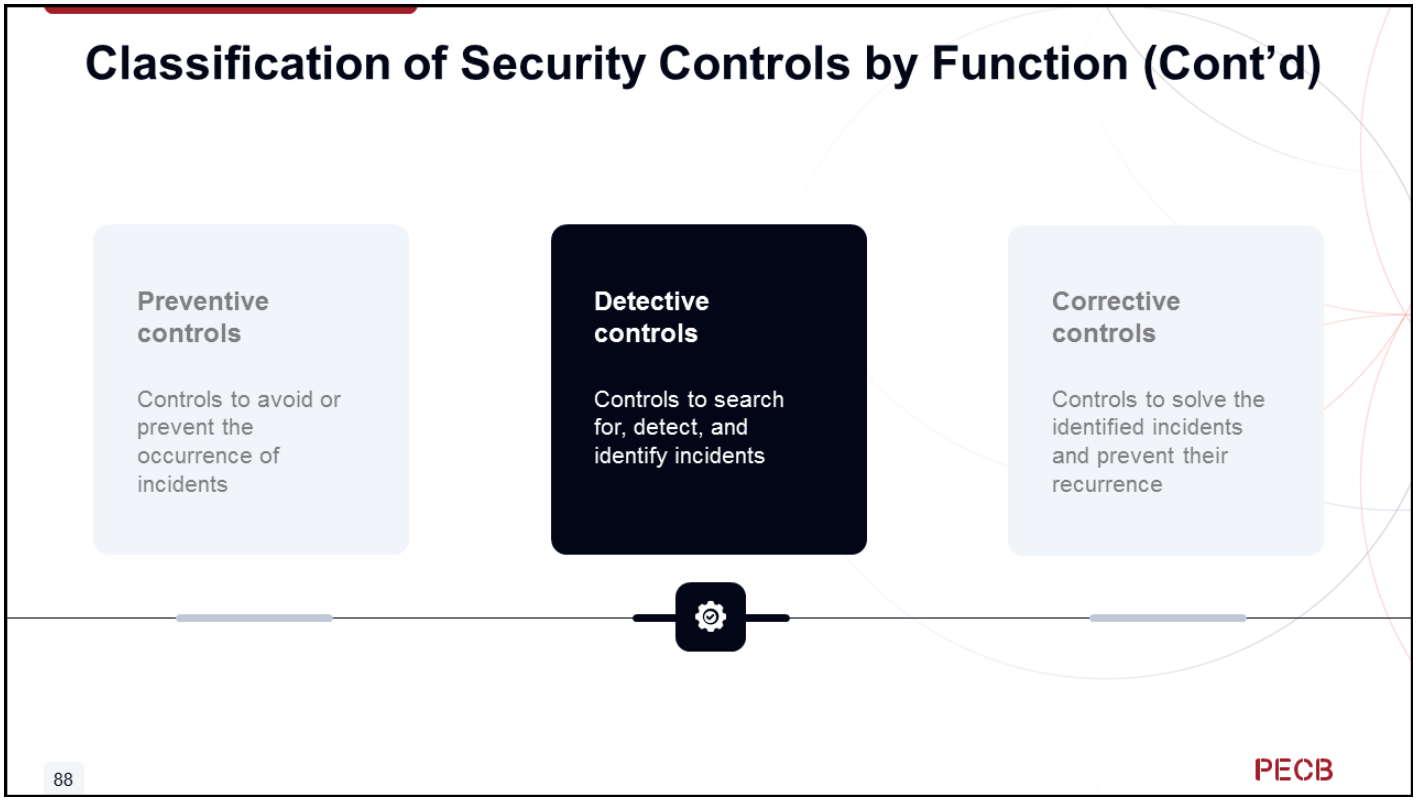
Goal: Avoid or prevent the occurrence of incidents

- Detect incidents before they occur
- Control operations
- Prevent errors, omissions, or malicious acts

Examples:

- Establish an information security policy
- Sign a confidentiality agreement
- Hire only qualified personnel
- Identify third party risks
- Assign duties appropriately
- Separate the development, testing, and operating equipment
- Secure offices, rooms, and equipment
- Use clearly defined procedures (to prevent errors and mistakes)
- Use cryptography
- Use an access control software that only allows authorized personnel to access sensitive files

Important note: These different types of controls are connected with one another. For example, the implementation of an antivirus is a preventive control because it provides protection against malware. At the same time, the antivirus serves as a detective measure when it detects a potential virus and provides a corrective measure when a suspicious file is quarantined or deleted.

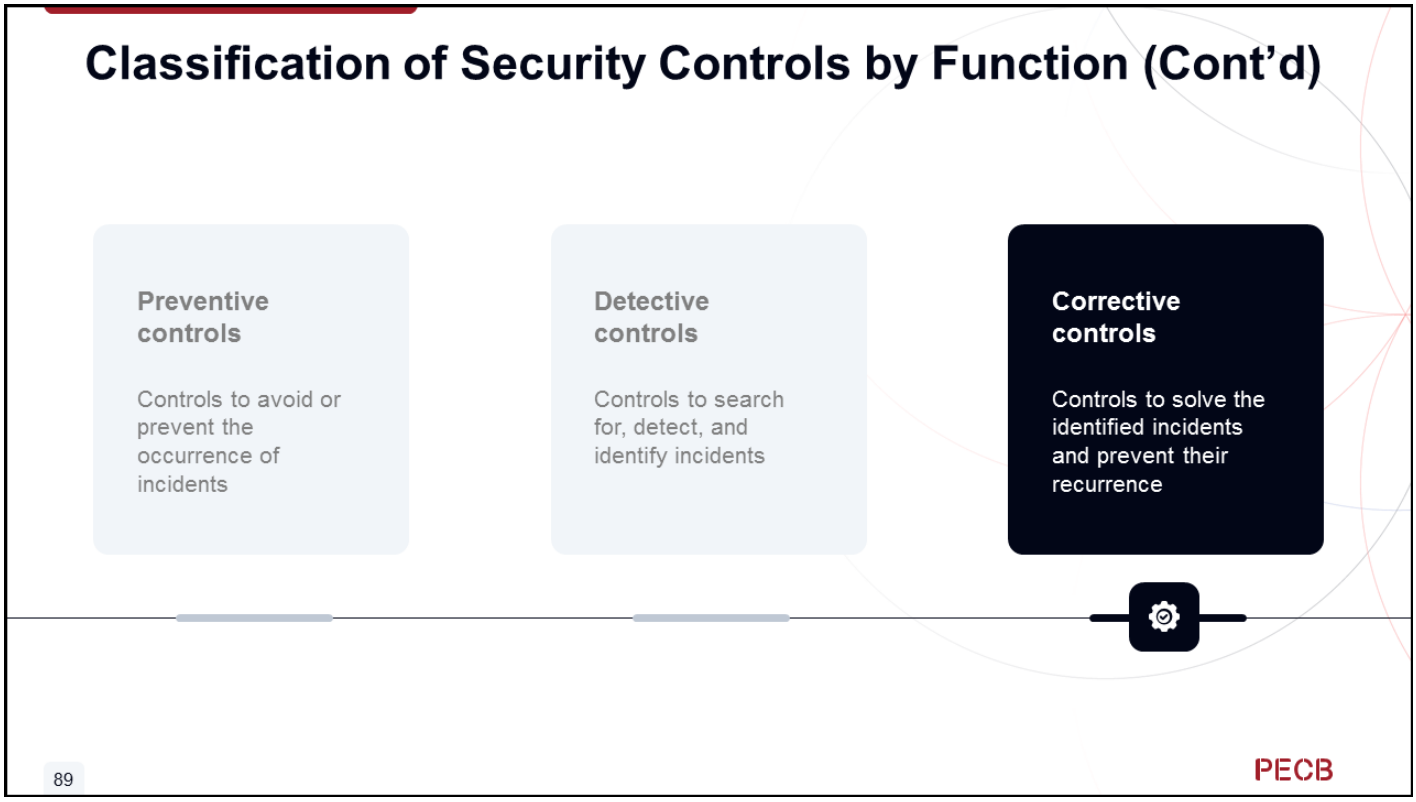


Goal: Search for, detect, and identify incidents

- Use controls that detect and report the occurrence of an error, omission, or malicious act

Examples:

- Monitor and review third party services
- Monitor the resources used by systems
- Use trigger alarms, e.g., fire alarm
- Review user access rights
- Analyze audit logs
- Integration of checkpoints in the applications in production
- Echo control in telecommunications
- Alarms to detect risks related to heat, smoke, fire, or water
- Verification of duplicate calculations in data processing
- Detection of break-ins with video cameras
- Detection of potential intrusions on networks with an intrusion detection system (IDS)
- Review of user access rights
- Technical review of applications after a modification of the operating system



Goal: Solve the identified incidents and prevent their recurrence

- Minimize the impact of a threat
- Solve the incidents discovered by detection controls
- Identify the causes of an incident
- Modify the processing system to reduce future incidents to a minimum

Examples:

- Conduct technical and legal investigation following an incident
- Enable the business continuity plan after the occurrence of a disaster
- Implement patches following the identification of technical vulnerabilities
- Review the security policy after the integration of a new division in the organization
- Appeal to authorities to report a computer crime
- Change all passwords of all systems when a computer network intrusion has been detected
- Recover the transactions with the backup procedure after discovering that some data has been corrupted
- Automatically disconnect idle sessions
- Implement patches following the identification of technical vulnerabilities

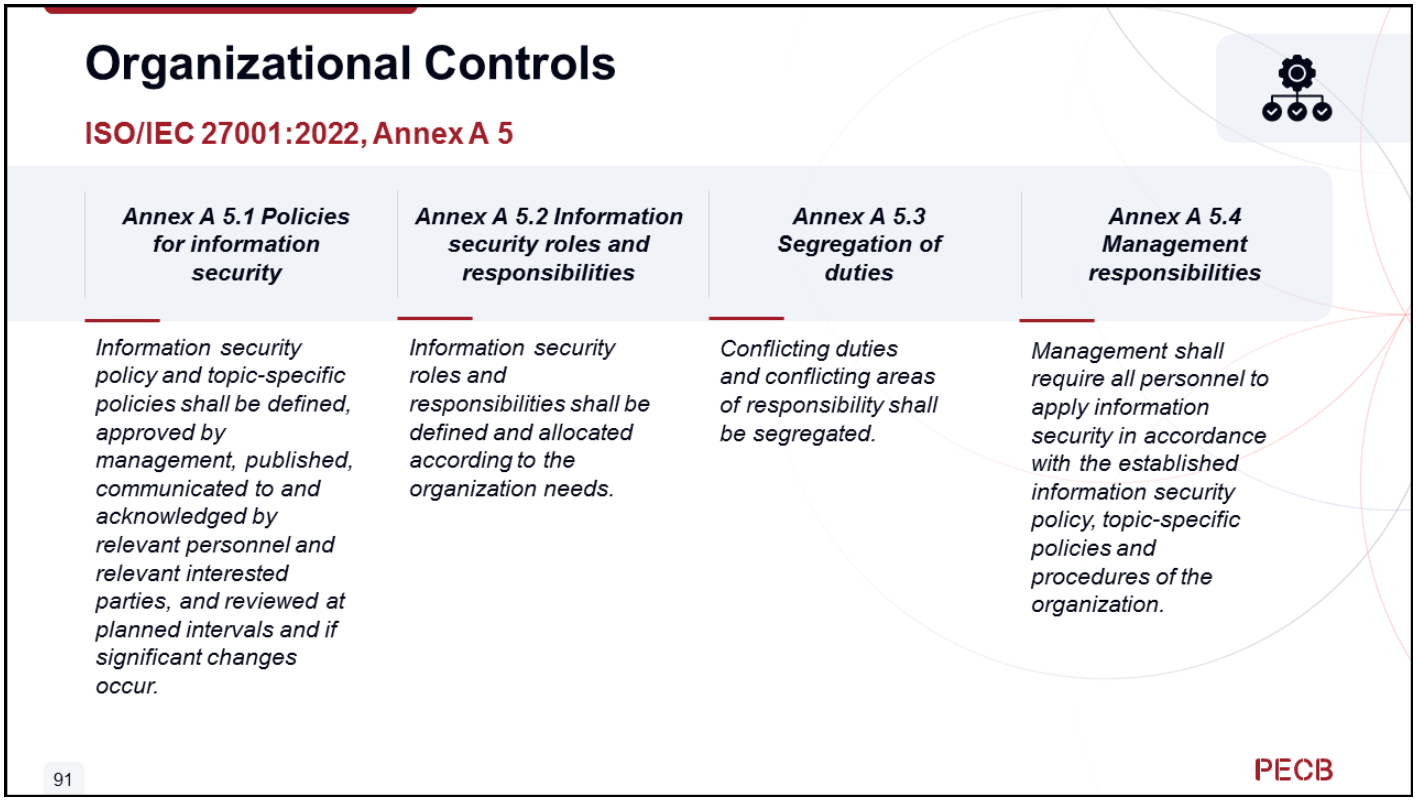
Introduction of Annex A Controls

What has changed in Annex A of ISO/IEC 27001:2022?

- The updated Annex A of ISO/IEC 27001:2022 based on ISO/IEC 27002 controls contains a list of information security controls. Annex A provides only information security controls and does not provide the control purpose and guidance as ISO/IEC 27002:2022.
- Annex A introduces **11 new information security controls**, **58 updated controls**, **and 24 controls that have been merged with the existing controls**. These controls are grouped into four categories.

5	**Organizational controls** 5.1-5.37	7	**Physical controls** 7.1-7.14
6	**People controls** 6.1-6.8	8	**Technological controls** 8.1-8.34

PECB



ISO/IEC 27002, clause 5.1 Policies for information security

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

ISO/IEC 27002, clause 5.2 Information security roles and responsibilities

Purpose

To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

ISO/IEC 27002, clause 5.3 Segregation of duties

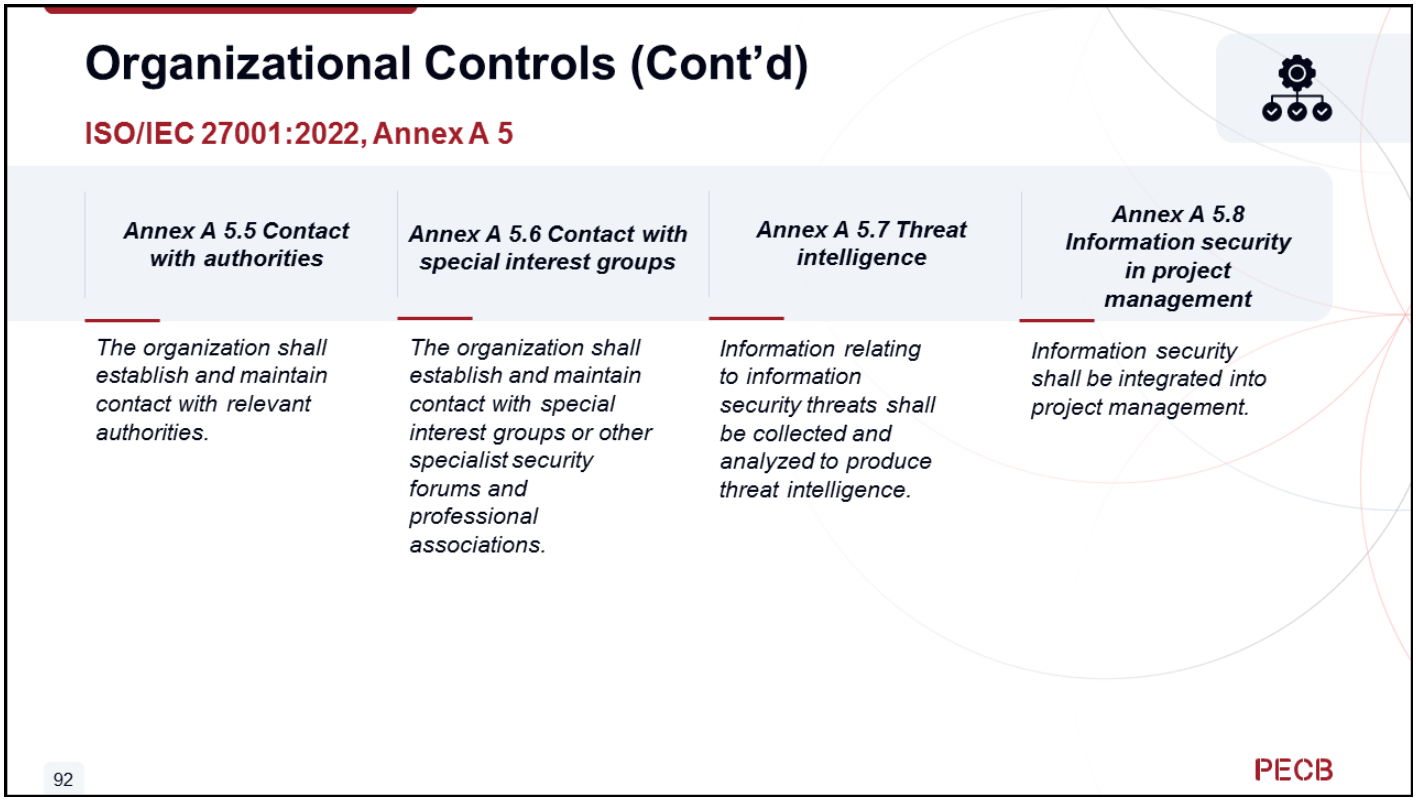
Purpose

To reduce the risk of fraud, error and bypassing of information security controls.

ISO/IEC 27002, clause 5.4 Management responsibilities

Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.



ISO/IEC 27002, clause 5.5 Contact with authorities

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

ISO/IEC 27002, clause 5.6 Contact with special interest groups

Purpose

To ensure appropriate flow of information takes place with respect to information security.

ISO/IEC 27002, clause 5.7 Threat intelligence

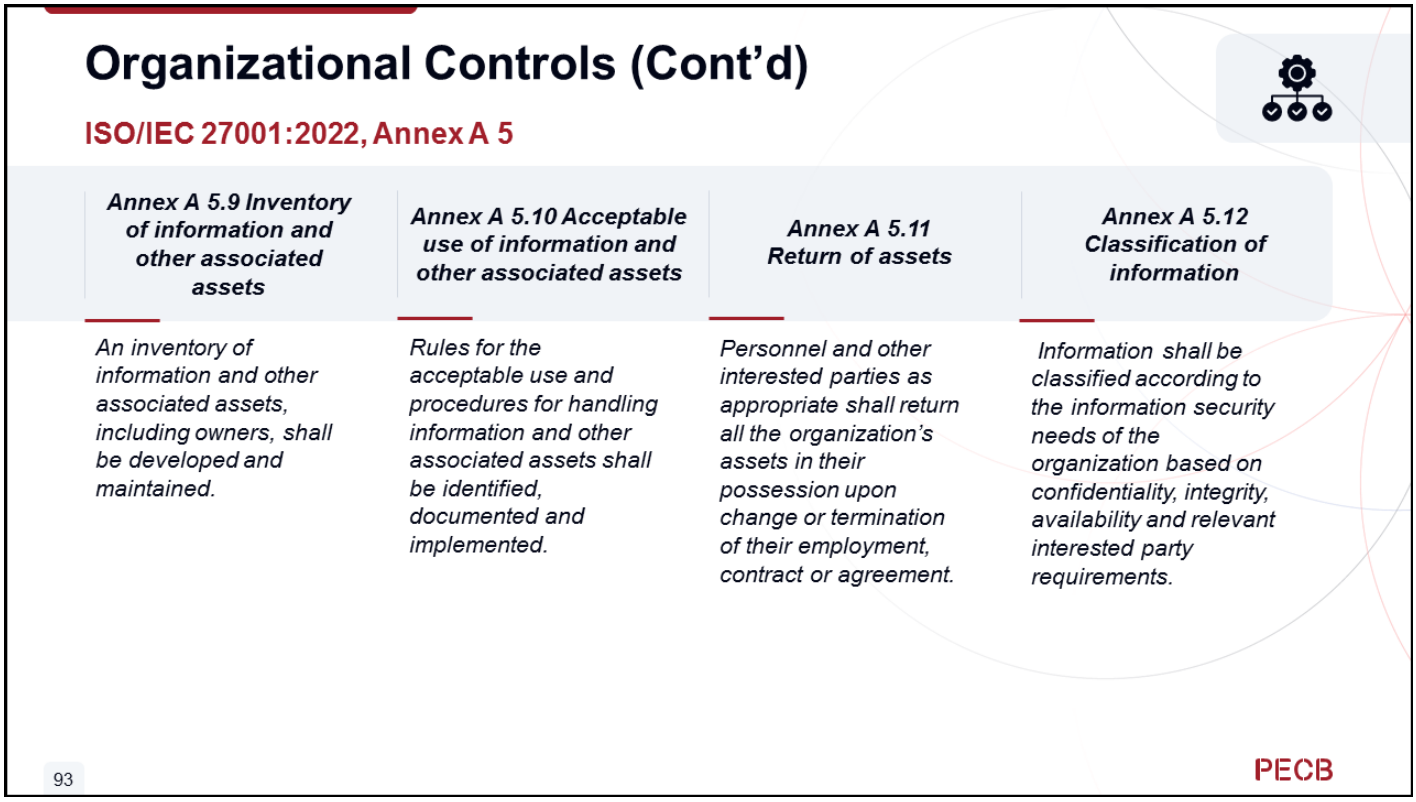
Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

ISO/IEC 27002, clause 5.8 Information security in project management

Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.



ISO/IEC 27002, clause 5.9 Inventory of information and other associated assets

Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

ISO/IEC 27002, clause 5.10 Acceptable use of information and other associated assets

Purpose

To ensure information and other associated assets are appropriately protected, used and handled.

ISO/IEC 27002, clause 5.11 Return of assets

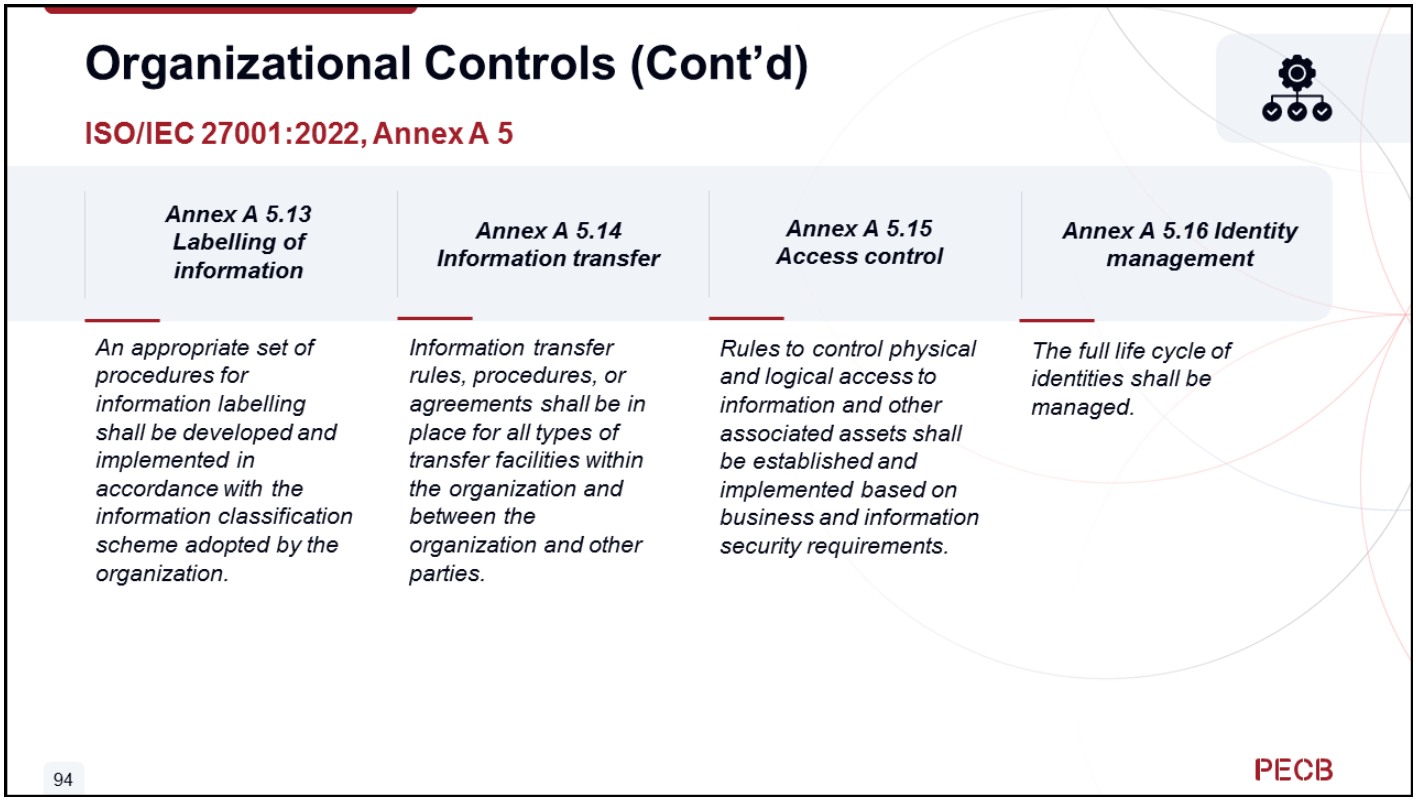
Purpose

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

ISO/IEC 27002, clause 5.12 Classification of information

Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.



ISO/IEC 27002, clause 5.13 Labelling of information

Purpose

To facilitate the communication of classification of information and support automation of information processing and management.

ISO/IEC 27002, clause 5.14 Information transfer

Purpose

To maintain the security of information transferred within an organization and with any external interested party.

ISO/IEC 27002, clause 5.15 Access control

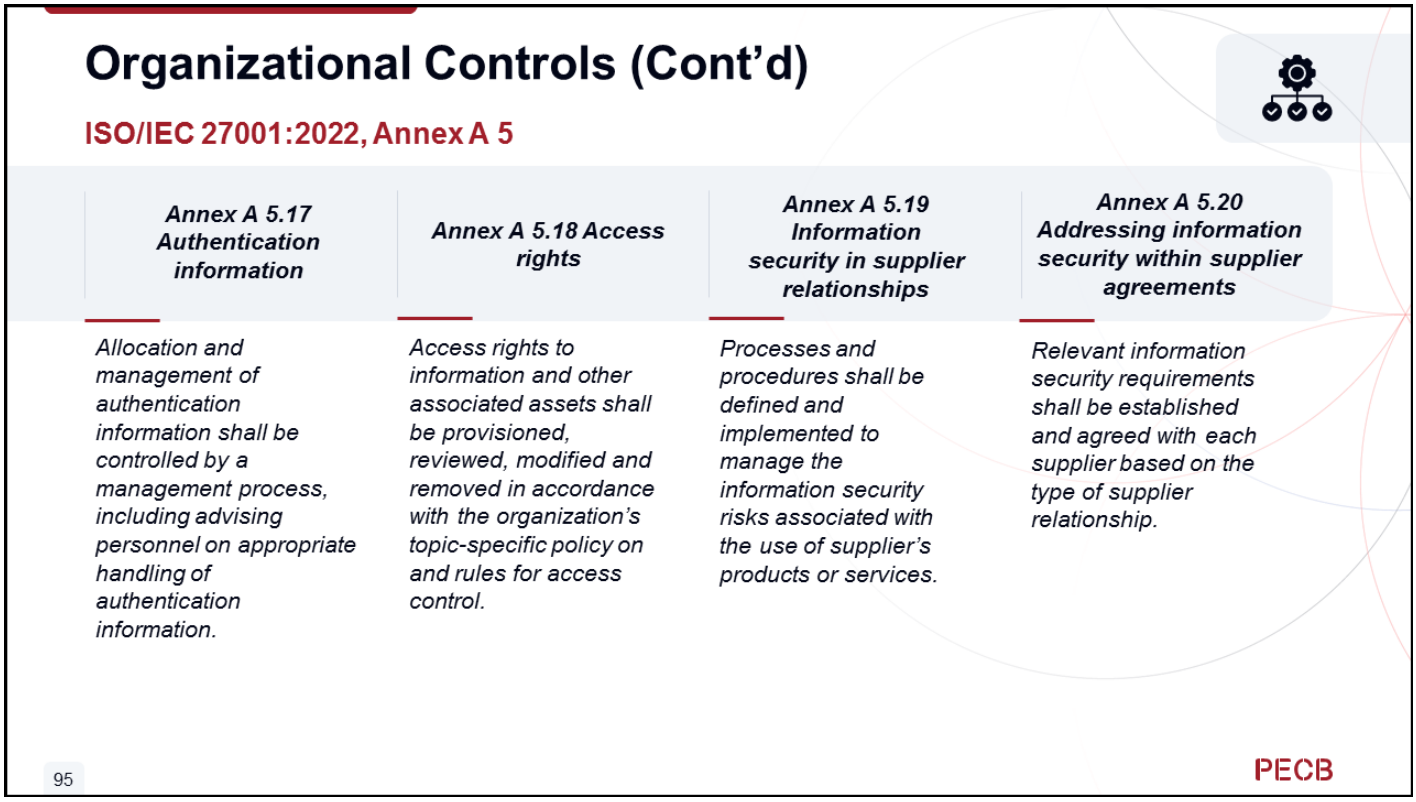
Purpose

To ensure authorized access and to prevent unauthorized access to information and other associated assets.

ISO/IEC 27002, clause 5.16 Identity management

Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.



ISO/IEC 27002, clause 5.17 Authentication information

Purpose

To ensure proper entity authentication and prevent failures of authentication processes.

ISO/IEC 27002, clause 5.18 Access rights

Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

ISO/IEC 27002, clause 5.19 Information security in supplier relationships

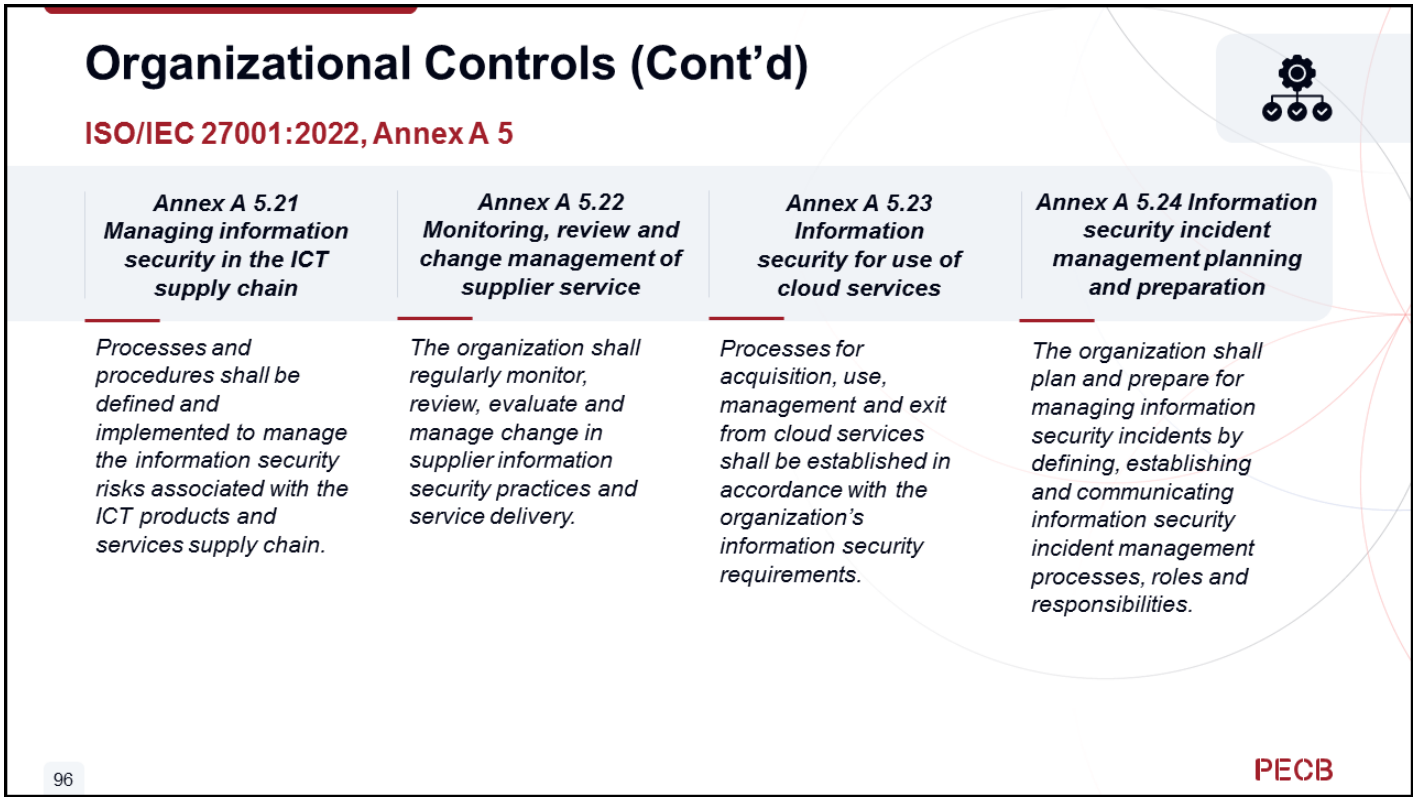
Purpose

To maintain an agreed level of information security in supplier relationships.

ISO/IEC 27002, clause 5.20 Addressing information security within supplier agreements

Purpose

To maintain an agreed level of information security in supplier relationships.



ISO/IEC 27002, clause 5.21 Managing information security in the ICT supply chain

Purpose

To maintain an agreed level of information security in supplier relationships.

ISO/IEC 27002, clause 5.22 Monitoring, review and change management of supplier services

Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements.

ISO/IEC 27002, clause 5.23 Information security for use of cloud services

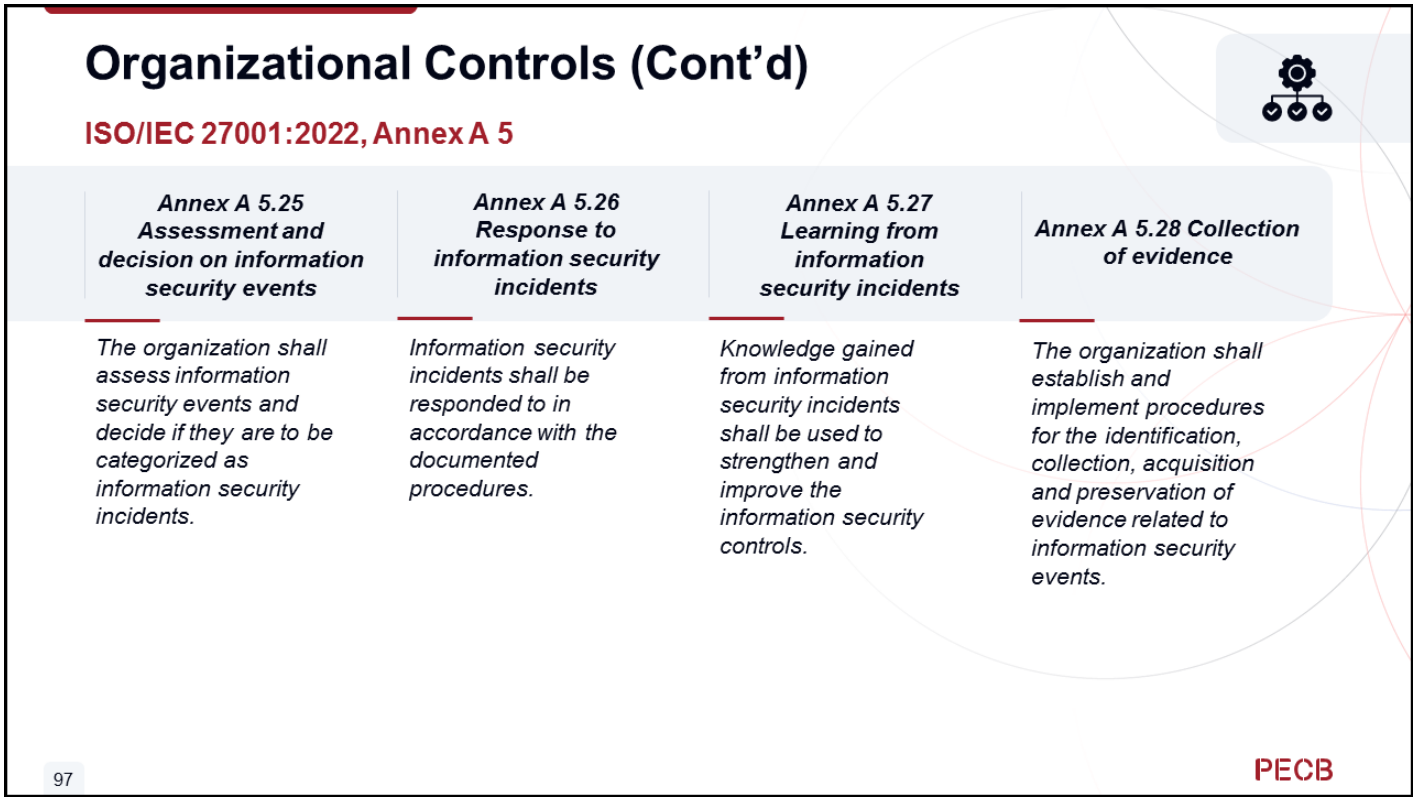
Purpose

To specify and manage information security for the use of cloud services.

ISO/IEC 27002, clause 5.24 Information security incident management planning and preparation

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.



ISO/IEC 27002, clause 5.25 Assessment and decision on information security events

Purpose

To ensure effective categorization and prioritization of information security events.

ISO/IEC 27002, clause 5.26 Response to information security incidents

Purpose

To ensure efficient and effective response to information security incidents.

ISO/IEC 27002, clause 5.27 Learning from information security incidents

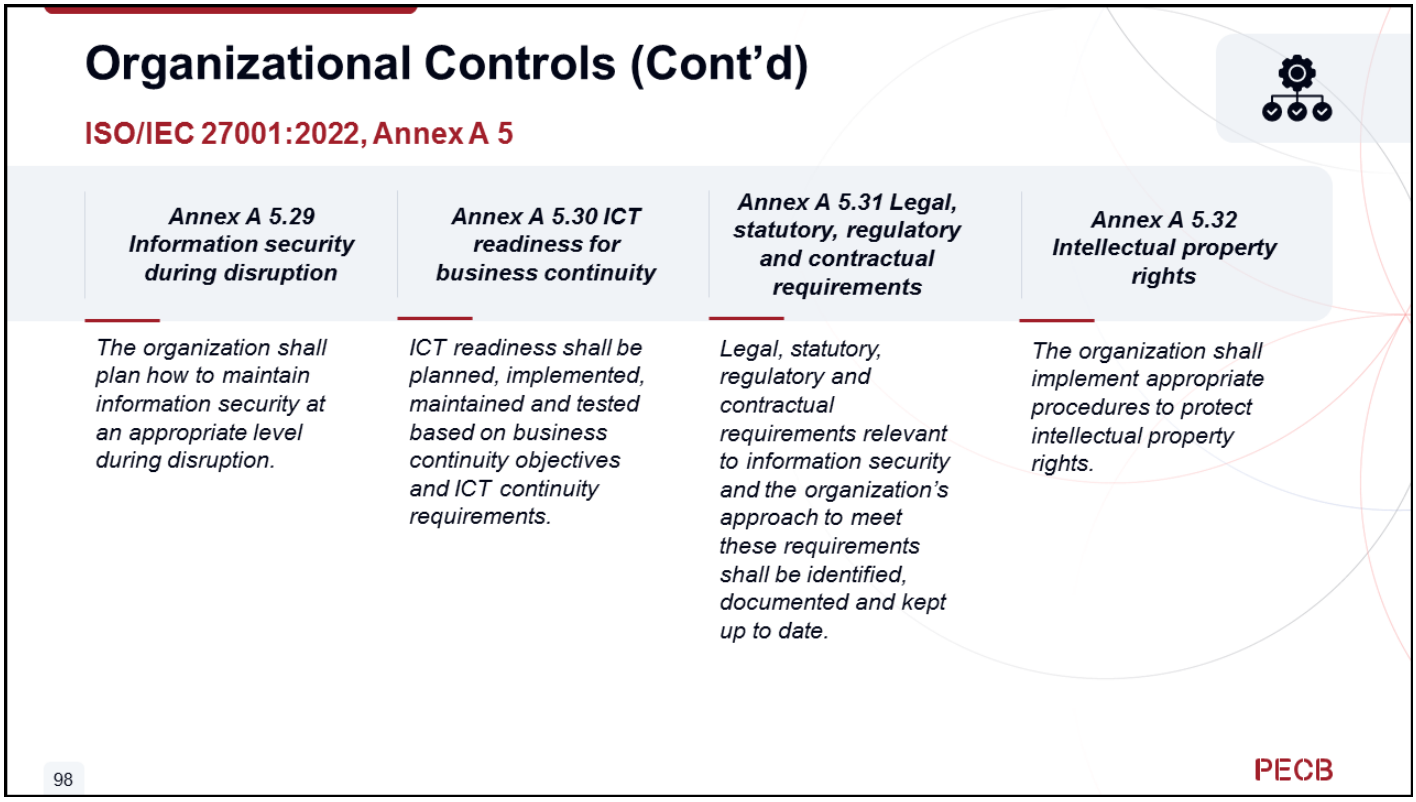
Purpose

To reduce the likelihood or consequences of future incidents.

ISO/IEC 27002, clause 5.28 Collection of evidence

Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.



ISO/IEC 27002, clause 5.29 Information security during disruption

Purpose

To protect information and other associated assets during disruption.

ISO/IEC 27002, clause 5.30 ICT readiness for business continuity

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

ISO/IEC 27002, clause 5.31 Legal, statutory, regulatory and contractual requirements

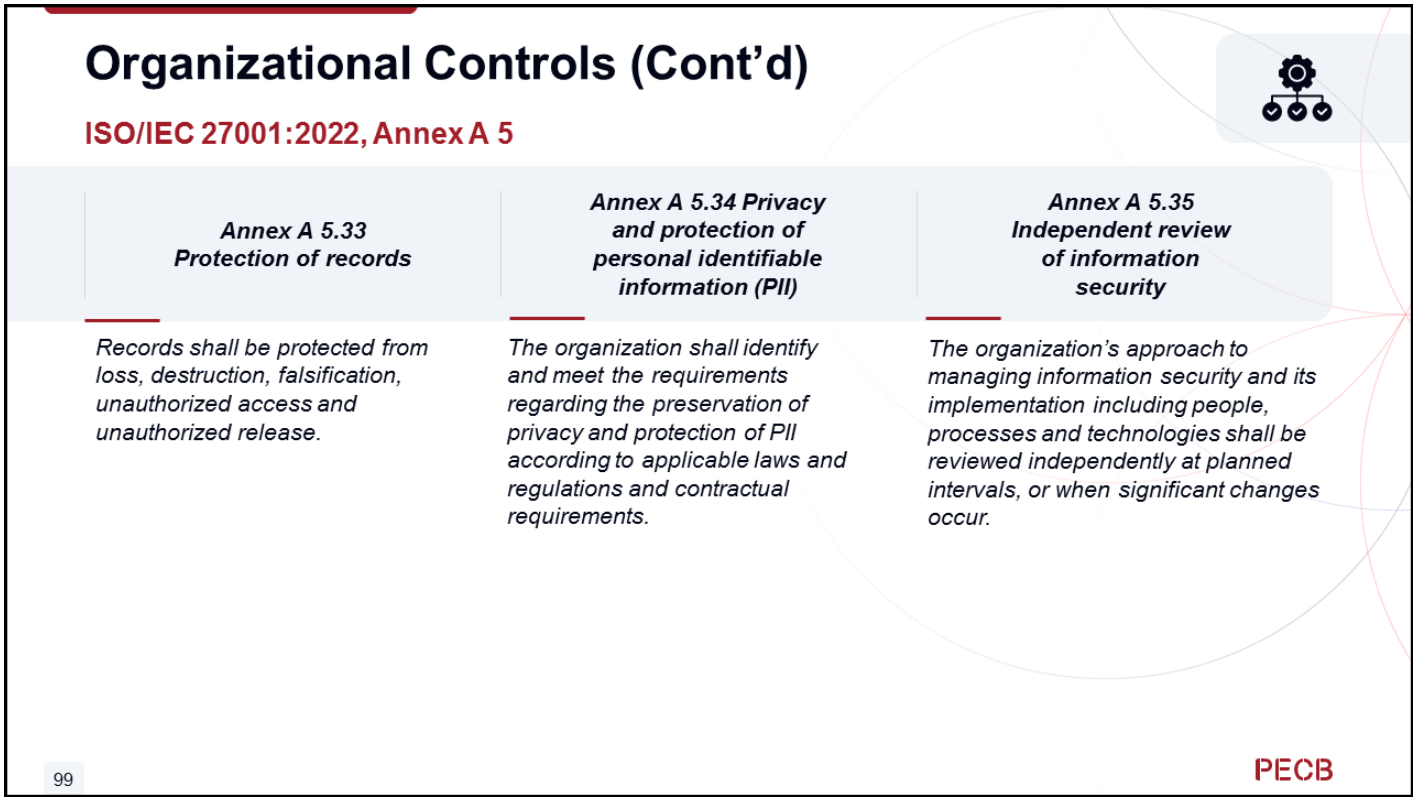
Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

ISO/IEC 27002, clause 5.32 Intellectual property rights

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.



ISO/IEC 27002, control 5.33 Protection of records

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

ISO/IEC 27002, control 5.34 Privacy and protection of personal identifiable information (PII)

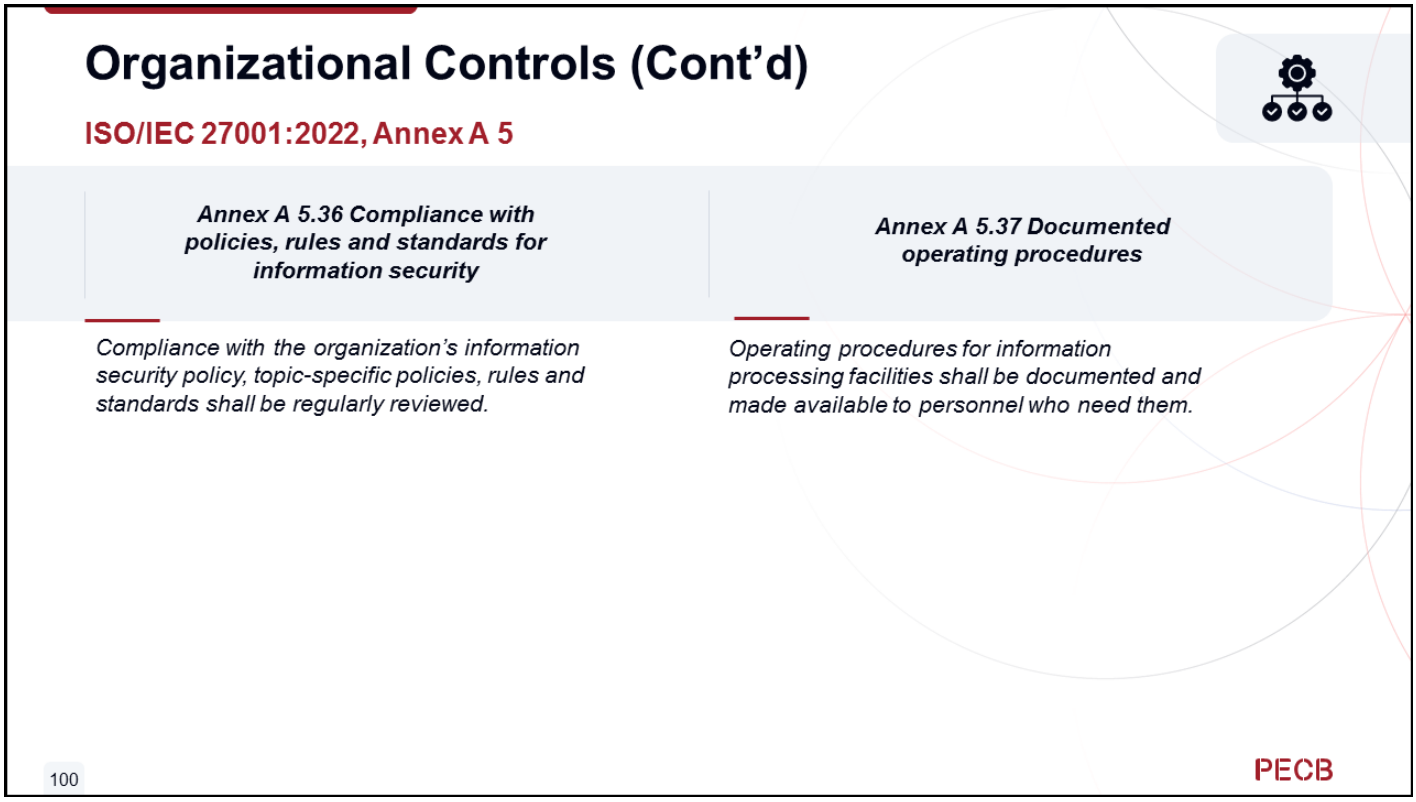
Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

ISO/IEC 27002, control 5.35 Independent review of information security

Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.



ISO/IEC 27002, clause 5.36 Compliance with policies, rules and standards for information security

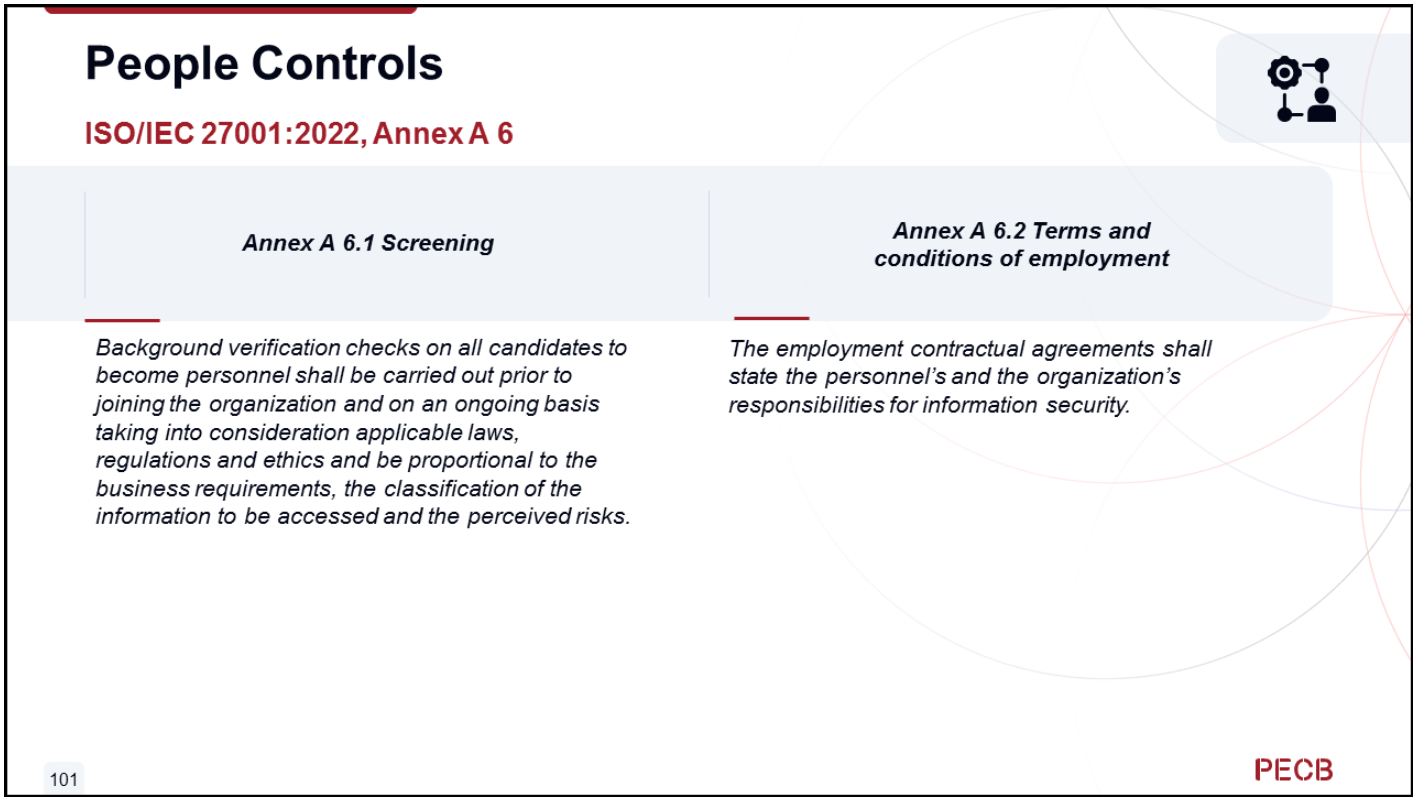
Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

ISO/IEC 27002, clause 5.37 Documented operating procedures

Purpose

To ensure the correct and secure operation of information processing facilities.



ISO/IEC 27002, clause 6.1 Screening

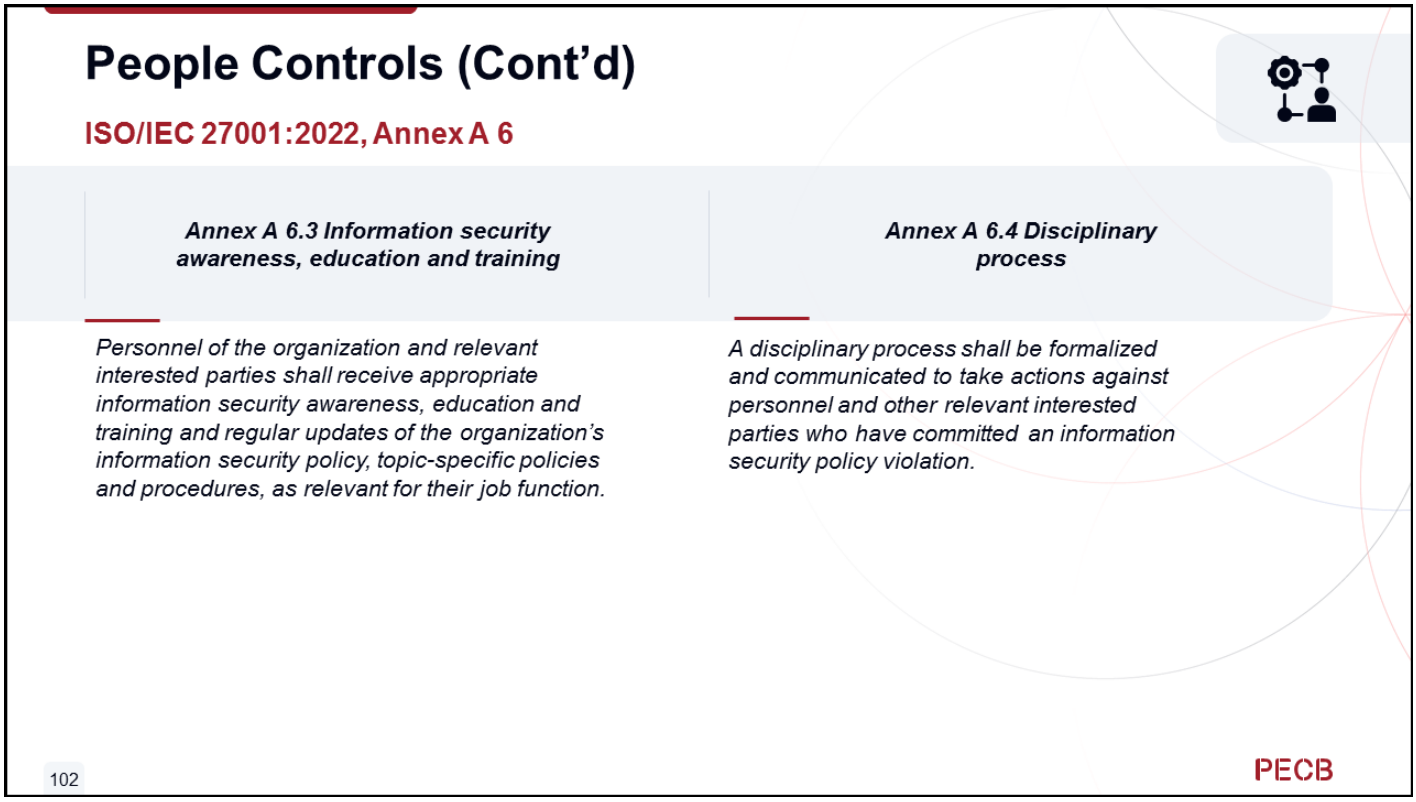
Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

ISO/IEC 27002, clause 6.2 Terms and conditions of employment

Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered.



ISO/IEC 27002, clause 6.3 Information security awareness, education and training

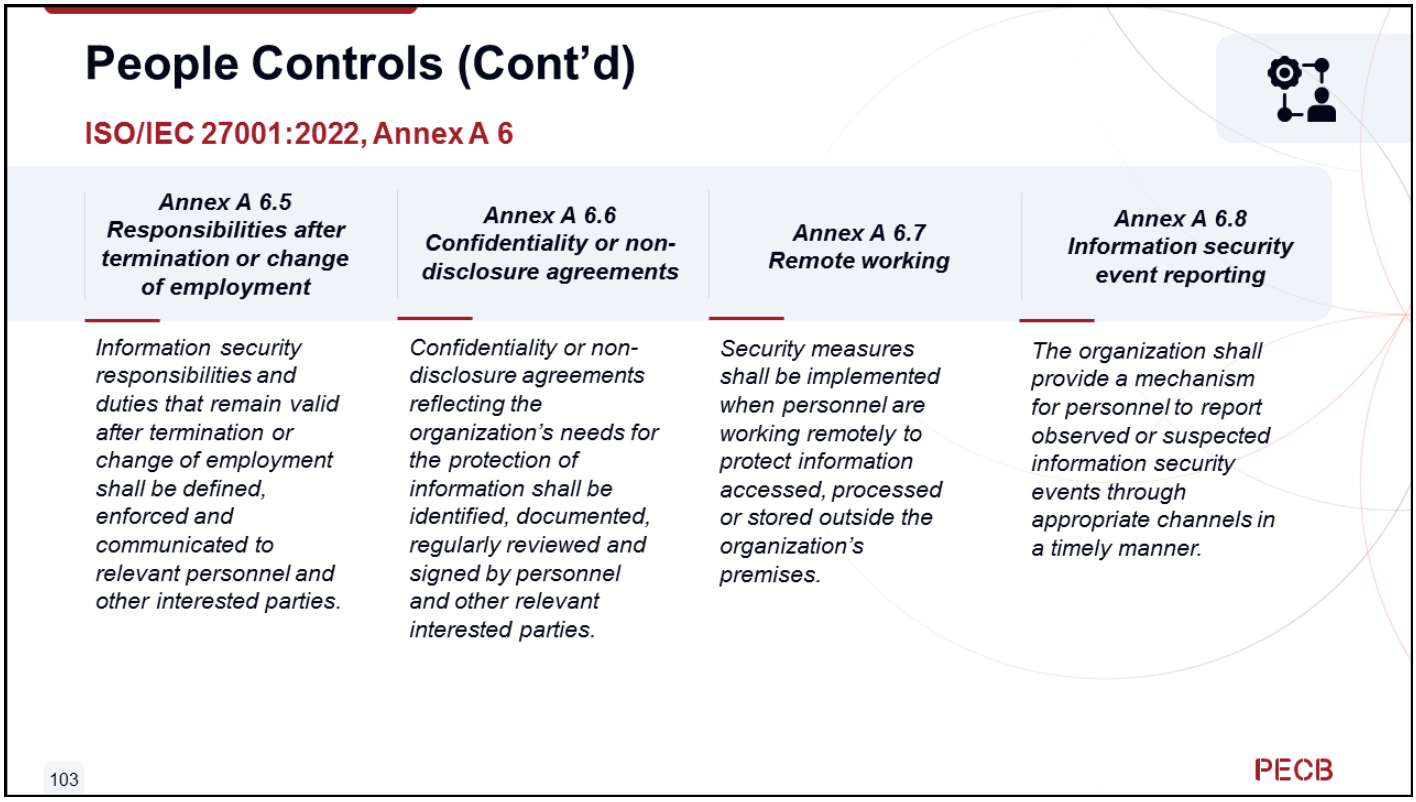
Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

ISO/IEC 27002, clause 6.4 Disciplinary process

Purpose

To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.



ISO/IEC 27002, clause 6.5 Responsibilities after termination or change of employment

Purpose

To protect the organization's interests as part of the process of changing or terminating employment or contracts.

ISO/IEC 27002, clause 6.6 Confidentiality or non-disclosure agreements

Purpose

To maintain confidentiality of information accessible by personnel or external parties.

ISO/IEC 27002, clause 6.7 Remote working

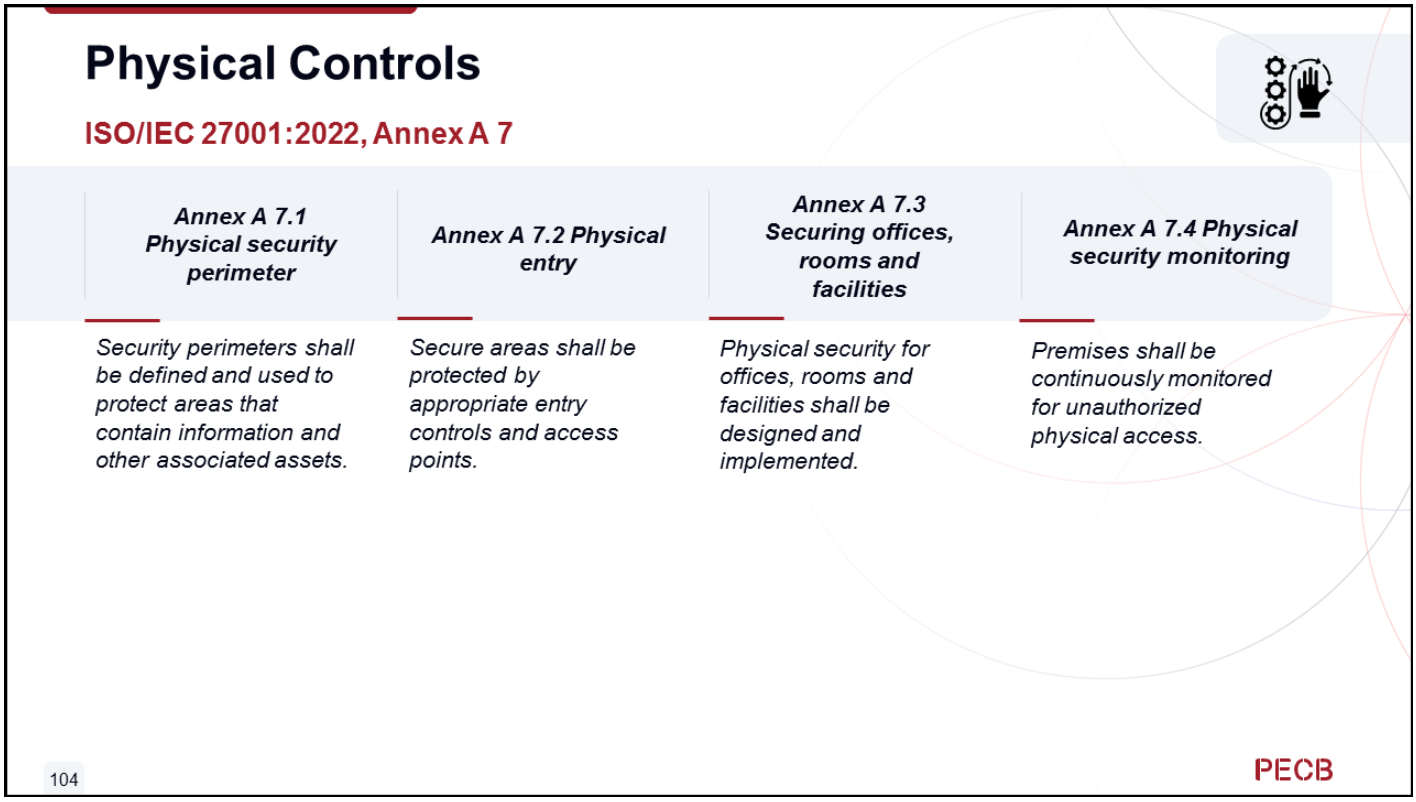
Purpose

To ensure the security of information when personnel are working remotely.

ISO/IEC 27002, clause 6.8 Information security event reporting

Purpose

To support timely, consistent and effective reporting of information security events that can be identified by personnel.



ISO/IEC 27002, clause 7.1 Physical security perimeter

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

ISO/IEC 27002, clause 7.2 Physical entry

Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs.

ISO/IEC 27002, clause 7.3 Securing offices, rooms and facilities

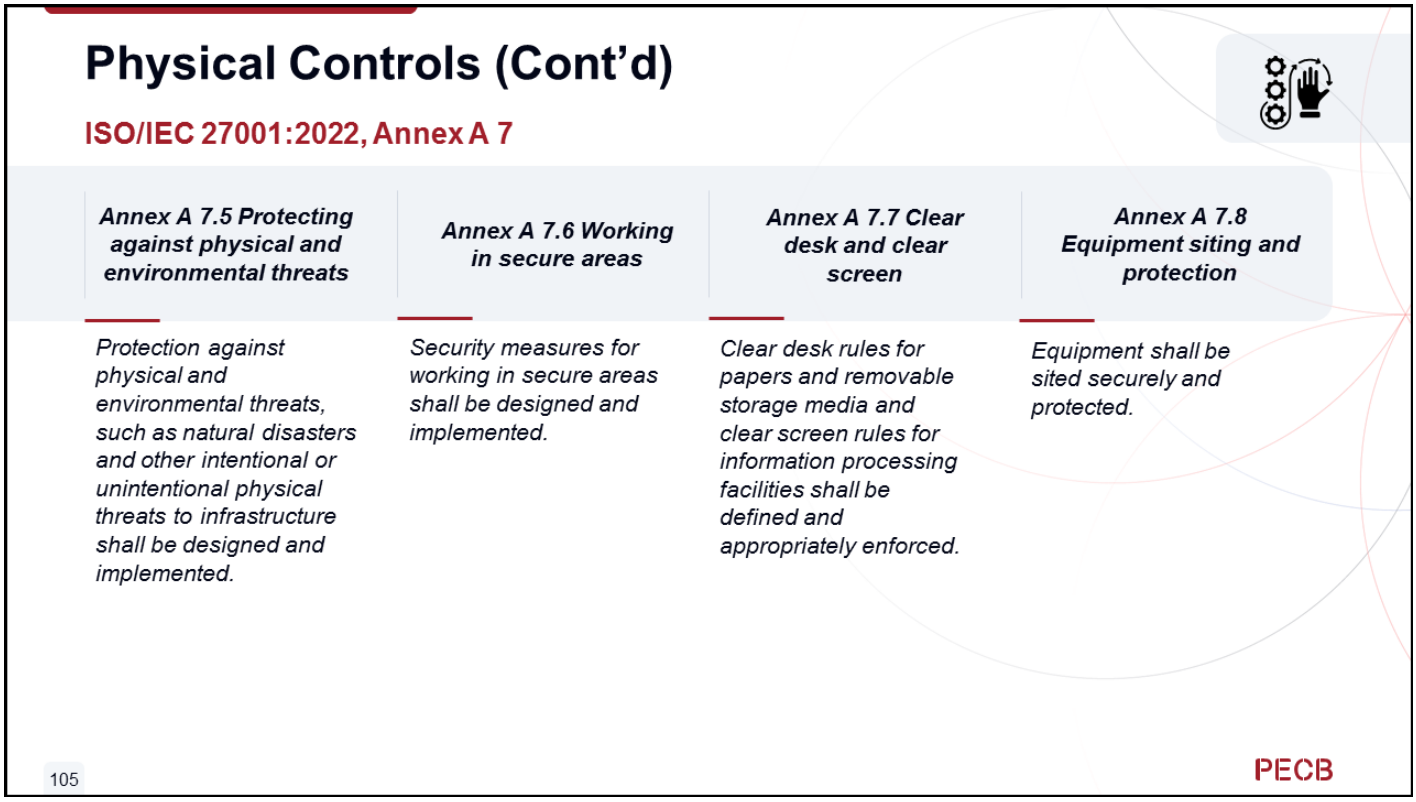
Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

ISO/IEC 27002, clause 7.4 Physical security monitoring

Purpose

To detect and deter unauthorized physical access.



ISO/IEC 27002, clause 7.5 Protecting against physical and environmental threats

Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

ISO/IEC 27002, clause 7.6 Working in secure areas

Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

ISO/IEC 27002, clause 7.7 Clear desk and clear screen

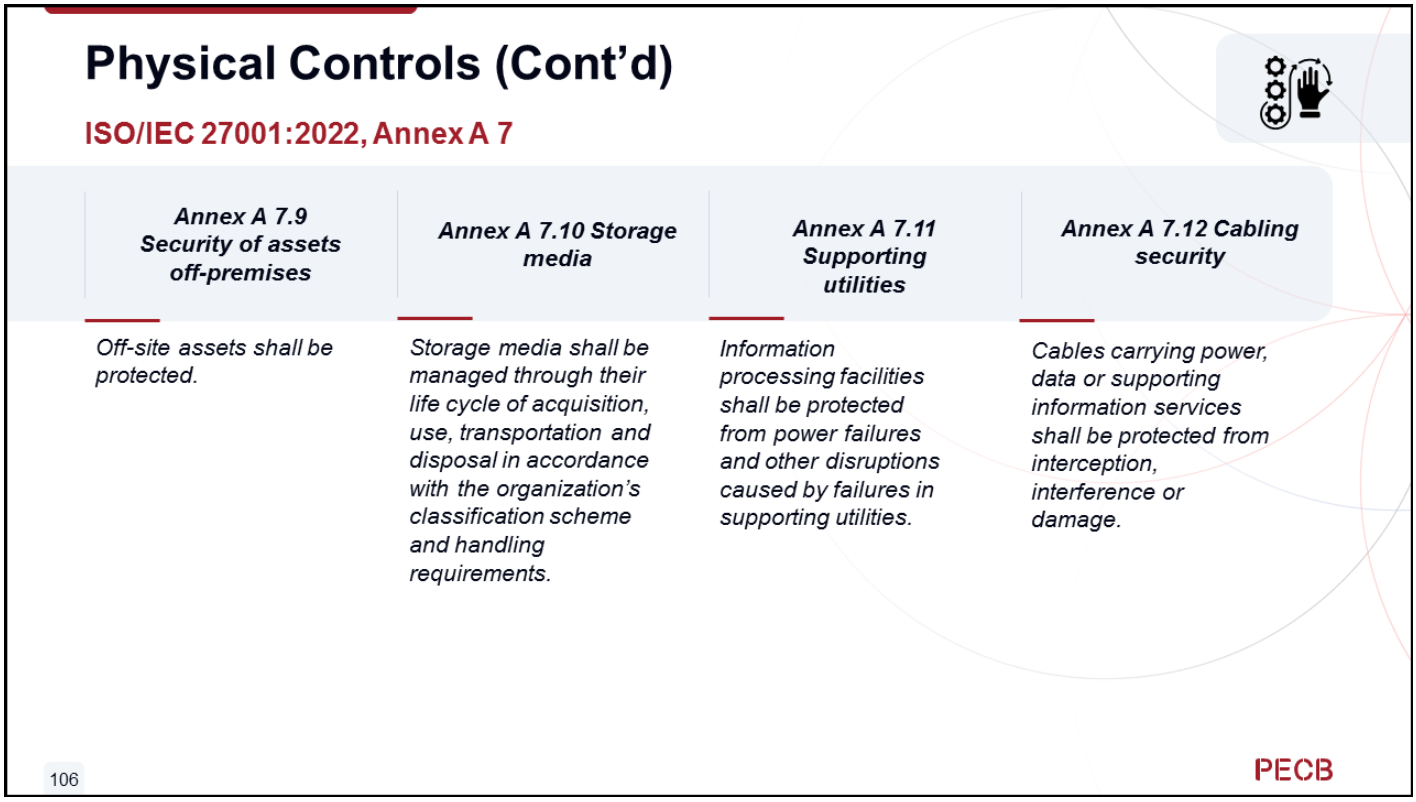
Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

ISO/IEC 27002, clause 7.8 Equipment siting and protection

Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.



ISO/IEC 27002, clause 7.9 Security of assets off-premises

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

ISO/IEC 27002, clause 7.10 Storage media

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

ISO/IEC 27002, clause 7.11 Supporting utilities

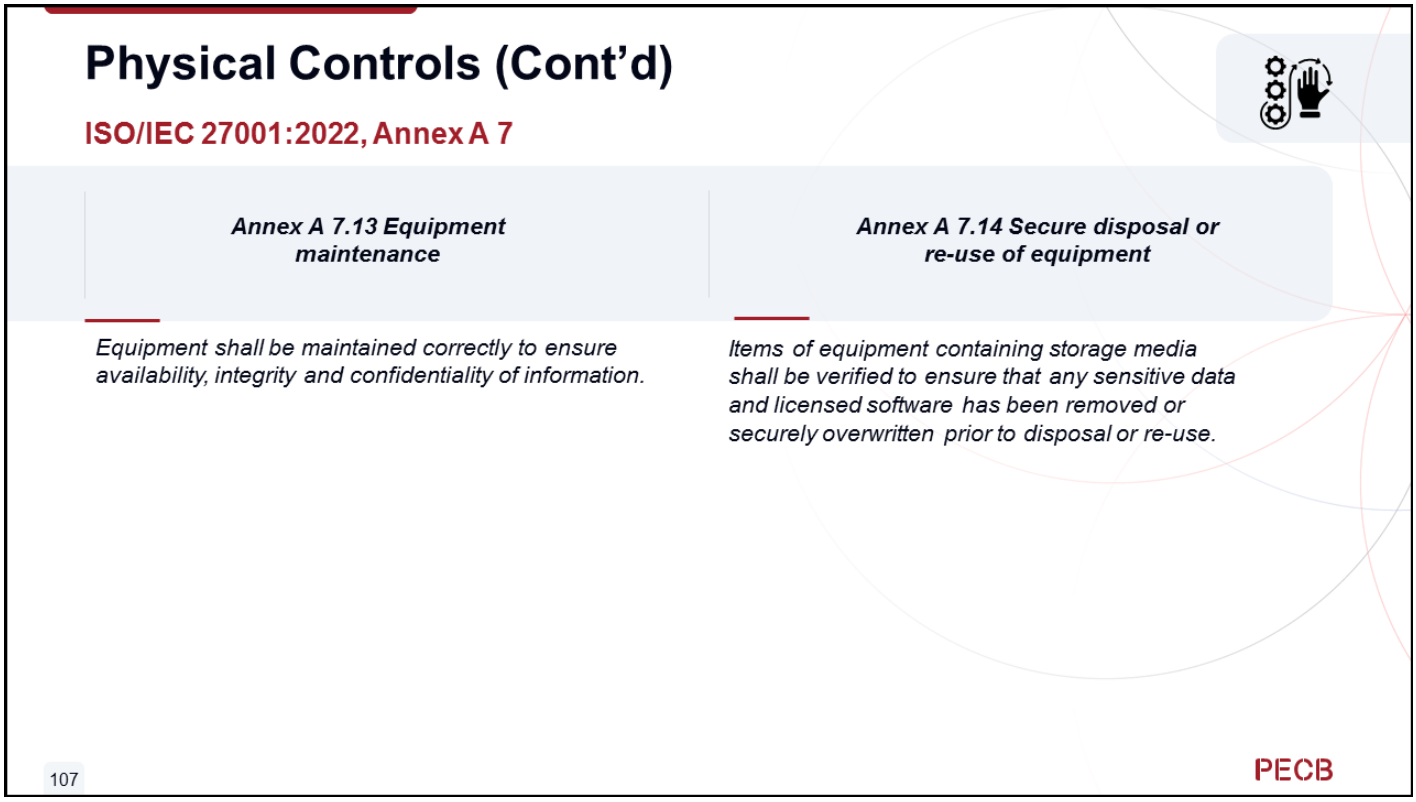
Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

ISO/IEC 27002, clause 7.12 Cabling security

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.



ISO/IEC 27002, clause 7.13 Equipment maintenance

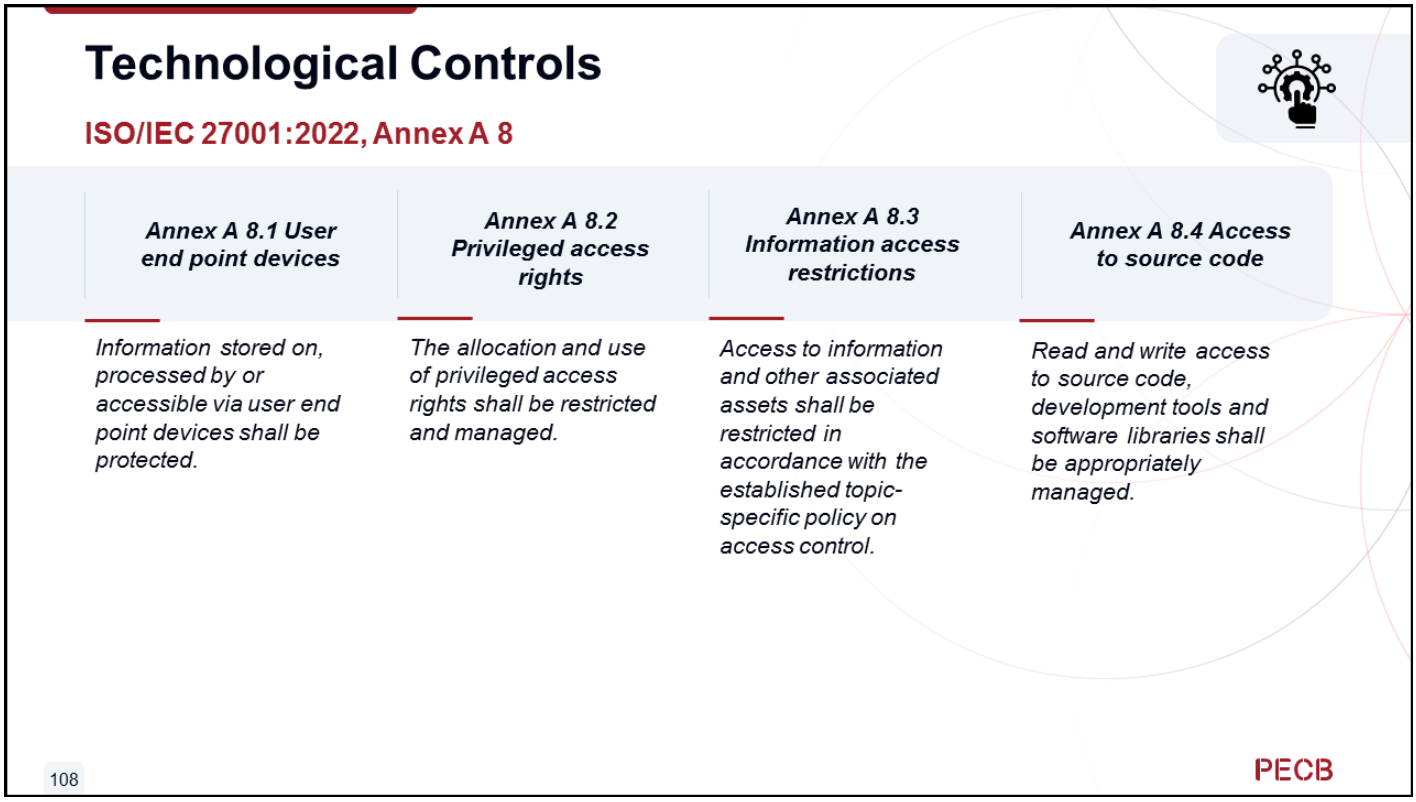
Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

ISO/IEC 27002, clause 7.14 Secure disposal or re-use of equipment

Purpose

To prevent leakage of information from equipment to be disposed or re-used.



ISO/IEC 27002, clause 8.1 User endpoint devices

Purpose

To protect information against the risks introduced by using user endpoint devices.

ISO/IEC 27002, clause 8.2 Privileged access rights

Purpose

To ensure only authorized users, software components and services are provided with privileged access rights.

ISO/IEC 27002, clause 8.3 Information access restrictions

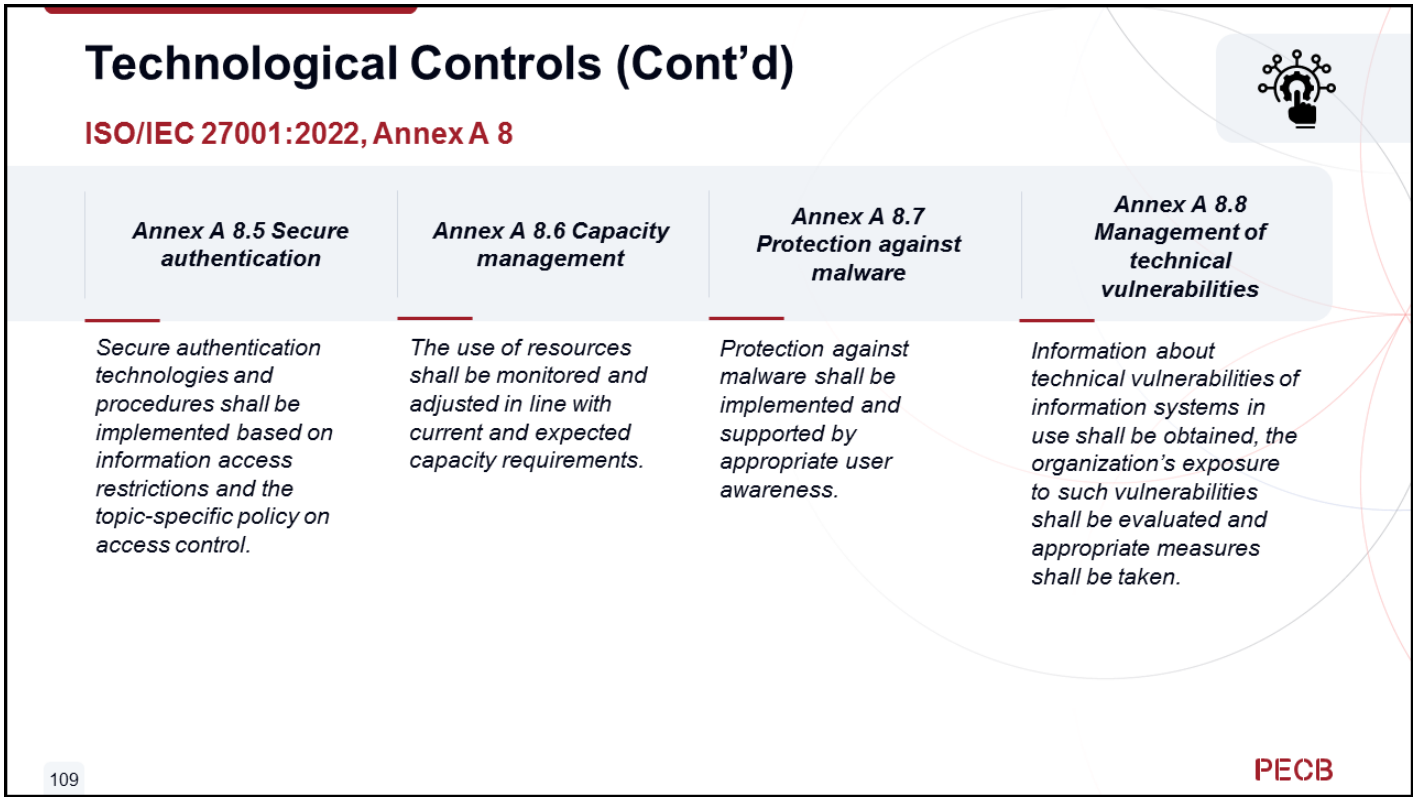
Purpose

To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

ISO/IEC 27002, clause 8.4 Access to source code

Purpose

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.



ISO/IEC 27002, clause 8.5 Secure authentication

Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

ISO/IEC 27002, clause 8.6 Capacity management

Purpose

To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

ISO/IEC 27002, clause 8.7 Protection against malware

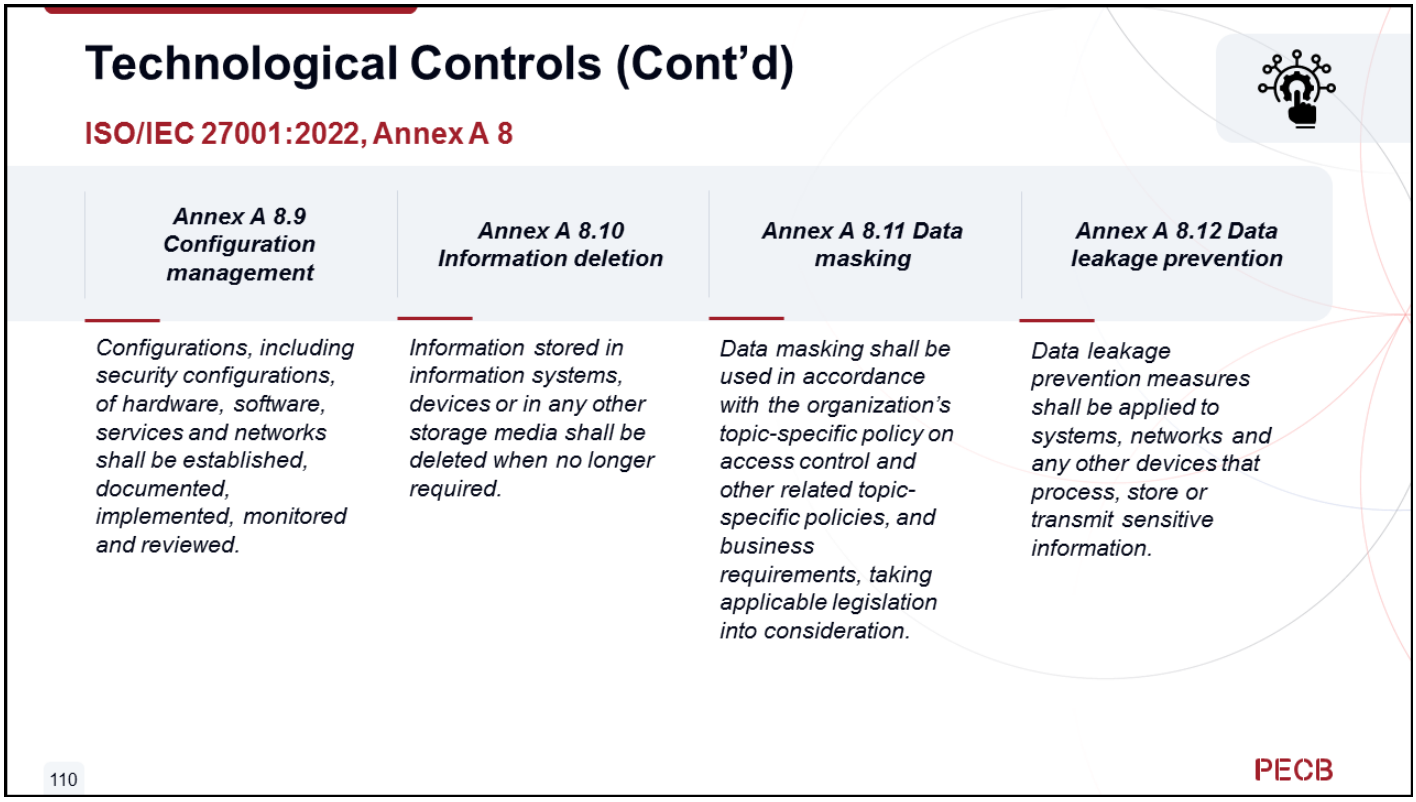
Purpose

To ensure information and other associated assets are protected against malware.

ISO/IEC 27002, clause 8.8 Management of technical vulnerabilities

Purpose

To prevent exploitation of technical vulnerabilities.



ISO/IEC 27002, clause 8.9 Configuration management

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

ISO/IEC 27002, clause 8.10 Information deletion

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

ISO/IEC 27002, clause 8.11 Data masking

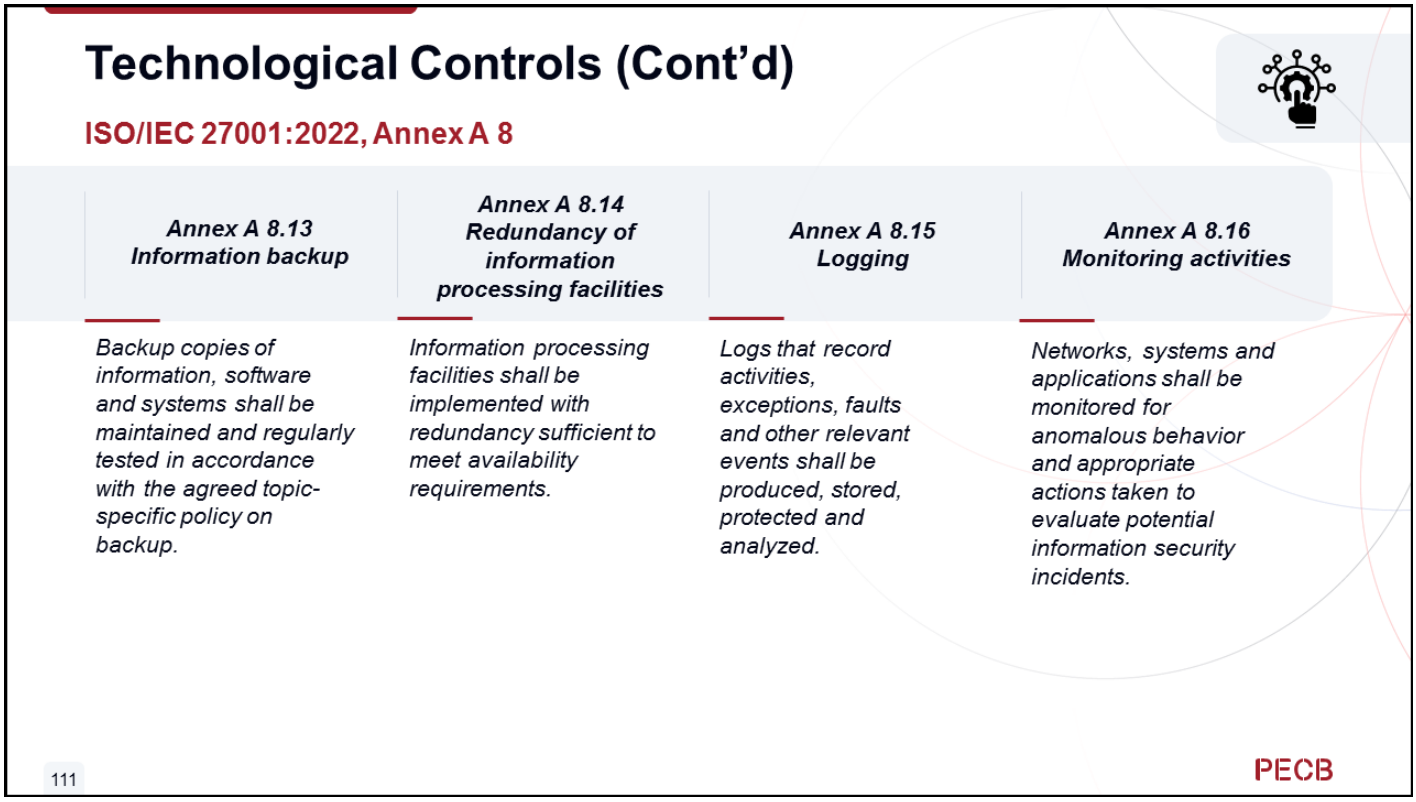
Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

ISO/IEC 27002, clause 8.12 Data leakage prevention

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.



ISO/IEC 27002, clause 8.13 Information backup

Purpose

To enable recovery from loss of data or systems.

ISO/IEC 27002, clause 8.14 Redundancy of information processing facilities

Purpose

To ensure the continuous operation of information processing facilities.

ISO/IEC 27002, clause 8.15 Logging

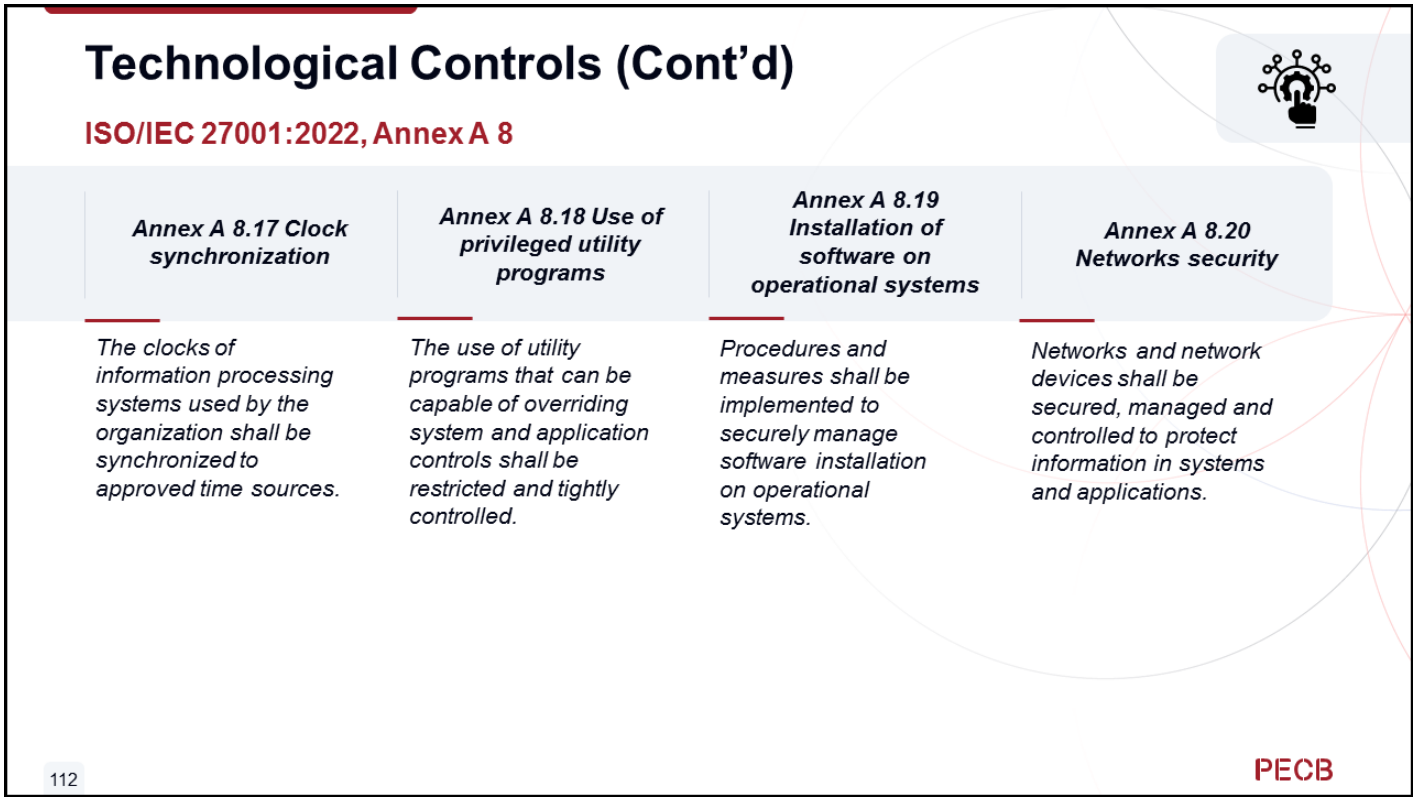
Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

ISO/IEC 27002, clause 8.16 Monitoring activities

Purpose

To detect anomalous behavior and potential information security incidents.



ISO/IEC 27002, clause 8.17 Clock synchronization

Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

ISO/IEC 27002, clause 8.18 Use of privileged utility programs

Purpose

To ensure the use of utility programs does not harm system and application controls for information security.

ISO/IEC 27002, clause 8.19 Installation of software on operational systems

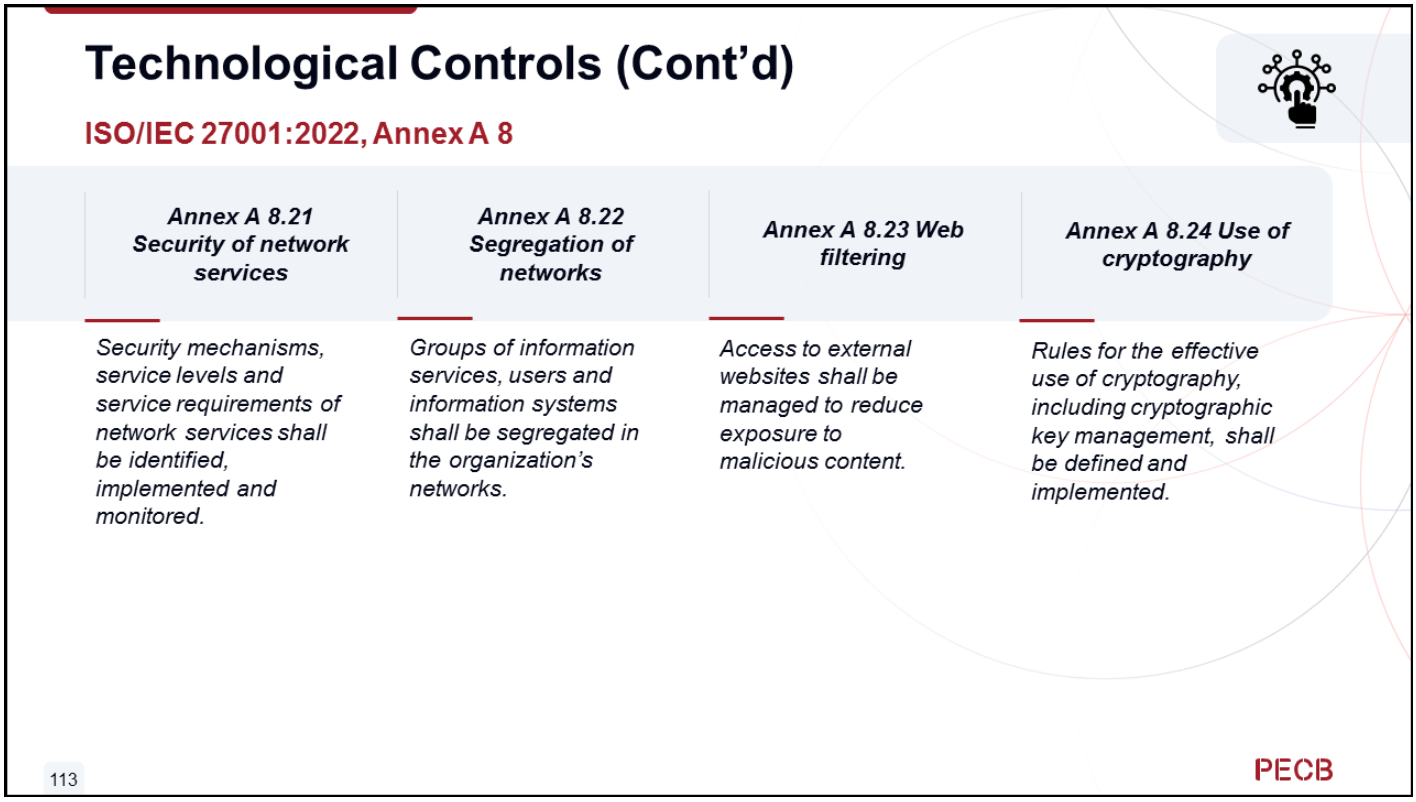
Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

ISO/IEC 27002, clause 8.20 Networks controls

Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network.



ISO/IEC 27002, clause 8.21 Security of network services

Purpose

To ensure security in the use of network services.

ISO/IEC 27002, clause 8.22 Segregation of networks

Purpose

To split the network in security boundaries and to control traffic between them based on business needs.

ISO/IEC 27002, clause 8.23 Web Filtering

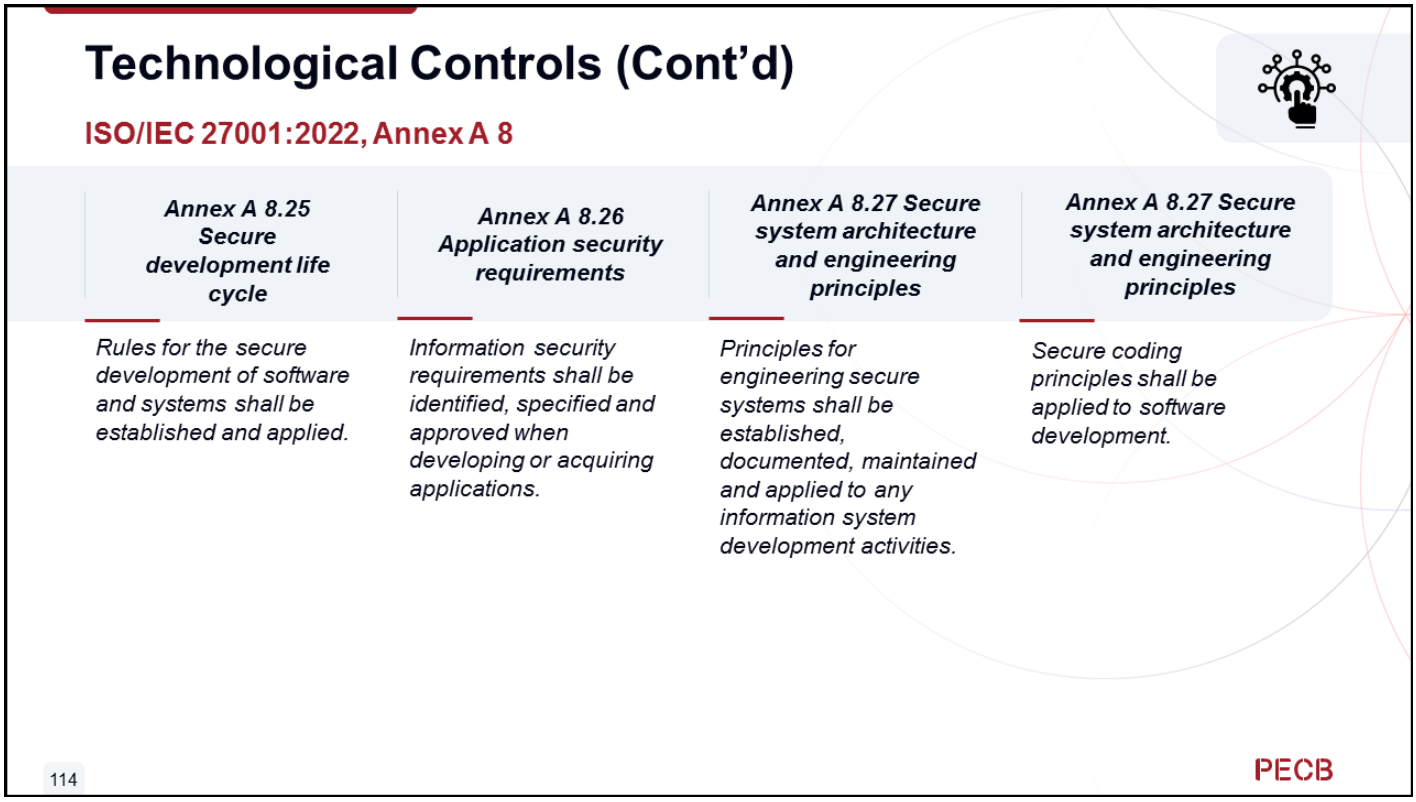
Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

ISO/IEC 27002, clause 8.24 Use of cryptography

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.



ISO/IEC 27002, clause 8.25 Secure development life cycle

Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

ISO/IEC 27002, clause 8.26 Application security requirements

Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications.

ISO/IEC 27002, clause 8.27 Secure system architecture and engineering principles

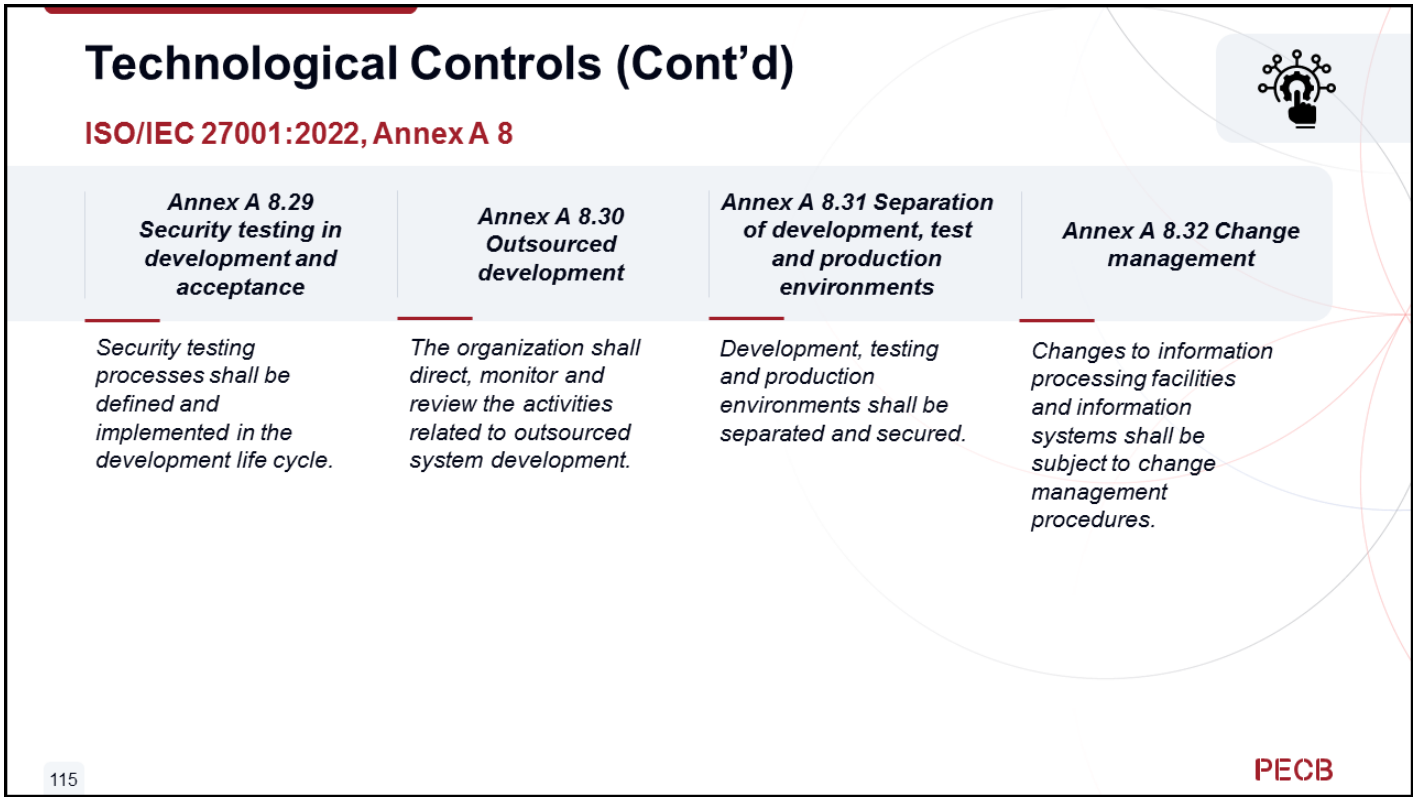
Purpose

To ensure information systems are securely designed, implemented and operated within the development life cycle.

ISO/IEC 27002, clause 8.28 Secure coding

Purpose

To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.



ISO/IEC 27002, clause 8.29 Security testing in development and acceptance

Purpose

To validate if information security requirements are met when applications or code are deployed to the production environment.

ISO/IEC 27002, clause 8.30 Outsourced development

Purpose

To ensure information security measures required by the organization are implemented in outsourced system development.

ISO/IEC 27002, clause 8.31 Separation of development, test and production environments

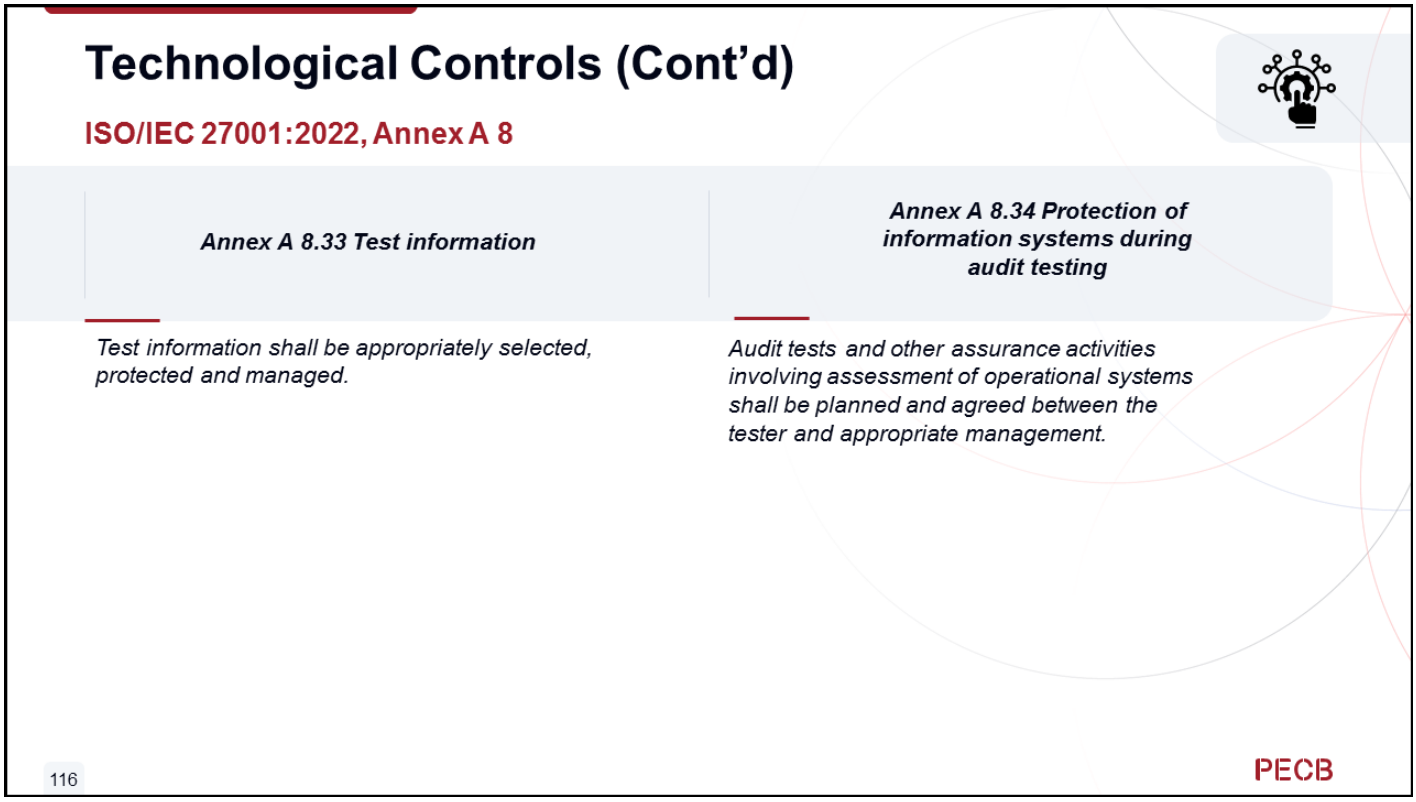
Purpose

To protect the production environment and data from compromise by development and test activities.

ISO/IEC 27002, clause 8.32 Change management

Purpose

To preserve information security when executing changes.



ISO/IEC 27002, clause 8.33 Test information

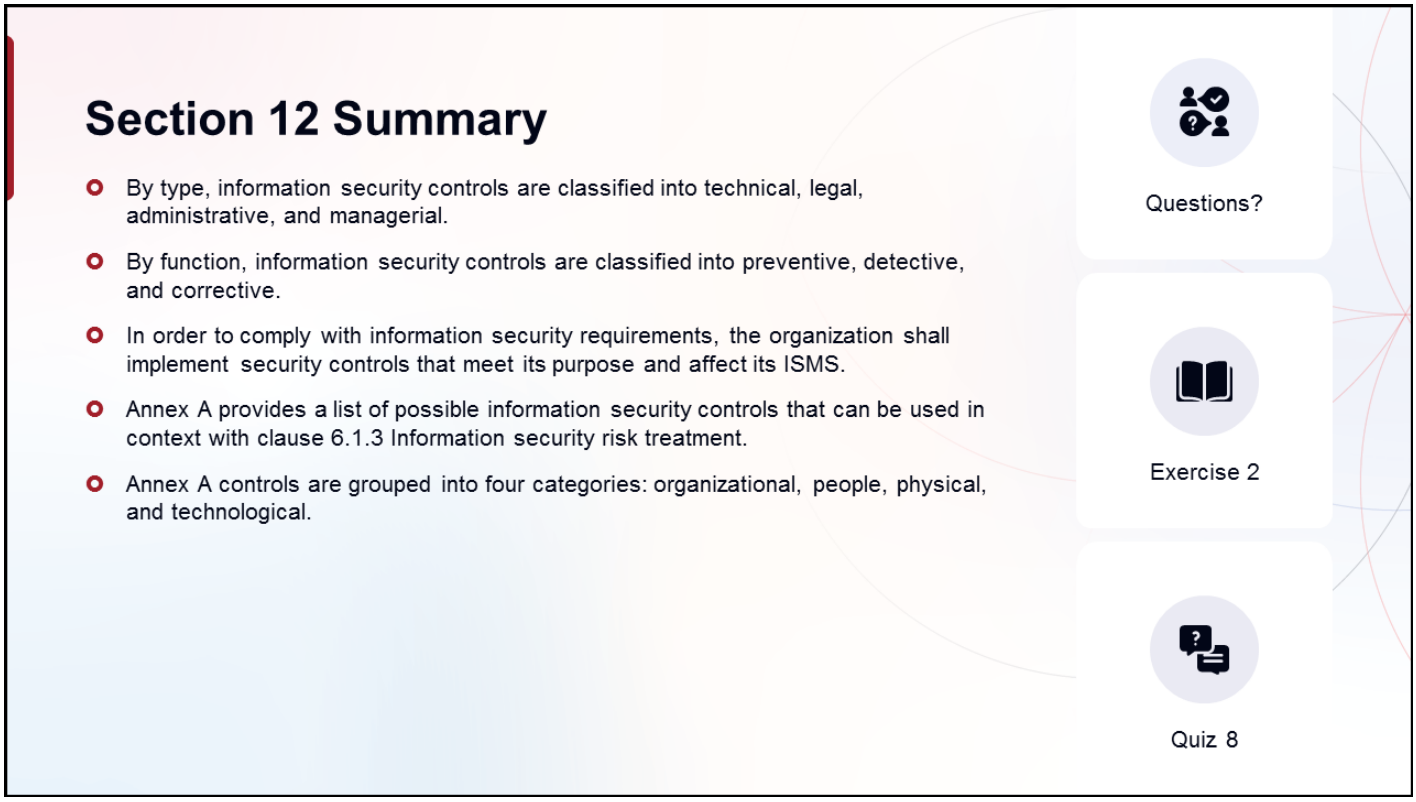
Purpose

To ensure relevance of testing and protection of operational information used for testing.

ISO/IEC 27002, clause 8.34 Protection of information systems during audit testing

Purpose

To minimize the impact of audit and other assurance activities on operational systems and business processes.



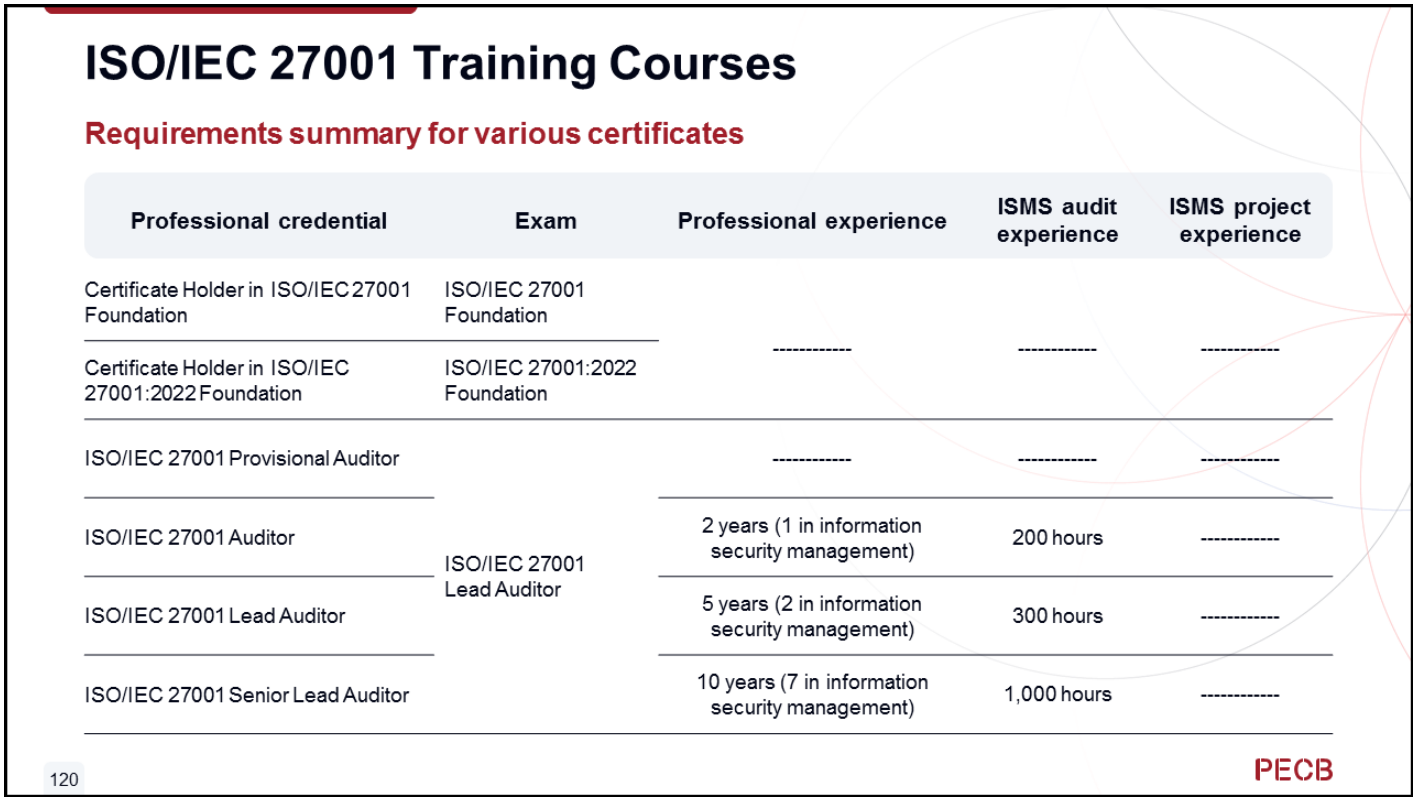
Note: To complete Exercise 2 and Quiz 7, please go to the Exercises Worksheet and Quizzes Worksheet, respectively.

Day 2 Summary

The following topics were covered on the second day of this training course:

- Risk management process and risk assessment methodology
- Resource management
- Training, awareness, and communication
- Change management
- Monitoring, measurement, analysis, and performance evaluation
- Corrective actions and continual improvement
- Internal and external audits
- Management reviews
- Nonconformities
- Introduction of Annex A controls

This section provides a requirements summary for various ISO/IEC 27001 certificates as well as information on the certificate program process, other PECB services, and other PECB training courses.



The **"Foundation"** certificate recognizes that individuals understand the basic concepts, methods, and techniques used for the effective management of a management system.

The main auditor certificates:

1. The "**Certified Provisional Auditor**" recognizes that individuals possess the basic knowledge about auditing and that they can be a member of an audit team.
2. The "**Certified Auditor**" recognizes that individuals have the necessary knowledge to participate in an audit and that they possess the basic skills to conduct a management system certification audit having been members of an audit team.
3. The "**Certified Lead Auditor**" recognizes that individuals have mastered the audit techniques and demonstrate the audit competences to manage an audit team.
4. The "**Certified Senior Lead Auditor**" is targeted toward professionals who have extensive experience in auditing.

ISO/IEC 27001 Training Courses (cont'd)

Requirements summary for various certificates

Professional credential	Exam	Professional experience	ISMS audit experience	ISMS project experience
ISO/IEC 27001 Provisional Implementer	ISO/IEC 27001 Lead Auditor	----------	----------	----------
ISO/IEC 27001 Implementer		2 years (1 in information security management)	----------	200 hours
ISO/IEC 27001 Lead Implementer		5 years (2 in information security management)	----------	200 hours
ISO/IEC 27001 Senior Lead Implementer		10 years (7 in information security management)	----------	1,000 hours
ISO/IEC 27001 Master	ISO/IEC 27001 LA + LI (four additional Foundation exams)	15 years (10 in information security management)	700 hours	700 hours

121

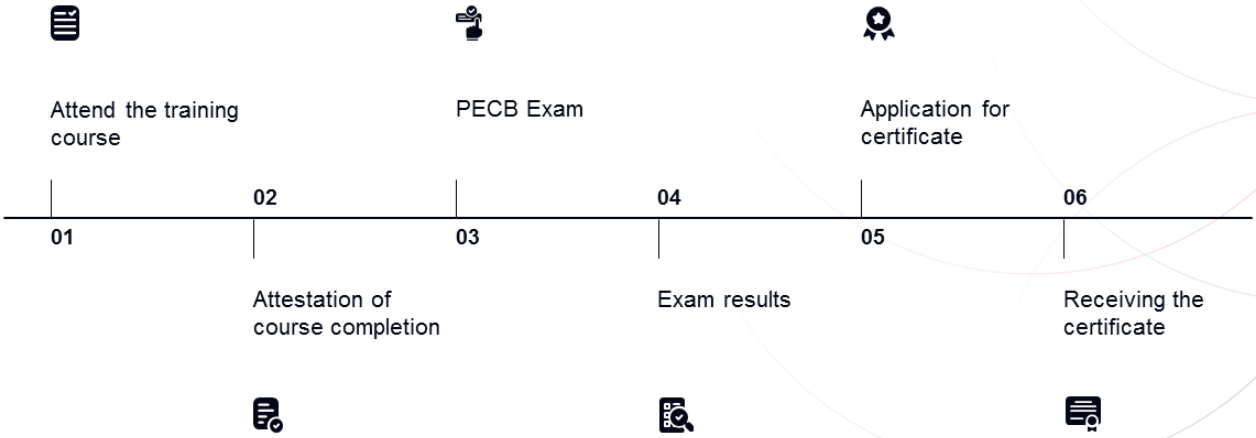
PECB

The main implementer certificates:

1. The "**Certified Provisional Implementer**"recognizes that individuals have the basic knowledge to participate in the implementation and management of a management system.
2. The "**Certified Implementer**" recognizes that individuals have the necessary knowledge to participate in the implementation and management of a management system.
3. The "**Certified Lead Implementer**"recognizes that individuals are equipped with the skills needed to implement a management system and possess the competences of managing a team.
4. The "**Certified Senior Lead Implementer**" is targeted toward professionals who have extensive experience in implementation projects.

The "**Master**" certificate recognizes that individuals have mastered the basic concepts, approaches, methods, and techniques to lead an audit team and to lead the implementation of a management system.

PECB Certificate Program Process



PECB

2. Attestation of Course Completion

After completing the training course and submitting the **Training Course Evaluation Form**, an Attestation of Course Completion will be generated at myPECB Dashboard, under the **My Courses** tab. The Attestation of Course Completion is worth 14 CPD credits.


PECB BEYOND RECOGNITION

Attestation of Course Completion

This document confirms that

John Doe

Has completed the

ISO/IEC 27001:2022 Foundation Training Course

This attestation of course completion is worth 14 Continuing Professional Development (CPD*) credits.

City/Country Location: XX, XX
Course Completion Date: 2022-01-01

This document is not a PECB Professional Certificate.

*1 CPD credit is worth 1 hour of activity. For more information, consult the PECB CPD policy.

123

PECB

Note: It is important to not confuse the Attestation of Course Completion with the actual certificate. The former is only a confirmation of having participated a training course, not gaining a certificate. To obtain a certificate, candidates will have to pass the exam, go through the application process, and get the certificate once the evaluation of the application is completed.

We strive to constantly improve the quality and the practical relevance of our trainings. Therefore, your opinion on this training is of great value to us.

We would be very grateful if you could provide us with your evaluation of the training course and the trainer(s).

Moreover, if you have any suggestions for improving PECB's training course materials, we would like to hear from you. Please open a ticket directed to the Training Development Department on PECB's website (https://pecb.com) in the**Contact Us**section. We thoroughly read and evaluate the input we get from our members. Another way of providing feedback for training course materials is via the Kate application.

In case of dissatisfaction with the training (trainer, training room, equipment, etc.), the examination, or the certification processes, please open a ticket under the **Make a complaint** category on PECB's website (https://pecb.com) in the **Contact Us** section.

3. PECB Exam

The objective of the exam is to ensure that candidates have understood the basic concepts of an information security management system based on ISO/IEC 27001:2022.

The exam for this training course is going to be in the **multiple-choice format.**

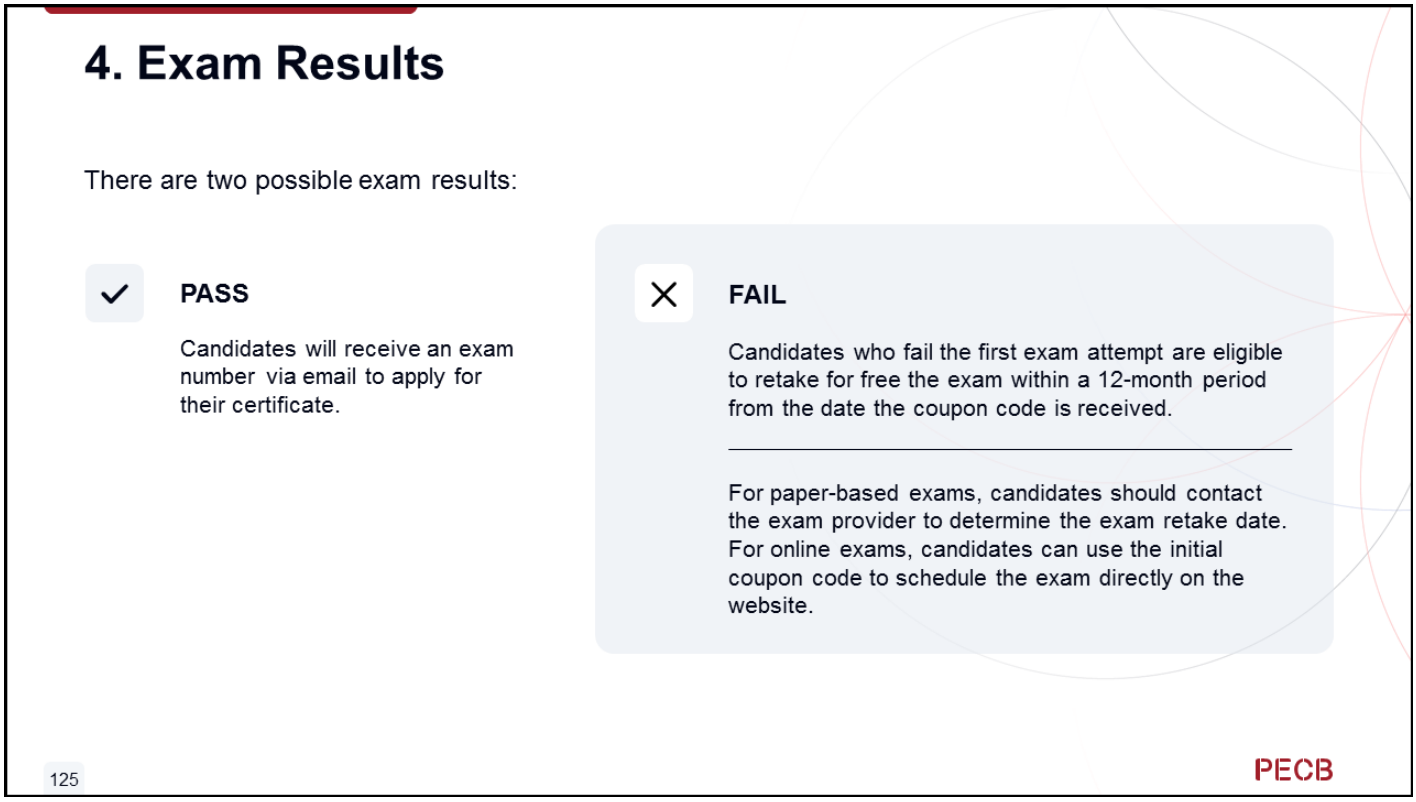
For specific information about exam types, languages available, and other details, please visit the PECB website at https://pecb.com.

For more information about the examination process, please visit https://pecb.com/examination-rules-and-policies.

124

PECB

- The PECB Examination Committee ensures that the development and adequacy of the exam questions are maintained based upon current professional practice.
- To take an exam in a particular language, please ask the trainer or contact us by sending an email to examination@pecb.com.
- All competency domains are covered in the exam. To read a detailed description of each competency domain, please visit the PECB website at https://pecb.com.



Exams are reviewed by qualified examiners who are assigned anonymously.

To ensure independence and impartiality and to avoid conflicts of interest, trainers, training course organizers, and invigilators do not participate in the exam review process or the certificate provision process.

In case candidates fail the exam, an explanation will be provided to them about the domains that they failed to demonstrate the required competence. To retake the exam, candidates must contact the head of the training organization.

5. Application for Certificate

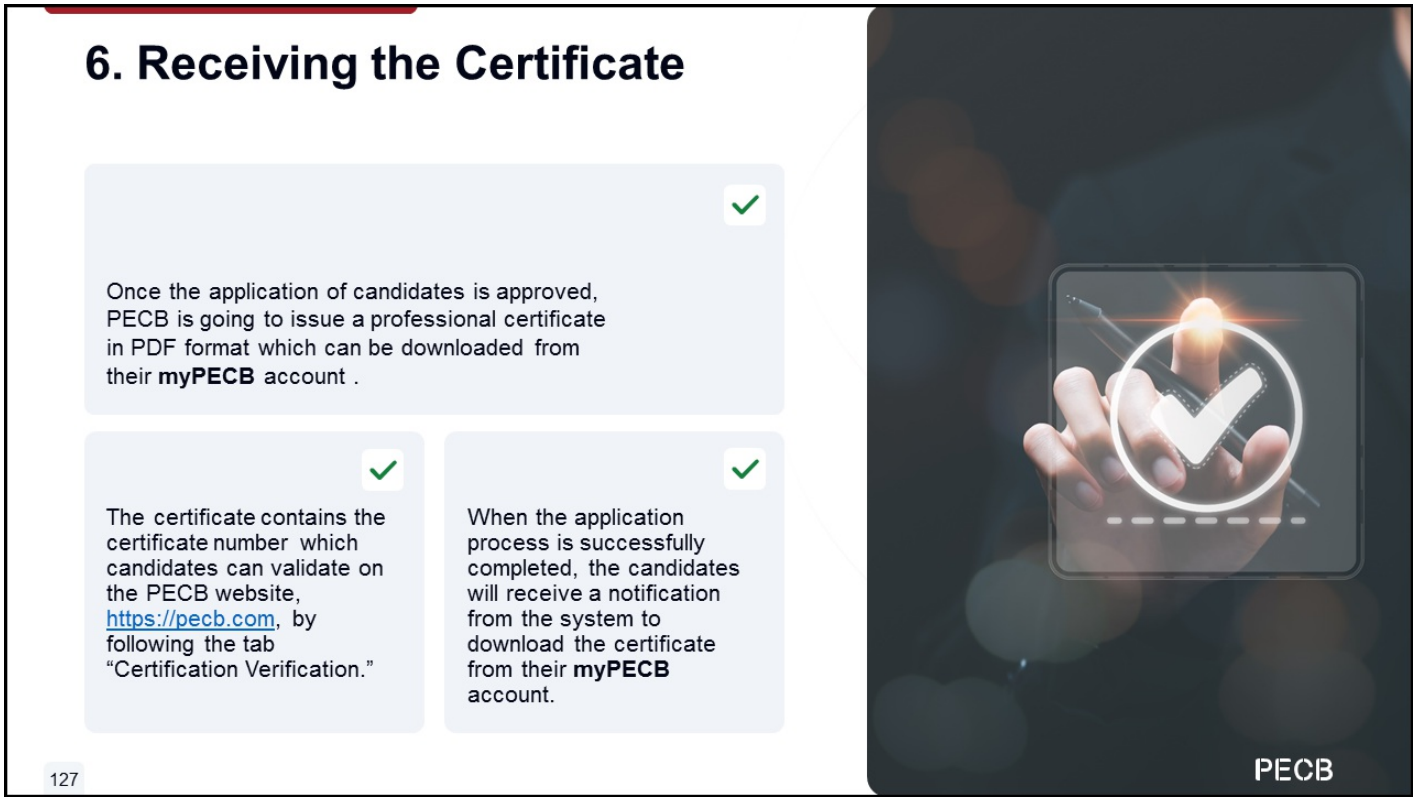
General process

- After successfully passing the exam, candidates can apply online to get their PECB certificate at https://pecb.com.
- Candidates have a maximum period of one year to submit a professional file in order to obtain the certificate.
- Candidates must complete the whole cycle of the training course, first exam attempt and retake (if applicable), and certification application within a year from the last day of the training course.
- For more information about the certificate program process, please visit https://pecb.com/certification-rules-and-policies.

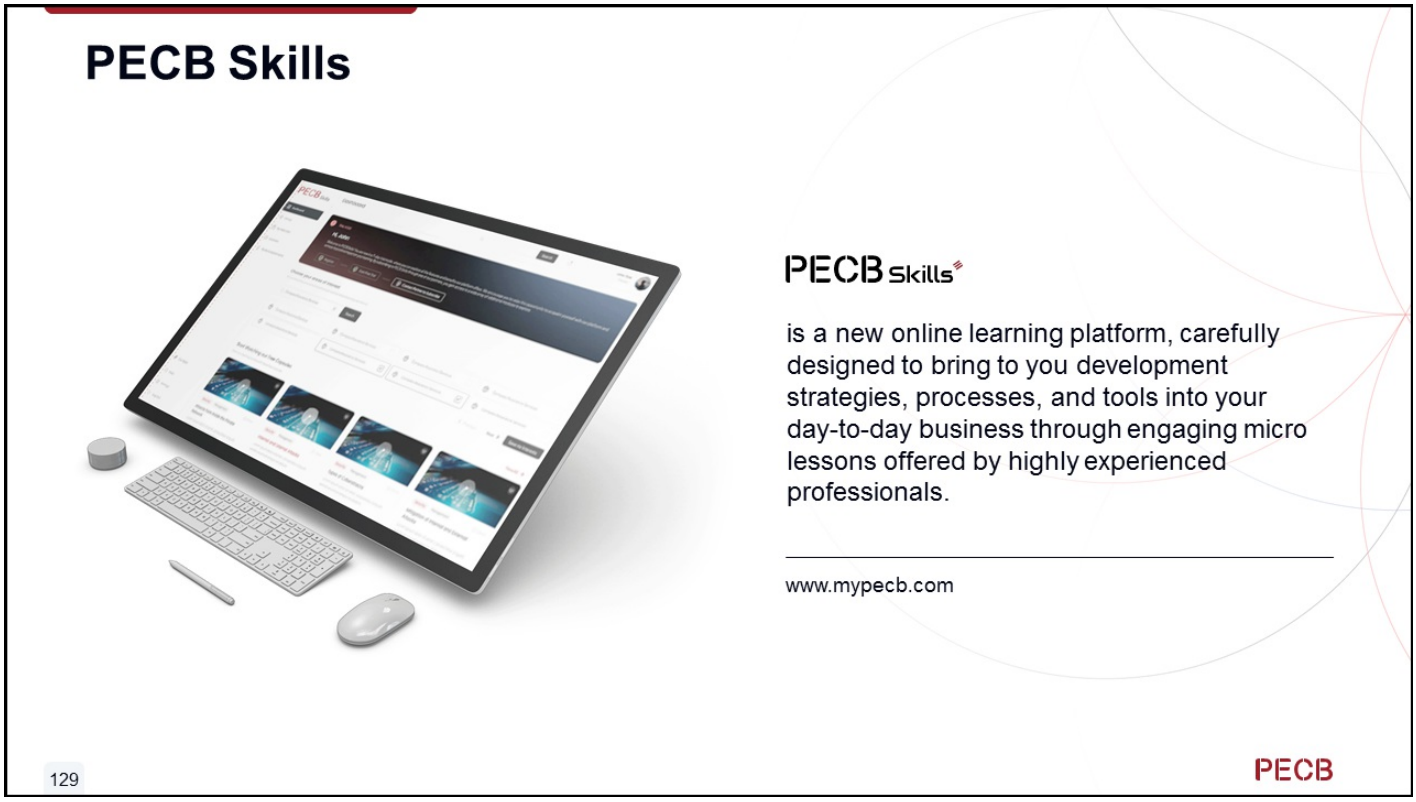
126

PECB

When applying, candidates must provide their contact details. Candidates should write their name as they wish it to appear on their certificate (in ASCII format). Before submitting their certificate application, candidates should make sure to review the accuracy of the contact details they have provided when creating their PECB account. The certificate will be issued with the name that they provided when they created the account. To update the name in their PECB account, candidates should contact support@pecb.com.



PECB has partnered with Credly to offer you the chance to claim a digital badge. You can share the badges online safely and easily. For more information, please go to https://pecb.com/pecb-digital-badges.



PECB Skills offers interactive micro lessons for all core content areas and more, thus providing professionals with a plethora of choices.

- **Information security:** Equip yourself with the skills to protect vital data and maintain the integrity of information systems
- **Cybersecurity:** Stay vigilant and ahead of cyber threats with best practices and advanced techniques
- **Privacy and data protection:** Delve into the critical aspects of safeguarding personal data and ensuring privacy in an interconnected world
- **Risk management:** Navigate through uncertainties with confidence, identifying and mitigating potential risks
- **Continuity, resilience, and recovery:** Learn to build robust systems, ensuring business continuity even in unforeseen circumstances
- **CMMC (Cybersecurity Maturity Model Certification):** Familiarize yourself with the defense standard for ensuring cybersecurity throughout the Defense Industrial Base (DIB)
- **GDPR (General Data Protection Regulation):** Master the European Union's benchmark regulation on data protection and privacy
- **NIST (National Institute of Standards and Technology):** Engage with guidelines and standards for ensuring cybersecurity and privacy, backed by one of the most reputable institutions in the field

With PECB Skills, you're not just learning; you are future-proofing your career and making strides in the dynamic digital ecosystem. For more information, please visit www.mypecb.com or contact us at marketing@pecb.com.

PECB Skills Certificates

Elevate your profile and unlock new opportunities through these recognitions which will further enhance your professional standing and growth:

- **Attestation of module completion:** Demonstrate proficiency in specific modules and receive 1 CPD credit.
- **Essentials certificate:** Demonstrate your competencies through a comprehensive 4-hour program, earning 4 CPD credits.

130

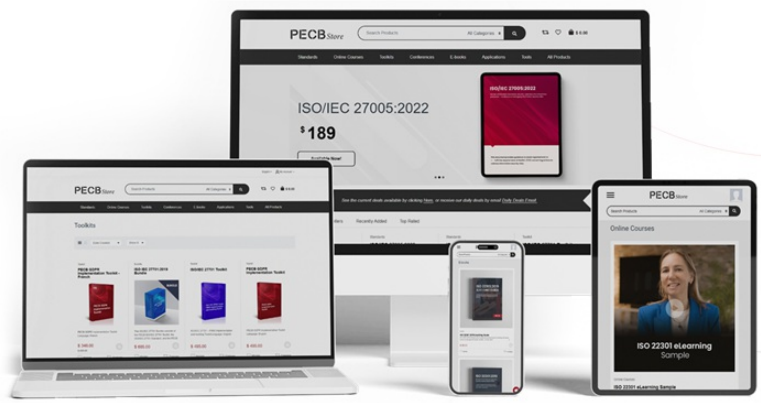
PECB

Our micro-courses are accredited by the ANSI National Accreditation Board (ANAB), a testament to their quality and adherence to rigorous educational standards.

Note: Modules comprise four short video capsules.

PECB Store

- Join PECB's online store and become part of our global network.
- Explore the wide range of standards, toolkits, and more.
- Advance your career from the comfort of your home through our digital platforms
- Buying online has never been easier!



https://store.pecb.com

131

PECB

PECB Store is PECB's online store where clients can purchase various ISO and IEC international standards, PECB Toolkits and eBooks, and many other related products and services that will be added in the future.

Standards mentioned on this training course are all available on PECB Store. We are committed to support the growth of our customers, which is why we offer you the opportunity to buy qualitative products on PECB Store and advance your professional career by applying the knowledge gained.

For more information, please visit https://store.pecb.com or contact us at store@pecb.com.

PECB Certified ISO/IEC 27001 Lead Implementer (five days)

This five-day intensive training course allows the participants to develop the skills to support an organization in the implementation and management of an information security management system (ISMS) based on ISO/IEC 27001. In addition, the participants will be able to acquire proficiency in the best practices for implementing information security controls from ISO/IEC 27002.

PECB Certified ISO/IEC 27001 Lead Auditor (five days)

The ISO/IEC 27001 Lead Auditor training course enables the participants to develop the necessary capabilities to perform an information security management system (ISMS) audit by applying widely recognized audit principles, procedures, and techniques. During this training course, the participants will acquire the knowledge and skills to plan and carry out internal and external audits in compliance with ISO 19011.

Thank You!


linkedin.com/company/pecb


facebook.com/PECBInternational/


instagram.com/pecb.official


x.com/pecb


youtube.com/pecbgroup

PECB