When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified ISO/IEC 38500 IT Governance Manager

The objective of the “PECB Certified ISO/IEC 38500 IT Governance Manager” examination is to ensure that the candidate has the knowledge and skills to support an organization in implementing, maintaining and managing an ongoing information security risk management program according to ISO/IEC 38500:2015.

The target population for this examination is:

- Project managers or consultants wanting to prepare and to support an organization in the implementation of corporate governance of Information Technology
- ISO/IEC 38500 auditors who wish to fully understand the corporate governance of IT implementation process
- Senior Managers responsible for the IT governance of an enterprise and the management of its risks
- Members of groups monitoring the resources within the organization
- External business or technical specialists, such as legal or accounting specialists, retail associations, or professional bodies
- Vendors of hardware, software, communications and other IT products
- Internal and external service providers (including consultants)

The exam content covers the following domains:

- Domain 1 : Principles for good Corporate Governance of IT
- Domain 2 : Evaluate-Direct-Monitor Model of ISO/IEC 38500
- Domain 3 : Guidance for the Corporate Government of IT
- Domain 4 : Evaluate the need and applicability of each principle
- Domain 5 : Direct the adherence to each principle
- Domain 6 : Monitor all or key activities related to all the principles

The content of the exam is divided as follows:

Domain 1: Principles for good Corporate Governance of IT

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can understand, interpret and illustrate the main IT Governance management concepts and guidelines related to Corporate Governance of IT based on ISO/IEC 38500.

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the development of Corporate Governance of IT principles. 2. Ability to identify, analyze and evaluate the guidance coming from information technology frameworks for an organization. 3. Ability to explain and illustrate the main concepts in IT Corporate Governance. 4. Ability to understand relationship between different standards	1. Knowledge of the guiding principles provided by the framework for the use of Information Technology. 2. Knowledge of the main standards in information technology 3. Knowledge of the different sources of information technology frameworks for an organization: laws, regulations, international and industry standards, contacts, market practices and internal policies 4. Knowledge of the main information security concepts and terminology

Domain 2: Evaluate-Direct-Monitor Model of ISO/IEC 38500

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can evaluate direct and monitor the use of information technology based on the IT Governance Model provided by ISO/IEC 38500.

Competencies	Knowledge statements
1. Ability to evaluate, direct and monitor the use of information technology (IT) in organizations by complying with the IT Governance Model provided by ISO/IEC 38500. 2. Ability to evaluate the current and future use of information technology by organizations 3. Ability to direct the preparation and implementation of plans and policies to ensure that the use of information technology meets organizations requirements 4. Ability to monitor the conformance of policies and performance of information technology	1. Knowledge of the concepts, principles and terminology related to guidance on corporate governance management. 2. Knowledge on the current and future use of IT, including plans, proposals and supply arrangements whether internal or external. 3. Knowledge on implementation of strategies that set direction for investments in IT and policies that establish sound behavior in the use of IT. 4. Knowledge of the measurement systems that help in monitoring the performance of IT

Domain 3: Guidance for the Corporate Government of IT

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can understand, interpret and apply the provided guidance for the general principles of good governance of IT.

Competencies	Knowledge statements
1. Understand, explain and illustrate the application of the sub-clauses that provide guidance for the general principles of governance of IT 2. Ability to assign roles and responsibilities in respect of the organization's current and future use of IT 3. Ability to understand, analyze needs and provide guidance on the attribution of roles and responsibilities in the context of the implementation and management of an information technology framework 4. Ability to determine if strategies are followed according to the assigned IT responsibilities and to monitor IT governance mechanisms 5. Ability to establish GEIT Project team and project plan	1. Knowledge of the sub clauses that provide guidance for the general principles of governance of IT 2. Knowledge on the evaluation of options for assigning roles and responsibilities in respect of the organization's current and future use of IT 3. Knowledge of the roles and responsibilities of the key actors during the implementation of information technology framework. 4. Knowledge of identification of IT Governance mechanisms and ensure their appropriateness 5. Knowledge of the competencies and skills needed for the GEIT Project Plan when selecting the GEIT project team members

Domain 4: Evaluate the need and applicability of each principle

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can evaluate the strategic alignment of ISO/IEC 38500 principles and organization's objectives

Competencies	Knowledge statements
1. Ability to determine IT the overall plan which compromises objectives, tactics and principles related to the use of technology within an organization 2. Ability to evaluate and integrate the need and applicability of each IT Governance principle with the business strategy, IT strategy, business structure and IT structures 3. Ability to ensure that IT related activities contribute to the effective and efficient execution of the enterprise strategy 4. Ability to align IT strategy with enterprise strategy 5. Understand the strategic alignment model and alignment domain relationships 6. Understand the main strategy formulation steps 7. Ability to understand changes in business strategy and list the strategic alignment barriers 8. Ability to support business strategic alignment and IT 9. Ability to monitor the extent to which IT supports the organization 10. Ability to prioritize processes	1. Knowledge on organizations ongoing needs 2. Knowledge on IT activities and ensure they align with organization's objectives for changing circumstances 3. Knowledge on enterprises strategic plan, goals and expectations 4. Knowledge on IT strategy implementation plan and ensure plan endorsement by relevant parties 5. Knowledge of the strategic alignment model including business strategy, IT strategy, organizational infrastructure and processes and IS infrastructure and process 6. Knowledge of alignment domain relationships including strategic execution alignment, technology transformation alignment, competitive potential alignment and service level alignment 7. Knowledge of the four strategy formulation steps 8. Knowledge on IT related goals, changes in business strategy and barriers to strategic alignment 9. Knowledge of portfolio management goals and activities

Domain 5: Direct the adherence to each principle

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can evaluate, direct and monitor the adherence to each principle of IT governance

Competencies	Knowledge statements
1. Ability to evaluate, direct and monitor adherence to responsibility principle 2. Ability to evaluate, direct and monitor adherence to strategy principle 3. Ability to evaluate, direct and monitor adherence to acquisition principle 4. Ability to evaluate, direct and monitor adherence to performance principle 5. Ability to evaluate, direct and monitor adherence to conformance principle 6. Ability to evaluate, direct and monitor adherence to human behavior principle	1. Knowledge of the main options to evaluate, direct and monitor responsibilities assigned 2. Knowledge of the main developments in IT, business processes and business needs 3. Knowledge on the IT assets acquisition 4. Knowledge on how to measure the level of governance IT performance 5. Knowledge of risks faced by the organization related to IT governance 6. Knowledge of measurement methods that determine if governance IT support business processes 7. Knowledge on IT obligations such as regulatory, legislation, contractual, internal policies, standards and professional guidelines 8. Knowledge of measurement methods that determine if governance IT satisfies obligations

Domain 6: Monitor all or key activities related to all the principles

Main objective: To ensure that the ISO/IEC 38500 IT Corporate Governance Manager candidate can evaluate and monitor governance of IT performance and achieve effective strategic alignment with organizations objectives

Competencies	Knowledge statements
1. Ability to evaluate the extent to which IT satisfies obligations 2. Ability to evaluate organization's internal conformance to its system for governance of IT 3. Ability to monitor IT compliance and conformance through appropriate reporting and audit practices 4. Ability to monitor IT activities including disposal of assets and data 5. Ability to evaluate if governance of IT supports the business process 6. Ability to evaluate proposal plans that address the operations continuity and treatment of risk associated with the use of IT 7. Ability to evaluate the risk arising from IT-related activities	1. Knowledge on the extent to which IT satisfies obligations: regulatory, legislation, common law, contractual, internal policies, standards and professional guidelines 2. Knowledge on the performance measurement process 3. Knowledge of the measures taken to ensure effective performance of governance of IT 4. Knowledge of measurement objectives and benefits 5. Knowledge of the metrics defied in COBIT such as enterprise goals metrics, process goals metrics and IT-related goals metrics 6. Knowledge on proposed plans to ensure that IT supports the business process with the required capability and capacity 7. Knowledge on risk assessment methods

Based on these 6 domains and their relevance, 5 questions are included in the exam, as summarized in the following table:

			Level of Understanding (Cognitive/Taxonomy) Required					
		Points per Question	Questions that measure Comprehension, Application and Analysis	Questions that measure Synthesis and Evaluation	Number of Questions per competency domain	% of test devoted to each competency domain	Number of Points per competency domain	% of Points per competency domain
Competency/Domains	Principled for good Corporate Governance of IT	10	X		1	20.00	10	20.00
	Evaluate-Direct-Monitor Model of ISO/IEC 38500	10	X		1	20.00	10	20.00
	Guidance for the Corporate Government of IT	10	X		1	20.00	10	20.00
	Evaluate the need and applicability of each principle	10		X	1	20.00	10	20.00
	Direct the adherence to each principle							
	Monitor all or key activities related to all the principles	10		X	1	20.00	10	20.00
Total points		50						
Number of Questions per level of understanding			3	2				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			66.67	33.33				

The passing score is established at **70%.**

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified ISO/IEC 38500 IT Governance Manager, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the late arrival and may be denied entry to the exam room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates will need to present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is two (2) hours.

The questions are essay type questions. This type of format was chosen because the intent is to determine whether an examinee can write a clear coherent answer/argument and to assess problem solving techniques. Because of this particularity, the exam is set to be "open

book" and does not measure the recall of data or information. The examination evaluates, instead, comprehension, application, analysis, synthesis and evaluation, which mean that even if the answer is in the course material, candidates will have to justify and give explanations, to show they really understood the concepts. At the end of this document, you will find sample exam questions and their possible answers.

As the exams are "open book"; candidates are authorized to use the following reference materials:

- A copy of the ISO/IEC 38500:2015 standard,
- Course notes from the Participant Handout,
- Any personal notes made by the student during the course and
- A hard copy dictionary.

The use of electronic devices, such as laptops, cell phones, etc., is not allowed.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email in a period of 6 to 8 weeks, after taking the exam. The results will not include the exact grade of the candidate, only a mention of pass or fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied with the list of domains in which the candidate had a low grade, to provide guidance for exams' retake preparation.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limitation on how many times a candidate can retake the same exam. However, there are some limitations in terms of allowed time-frame in between exams.

When candidates fail the examination, they are only allowed to retake the examination once within 12 months after the first attempt. If second examination is unsuccessful, candidates will be allowed to retake the exam only after 1 year (12 months). Retake fee applies.

Only candidates, who have completed a full PECB training but fail the written exam, are eligible to retake the exam for free, under one condition:

"A candidate can only retake the exam once and this retake must occur within 12 months from the initial exam's date."

When candidates fail the same examination for the second time, their file is automatically closed for 1 year.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behaviour of certificate holders and applicants to maintain the security and confidentiality of

PECB examinations. When someone who holds PECB credentials reveals information about PECB examination content, they violate the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. Identification of assets

ISO/IEC 38500:2015 under clause 4.1 Principles states that “The principles express preferred behavior to guide decision making.”

For each of the principles mentioned below, please describe preferred behavior that guides in decision making.

Conformance

Possible answers:

1) When we have all information needed

2) We are receiving positive feedbacks

2. Identification of risk associated with information security

In your own words, please write how you understand the following:

The organization’s business strategy takes into account the current and future capabilities of IT (*text from 4.1.2 Principle 2: Strategy*)

Possible answers:

The strategic plans for IT satisfy the current and ongoing needs of the organization’s business strategy.