PECB

When Recognition Matters

EXAM PREPARATION GUIDE

ISO/IEC 27035 Lead Incident Manager

The objective of the "PECB Certified ISO/IEC 27035 Lead Incident Manager" examination is to ensure that the candidate has the knowledge and skills to support an organization in implementing and managing an Information Security Incident Management process, and for understanding best practices based on ISO/IEC 27035.

The target population for this examination is:

- Critical Incident Response Team's (CIRT) Analyst
- Major Incident Manager
- Incident Management Coordinator
- IT Security Operations Centre – Team Lead
- Senior Security Analyst
- Information Security Officer

The exam content covers the following domains:

- Domain 1: Fundamental principles and concepts in Incident Management
- Domain 2: Incident Management Best Practices based on ISO/IEC 27035
- Domain 3: Designing and Developing an Organizational Incident Management Process based on ISO/IEC 27035
- Domain 4: Preparing for Incident Management and implementing an Incident Management Process
- Domain 5: Enacting the Incident Management Process and handling Security Incidents
- Domain 6: Performance Monitoring and Measuring
- Domain 7: Improving the Incident Management Process

The content of the exam is divided as follows:

Domain 1: Fundamental principles and concepts in Incident Management

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can understand, interpret and illustrate the main Incident Management concepts related to published standards including ISO/IEC 27035

Competencies	Knowledge statements
1. Understand and explain the operations of the ISO organization and the development of Incident Management Standards 2. Ability to identify, analyze and evaluate the Incident Management compliance requirements for an organization 3. Ability to explain and illustrate the main concepts in Incident Management and Information Security risk management 4. Ability to distinguish between Incident Management, Business Continuity, Disaster Recovery and Investigations and understand their relationships 5. Understand the issues Incident Manager is designed to address and the fundamental components of an Incident Management process. 6. Understanding of the relevant legal, regulatory and contractual issues related to Incident Management	1. Knowledge of the application of the eight ISO management principles to Incident Management 2. Knowledge of the main standards in Incident Management 3. Knowledge of the different sources of Incident Management requirement for an organization: laws, regulations, international and industry standards, contracts, market practices, internal policies 4. Knowledge of the main Incident Management concepts and terminology as described in ISO 27035 5. Knowledge of the concept of risk and its application in Incident Management 6. Knowledge of the relationship between Incident Management, Business Continuity, Disaster Recovery and Investigations. 7. Knowledge of the strategies and approaches to develop an effective Incident Management Process

Domain 2: Incident Management Best Practice based on ISO/IEC 27035

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can understand, interpret and provide guidance on how to implement and manage Incident Management requirements based on best practices of ISO/IEC 27035

Competencies	Knowledge statements
1. Ability to identify, understand, classify and explain the clauses with requirements from ISO 27035 2. Ability to detail and illustrate the requirements and best practices by concrete examples 3. Ability to compare possible solutions to Incident Management issues of an organization and identify/analyze the strength and weakness of each solution 4. Ability to select and demonstrate the best Incident Management solution in order to address Incident Management objectives stated by the organization 5. Ability to create and justify an action plan to implement an Incident Management process by identifying the stages and key components. 6. Ability to prepare a credible incident management process which can be incorporated into an operating environment.	1. Knowledge of operational planning and control 2. Knowledge of business impact analysis and risk assessment 3. Knowledge of Incident Management strategy 4. Knowledge of establishing and implementing Incident Management procedures 5. Knowledge of establishing Incident Response Procedures 6. Knowledge of exercising and testing 7. Knowledge of Incident Management Incident Management Controls Best Practices 8. Knowledge of Incident Management Best Practices

Domain 3: Designing and Developing an Organizational Incident Management Process based on ISO/IEC 27035

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can plan the implementation of an effective Incident Management Process

Competencies

1. Ability to manage a project to develop effective Incident Management processes following project management best practices
2. Ability to gather, analyze and interpret the necessary information to plan the implementation of an Incident Management Process
3. Ability to observe, analyze and interpret the external and internal environment of an organization
4. Ability to gather the necessary information to contribute to the design of an effective and aligned Incident Management Process
5. Ability to state and justify an Incident Management scope, response strategies and times adapted to the security objectives of a specific organization
6. Ability to select and justify the selected approach and methodology adapted to the needs of the organization
7. Ability to design and document an Incident Detection, Reporting and Management Process which can then be implemented in the implementation phase.

Knowledge statements

1. Knowledge of the main project management concepts, terminology, process and best practice as described in ISO 10006
2. Knowledge of the principal approaches and methodology frameworks to implement an Incident Management Process
3. Knowledge of the main concepts and terminology related to organizations
4. Knowledge of an organization's external and internal environment
5. Knowledge of the main interested parties related to an organization and their characteristics
6. Knowledge of techniques to gather information necessary to design the Incident Management Process
7. Knowledge of the characteristics of the Incident Management Scope, response strategies and timeframes
8. Knowledge of the Service Level Agreements, Operational Level Agreements, Key Performance Indicators (KPI's) and response times
9. Knowledge of the Incident Response Team, its members and the approach to creating such a team
10. Knowledge of the techniques used to identify incidents and the processes for reporting and escalation

Domain 4: Preparing for Incident Management and implementing an Incident Management Process

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can implement the Incident Management process and associated security controls required for an effective Incident Management process

Competencies

1. 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 Incident Management Process
2. Ability to define the document and record management processes needed to support the implementation and the operations of an Incident Management Process
3. Ability to define and design security controls & processes which support Incident Management and document them
4. Ability the define and writing an Incident Management policy and Incident Management policies & procedures
5. Ability to implement the required processes and security controls of an Incident Management Process
6. Ability to define and implement appropriate Incident Management training, awareness and communication plans
7. Ability to define and implement an incident management process based on Incident Management best practices
8. Ability to transfer an Incident Management Process project to operations and manage the change management process

Knowledge statements

1. Knowledge of the roles and responsibilities of the key actors during the implementation of an Incident Management Process and in its operation after the end of the implementation project
2. Knowledge of the main organizational structures applicable for an organization to effectively manage Information Security Incidents
3. Knowledge of the best practices on document and record management processes and the document management life cycle
4. Knowledge of the characteristics and the differences between the different documents related to Incident Management Process: policy, procedure, guideline, standard, baseline, worksheet, etc.
5. Knowledge of model-building controls and processes techniques and best practices
6. Knowledge of controls and processes deployment techniques and best practices
7. Knowledge of techniques and best practices to write Incident Management policies, procedures and others types of documents included in an Incident Management Process
8. Knowledge of the characteristics and the best practices to implement Incident Management training, awareness and communication plans
9. Knowledge of the characteristics and main processes information management related to the Incident Management Process based on best practices
10. Knowledge of change management techniques best practices

Domain 5: Enacting the Incident Management Process and handling Security Incidents

Main objective: To ensure that Certified ISO/IEC 27035 Lead Incident Manager Candidate can lead the response to an Incident in an effective, legal and professional manner

Competencies	Knowledge statements
1. Ability to analyze an incident when reported and to identify the severity 2. Ability to understand, the options to respond to an incident and the risks and impacts associated with these options from a business, legal and regulatory perspective 3. Ability to manage communication with all relevant parties during an incident. 4. Ability to understand when an incident is declared as a crisis, Business Continuity event and the associated processes 5. Ability to identify incidents which may have legal implications and to instigate suitable investigation processes. 6. Ability to ensure understands the processes to be followed to ensure any investigations meet relevant legal and regulatory requirements. 7. Ability to identify the members of the Incident Management Team that should be engaged and their roles in the Incident Response Process 8. Ability to manage communications with relevant authorities and with the media and other interested parties	1. Knowledge incident analysis processes and relevant legal, regulatory and business issues 2. Knowledge of effective communication and the communication strategies that can be adopted during an incidents 3. Knowledge of Crisis Management and Business Continuity and how to align with these processes 4. Knowledge of investigations and the principles of forensics investigations including protecting the chain of custody 5. Knowledge of the roles of the Incident Management Team and when such members are involved in Incident Handling.

Domain 6: Performance Monitoring and Measuring

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can evaluate, monitor and measure the performance of an Incident Management

Competencies	Knowledge statements
1. Ability to monitor and evaluate the effectiveness of an Incident Management Process in operation 2. Ability to verify the extent to which identified security requirements have been met 3. Ability to monitor trends and patterns related to Incidents and identify root causes 4. Ability to analyze the handling of an Incident to identify the performance of the incident response and identify opportunities to improve the process for managing future incidents 5. Ability to perform regular and methodical reviews regarding the suitability, adequacy, effectiveness and efficiency of an Incident Management Process with policies and objectives of an organization 6. Ability to define and implement a management review process and counsel management on it.	1. Knowledge of the techniques and best practices to monitor the effectiveness of an Incident Management Process 2. Knowledge of the main concepts and components related to an Incident Management Measurement Programme: measures, attributes, indicators, dashboard, etc. 3. Knowledge of the characteristics and the differences between an operational, tactical and strategic Incident Management indicators and dashboards 4. Knowledge of the techniques and methods to define and document an adequate and reliable indicators 5. Knowledge of how to evaluate the results of an incident response and assess opportunities for improvement 6. Knowledge of how to identify trends and the root cause of incidents.

Domain 7: Improving the Incident Management Process

Main objective: To ensure that the Certified ISO/IEC 27035 Lead Incident Manager candidate can provide guidance on the Continual improvement of an Incident Management

Competencies

1. Ability to understand the principle and concepts related to continual improvement
2. Ability to counsel an organization on how to continually improve the effectiveness and the efficiency of an Incident Management Process
3. Ability to implement Incident Management Process continual improvement processes in an organization
4. Ability to determine the appropriate business improvement tools to support continual improvement processes of a specific organization
5. Ability to identify, analyze the root-causes of negative findings
6. Ability to identify, analyze the root-cause of potential nonconformities and proposed action plans to treat them.

Knowledge statements

1. Knowledge of the main concepts related to continual improvement
2. Knowledge of the characteristics and the difference between the concept of effectiveness and the efficiency
3. Knowledge of the concept and techniques to perform a benchmarking
4. Knowledge of the main processes, tools and techniques used by professionals to identify the root-causes of negative findings
5. Knowledge of the characteristics and the difference between corrective actions and preventive actions

Knowledge of the main processes, tools and techniques used by professionals to develop and proposed the best corrective and preventive action plans.

Based on these 7 domains and their relevance, 12 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 competency domain
Competency Domains	Fundamental principles and concepts in Incident Management	5	x		2	16.67	20	26.67
		5	x					
	Incident Management Best Practices based on ISO/IEC 27035	10	x					
		5	x					
		10	x		3	25.00	15	20.00
	Designing and Developing an Organizational Incident Management Process based on ISO/IEC 27035	5		x	1	8.33	5	6.67
	Preparing for Incident Management and implementing an Incident Management Process	5		x	3	25.00	10	13.33
		5		x				
		5		x				
	Enacting the Incident Management Process and handling Security Incidents	10		x	1	8.33	15	20.00
	Performance Monitoring and Measuring	5		x	1	8.33	5	6.67
	Improving the Incident Management Process	5		x	1	8.33	5	6.67
Total points		75						
Number of Questions per level of understanding			5	7				
% of Test Devoted to each level of understanding (cognitive/taxonomy)			41.67	58.33				

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 27035 Lead Incident 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 proctor and the exam confirmation letter.

The exam duration is three (3) 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"; the candidates are authorized to use the following reference materials:

- A copy of the ISO/IEC 27035:2011 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.