PECB

BEYOND RECOGNITION

NIS 2 DIRECTIVE LEAD IMPLEMENTER

Candidate Handbook

PECB

Table of Contents

PECB

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

Our values

Integrity, Professionalism, Fairness

[1] Education refers to training courses developed by PECB and offered globally through our partners.

The Value of PECB Certification

Global recognition
PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click here.

High-quality products and services
We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards
Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service
We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience
Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter "PECB professionals") adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB's belief that to achieve organizational success, it has to fully understand the clients and stakeholders' needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB's primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB's reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB's Code of Ethics, go to Code of Ethics | PECB.

Introduction to NIS 2 Directive Lead Implementer

NIS 2 Directive specifies the requirements for enhancing the security of network and information systems across the European Union (EU). A cybersecurity program in compliance with NIS 2 Directive requirements enables organizations to strengthen their cybersecurity measures, protect critical infrastructure, and comply with legal requirements in the EU. NIS 2 Directive applies to a broad spectrum of organizations, defined as essential or important entities by the directive, with specific size thresholds for each sector, encompassing those that provide essential or important services to the European economy and society, as well as organizations that are the sole providers of a critical service in a Member State.

The "NIS 2 Directive Lead Implementer" credential is a professional certification for individuals aiming to demonstrate the competence regarding the NIS 2 Directive compliance requirements and leading an implementation team.

Given that implementation is a highly sought-after profession, obtaining an internationally recognized certification can significantly boost your career and enable you to attain your professional goals.

This document specifies the PECB NIS 2 Directive Lead Implementer certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at certification.team@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to Active Partners. The training course schedule is also available online and can be accessed on Training Events.
2. Take a PECB exam remotely through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

Rescheduling the exam

For any changes with regard to the exam date, time, location, or other details, please contact online.exams@pecb.com.

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification is $500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

[2] All prices listed in this document are in US dollars.

Competency domains

The objective of the "PECB NIS 2 Directive Lead Implementer" exam is to ensure that the candidate has acquired the necessary competence to support an organization in establishing, implementing, managing and maintaining a NIS 2 Directive compliance program.

The NIS 2 Directive Lead Implementer certification is intended for:

- Cybersecurity professionals seeking to gain a thorough understanding of the requirements of NIS 2 Directive and learn practical strategies to implement robust cybersecurity measures
- IT managers and professionals aiming to gain insights on implementing secure systems and improve the resilience of critical systems
- Government and regulatory officials responsible for enforcing the NIS 2 Directive

The content of the exam is divided as follows:

- **Domain 1:** Fundamental concepts and definitions of NIS 2 Directive
- **Domain 2:** Planning of NIS 2 Directive requirements implementation
- **Domain 3:** Cybersecurity roles and responsibilities and risk management
- **Domain 4:** Cybersecurity controls, incident management, and crisis management
- **Domain 5:** Communication and awareness
- **Domain 6:** Testing and monitoring of a cybersecurity program

Domain 1: Fundamental concepts and definitions of NIS 2 Directive

Main objective: Ensure that the candidate is able to interpret NIS 2 Directive concepts and definitions.

Competencies	Knowledge statements
1. Ability to explain the main concepts related to the NIS 2 Directive	1. Knowledge of the main concepts and terminology of NIS 2 Directive
2. Ability to develop a comprehensive knowledge on ISO standards related to information security	2. Knowledge of ISO standards related to information security, including ISO/IEC 27001 and ISO/IEC 27002
3. Ability to identify other industry cybersecurity best practices, including NIST Cybersecurity Framework and CIS controls	3. Knowledge of legal frameworks and regulations relevant to information security and cybersecurity, including Digital Markets Act, Digital Services Act, Digital Operational Resilience Act, EU Cybersecurity Act, European Cyber Resilience Act, Data Governance Act, GDPR, and Payment Services Directive 2
4. Ability to identify ENISA publications for cybersecurity	4. Knowledge of the scope of NIS 2 Directive and its comparison with NIS Directive
5. Ability to compare NIS 2 Directive with its predecessor, the NIS Directive	5. Knowledge of the relationship between the NIS 2 Directive and ISO/IEC 27000 series
6. Ability to analyze the structure, objectives, and subject matter of the NIS 2 Directive	6. Knowledge of the structure, objectives, and subject matter of the NIS 2 Directive and its implications for organizations and critical infrastructure sectors
7. Ability to assess the potential impact of the NIS 2 Directive on various stakeholders, including essential and important entities	7. Knowledge of the impact of the NIS 2 Directive
8. Ability to describe the administrative fines associated with noncompliance to the NIS 2 Directive	8. Knowledge of administrative fines associated with noncompliance to the NIS 2 Directive and the criteria for determining such fines
9. Ability to recognize and describe the important EU organizations involved in the enforcement and regulation of cybersecurity within the European Union	9. Knowledge of key EU organizations responsible for cybersecurity governance, regulation, and oversight, and their roles in enforcing the NIS 2 Directive

Domain 2: Planning of NIS 2 Directive requirements implementation

Main objective: Ensure that the candidate is able to identify and explain the main requirements of NIS 2 Directive and plan their implementation.

Competencies	Knowledge statements
1. Ability to explain the components of the NIS 2 Directive, including governance, crisis management, risk measures, and reporting obligations	1. Knowledge of the components and requirements of the NIS 2 Directive, including definitions, governance, crisis management, risk management, and reporting obligations
2. Ability to define the approach for implementing the NIS 2 Directive requirements	2. Knowledge of the main approaches and methodologies used to implement NIS 2 Directive requirements
3. Ability to collect, analyze, and interpret the information required to plan the implementation of NIS 2 Directive requirements	3. Knowledge of typical NIS 2 Directive compliance objectives and how to achieve them
4. Ability to interpret and set NIS 2 Directive compliance objectives	4. Knowledge of what typically constitutes an organization's internal and external context
5. Ability to analyze and consider the internal and external context of an organization	5. Knowledge of the approaches used to understand the context of an organization
6. Ability to identify the roles and responsibilities of key interested parties during and after the implementation of NIS 2 Directive's requirements	6. Knowledge of the techniques used to gather information on an organization and to perform a gap analysis
7. Ability to perform a gap analysis and clarify NIS 2 Directive compliance objectives	7. Knowledge of a NIS 2 Directive implementation project plan and a NIS 2 Directive implementation project team
8. Ability to define and justify the NIS 2 Directive implementation program scope adapted to the organization's specific NIS 2 Directive compliance objectives	8. Knowledge of the main organizational structures applicable for an organization to manage NIS 2 Directive implementation
9. Ability to explain the requirements of NIS 2 Directive related to governance and cybersecurity strategy	9. Knowledge of the characteristics of NIS 2 Directive implementation scope in terms of organizational, technological, and physical boundaries
10. Ability to develop a cybersecurity compliance program	10. Knowledge of NIS 2 Directive articles that address governance and national cybersecurity strategy
11. Ability to identify the types of policies and establish a cybersecurity policy	11. Knowledge of the necessary activities for developing a cybersecurity compliance program
	12. Knowledge of the best practices and techniques used to draft and establish cybersecurity policies and procedures

Domain 3: Cybersecurity roles and responsibilities and risk management

Main objective: Ensure that the candidate is able to define cybersecurity roles and responsibilities and conduct risk management

Competencies	Knowledge statements
1. Ability to analyze the organizational structure and assign key roles and responsibilities related to cybersecurity	1. Knowledge of the organizational structure
2. Ability to define roles and responsibilities within the organization	2. Knowledge of the roles and responsibilities related to cybersecurity
3. Ability to establish an effective cybersecurity team within the organization	3. Knowledge of NIS 2 Directive requirements regarding asset management
4. Ability to manage cybersecurity assets effectively	4. Knowledge of cybersecurity asset management
5. Ability to identify cybersecurity risks by assessing threats, vulnerabilities, and potential impacts	5. Knowledge of NIS 2 Directive requirements regarding risk management
6. Ability to analyze cybersecurity risks to determine their likelihood and potential consequences	6. Knowledge of the guidelines on risk management, such as ISO 31000, ISO/IEC 27005, and ENISA publications
7. Ability to evaluate cybersecurity risks to prioritize them based on their significance and potential impact on the organization	7. Knowledge of cybersecurity risk identification and analysis to determine the likelihood and potential consequences
8. Ability to implement risk treatment strategies to mitigate the identified cybersecurity risks	8. Knowledge of cybersecurity risk evaluation to implement effective risk treatment strategies
9. Ability to effectively communicate and consult with relevant stakeholders regarding cybersecurity risks and mitigation strategies	9. Knowledge of communication and consultation with relevant stakeholders regarding cybersecurity risks
10. Ability to maintain records and report on cybersecurity risks and continuously monitor and review the effectiveness of cybersecurity risk management efforts	10. Knowledge of maintenance of records and reporting on cybersecurity risks, treatments, and their status
	11. Knowledge of monitoring and reviewing the procedure to determine the effectiveness of cybersecurity risk management efforts

Domain 4: Cybersecurity controls, incident management, and crisis management

Main objective: Ensure that the candidate is able to implement the cybersecurity processes required for NIS 2 Directive compliance, including cybersecurity controls, supply chain security, incident management, and crisis management.

Competencies	Knowledge statements
1. Ability to interpret the requirements of NIS 2 Directive regarding cybersecurity risk management measures	1. Knowledge of NIS 2 Directive requirements regarding technical, operational, and organizational measures
2. Ability to explain human resources security measures based on industry best practices	2. Knowledge of cybersecurity controls necessary for managing risks, such as human resources security, access controls, cryptography, and network security
3. Ability to explain best practices for effective access control to safeguard network and information systems	3. Knowledge of NIS 2 Directive requirements that address measures for ensuring supply chain security
4. Ability to utilize cryptography techniques to improve data security	4. Knowledge of supply chain risk management, vulnerability handling, and information security practices in supplier relationships
5. Ability to identify and implement the necessary measures to protect network services and systems	5. Knowledge of the processes for preparing for, detecting, reporting, assessing, responding to, and learning from cybersecurity incidents
6. Ability to select and implement supply chain risk management processes, establish vulnerability handling processes, and enhance information security within supplier relationships	6. Knowledge of the role and responsibilities of CSIRTs in incident handling process as defined by NIS 2 Directive
7. Ability to prepare for, detect, report, assess, respond to, and learn from cybersecurity incidents	7. Knowledge of the incident reporting obligations enforced by NIS 2 Directive for the parties involved in incident handling
8. Ability to create a crisis management plan, crisis communication plans, and emergency communication systems to navigate challenging situations	8. Knowledge of the NIS 2 Directive requirements for Member States and CSIRTs regarding cyber crisis management
9. Ability to develop comprehensive business continuity plans and disaster recovery plans to ensure operational continuity	9. Knowledge of crisis management and the characteristic and importance of crisis communication
	10. Knowledge of business continuity management, including strategies and recovery planning

Domain 5: Communication and awareness

Main objective: Ensure that the candidate is able to develop and implement effective communication, competence development, and awareness programs to support cybersecurity and organizational goals and comply with NIS 2 Directive requirements.

Competencies	Knowledge statements
1. Ability to plan and provide competence development activities, including training and awareness programs	1. Knowledge of the requirements of NIS 2 Directive for cybersecurity awareness across the European Union
2. Ability to define the structure and type of competence development programs aligned with organizational objectives	2. Knowledge of competence development activities and programs
3. Ability to effectively deliver training and awareness programs to address the identified needs	3. Knowledge of competence program design to meet organizational objectives
4. Ability to assess and evaluate the outcomes and effectiveness of training and awareness programs	4. Knowledge of the process for delivering effective training and awareness programs
5. Ability to plan, execute, and evaluate communication activities to achieve communication objectives	5. Knowledge of evaluating the outcomes and effectiveness of training and awareness programs
6. Ability to identify NIS 2 Directive requirements regarding cybersecurity awareness and information sharing	6. Knowledge of strategic communication and its principles: transparency, appropriateness, credibility, responsiveness, and clarity
7. Ability to apply the principles of an effective communication strategy	7. Knowledge of effective communication strategies
	8. Knowledge of cybersecurity information-sharing arrangements and voluntary notification of relevant information as defined in NIS 2 Directive

Domain 6: Testing and monitoring of a cybersecurity program

Main objective: Ensure that the candidate is able to effectively audit, measure, monitor, and continually improve a cybersecurity program in accordance with NIS 2 Directive.

Competencies	Knowledge statements
1. Ability to understand and explain cybersecurity testing	1. Knowledge of cybersecurity testing techniques
2. Ability to identify the requirements of NIS 2 Directive regarding security audits and self-assessments	2. Knowledge of NIS 2 Directive requirements regarding self-assessments and the role of such assessment in ensuring NIS 2 Directive compliance
3. Ability to conduct internal audits, address nonconformities, and understand audit fundamentals	3. Knowledge of internal compliance audit and internal audit activities
4. Ability to perform self-assessments using frameworks such as ENISA Self-Assessment Framework	4. Knowledge of ENISA Self-Assessment Framework and other tools for evaluating cybersecurity
5. Ability to define measurement objectives establish performance indicators and determine monitoring methods	5. Knowledge of measurement objectives, performance indicators, and monitoring methods for assessing cybersecurity program effectiveness
6. Ability to identify the role of the CSIRTs and competent authorities in monitoring cyber threats as defined by NIS 2 Directive	6. Knowledge of the NIS 2 Directive requirements for CSIRTs on monitoring and analyzing threats, vulnerabilities, and incidents at national level
7. Ability to determine what needs to be monitored, report monitoring results effectively, and select appropriate monitoring methods	7. Knowledge of reporting monitoring results to stakeholders, and selecting appropriate monitoring methods
8. Ability to monitor change factors, maintain and improve cybersecurity measures, and document improvements	8. Knowledge of monitoring change factors, maintaining and improving cybersecurity measures, and documenting improvements

Based on the above-mentioned domains and their relevance, the exam contains 80 multiple-choice questions, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental concepts and definitions of NIS 2 Directive	10	12.5	X	
	Planning of NIS 2 Directive requirements implementation	20	25	X	
	Cybersecurity roles and responsibilities and risk management	15	18.75		X
	Cybersecurity controls, incident management, and crisis management	15	18.75		X
	Communication and awareness	10	12.5	X	
	Testing and monitoring of a cybersecurity program	10	12.5		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% of the exam devoted to each level of understanding (cognitive/taxonomy)			**50%**	**50%**

The passing score of the exam is **70%**.

After successfully passing the exam, candidates will be able to apply for obtaining the "PECB Certified NIS 2 Directive Lead Implementer" credential.

Taking the exam

General information about the exam
Candidates are required to arrive/be present at least 30 minutes before the exam starts.

Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:
- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB exam format and type
1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more information about online exams, go to the PECB Online Exam Guide.

PECB exams are available in two types:
1. Essay-type question exam
2. Multiple-choice question exam

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding on both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-depended, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

This is an open-book exam. The candidate is allowed to use the following reference materials:

- A hard copy of the NIS 2 Directive
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate).

For specific information about exam types, languages available, and other details, please contact examination.team@pecb.com or go to the List of PECB Exams.

Sample exam questions

TechLink, a multinational company, specializes in delivering a wide range of cloud computing services tailored to the finance and healthcare sectors. Its services empower organizations to harness the full potential of cloud technology, driving digital transformation and enhancing public services globally.

Operating within the European Union, *TechLink* falls under the regulatory framework of the NIS 2 Directive as an essential entity. *TechLink* had yet to implement the necessary safeguards to protect their networks and systems adequately and ensure compliance with the directive; therefore, it initiated a comprehensive cybersecurity program. The company adopted an approach that allowed setting high production standards without prescribing specific methods, enabling them to find efficient and innovative ways to meet these standards.

In accordance with Article 21 of the NIS 2 Directive, the company developed a business continuity management (BCM) strategy. Its approach to developing the BCM strategy entailed a third-party contractual recovery setup to seek external support for re-establishing key processes, and a key modification option to adjust operational processes under resource-constrained circumstances. This approach facilitated agile response to incident, balancing external support with internal adjustments to expedite the recovery process while addressing key management concern such as planning extent, implementation costs, and contractual agreements with third-party suppliers.

As part of the cybersecurity program, *TechLink* focused on ensuring the security of networks and information systems by fostering a culture of risk management, including risk assessments and the implementation of cybersecurity measures. In accordance with NIS 2 Directive, these measures were approved by the company's management body. The management body is well-versed in general risk management practices, while the company deemed it unnecessary to provide additional training on cybersecurity risk management as one of the members has expertise in cybersecurity.

Recently, *TechLink* faced a serious cybersecurity incident where a sophisticated cyberattack targeted its critical systems, resulting in a breach of sensitive customer data. This incident provided an opportunity to demonstrate its commitment to complying with NIS 2 Directive. The company isolated the affected systems and contained the intrusion to prevent further damage. Then, it promptly notified relevant authorities, including the national government within 24 hours of detection. It also communicated with affected customers, providing them with information about the incident and steps to protect data. The company submitted a final report including a detailed description, the type of threat, the applied and ongoing mitigation, and the cross border impact.

Based on the scenario above, answer the following questions:

1. **What potential penalties might *TechLink* face in case of noncompliance with the NIS 2 Directive?**
   A. €7 million or 1.4% of the total annual worldwide turnover
   B. **€10 million or 2% of the total annual worldwide turnover**
   C. €5 million or 1% of the total annual worldwide turnover

2. **Which requirement of NIS 2 Directive did *TechLink* neglect?**
   A. **Training the members of the management body on cybersecurity risk management practices**
   B. Ensuring approval of cybersecurity measures by the Critical Entities Resilience Groups
   C. Creating a management body of five members who have extensive experience in cybersecurity

3. **Which regulatory approach did *TechLink* adopt to comply with the NIS 2 Directive?**
   A. Command and control
   B. **Performance-based**
   C. Management-based

4. **Given the actions taken by *TechLink* in response to the cyberattack on its critical systems, which aspect of the incident reporting obligation outlined in Article 23 of the NIS 2 Directive did *TechLink* fail to adhere to?**
   A. **Submit an intermediate status update upon request**
   B. Provide ENISA with a summary report on significant incident
   C. Submit a public disclosure of the incident within 48 hours of detection

5. **Which approach for developing the BCM strategy did *TechLink* use?**
   A. Multi-site operation
   B. Backup arrangement
   C. **Combined arrangement**

Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
    - Looking at another candidate's exam material or answer sheet
    - Giving or receiving any assistance from the invigilator, candidate, or anyone else
    - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to examination.team@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

If a candidate does not pass the exam on the 1st attempt, they must wait 15 days after the initial date of the exam for the next attempt (1st retake).

Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received (the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this Policy. The process to schedule the exam retake is the same as for the initial exam.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

PECB NIS 2 Directive credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB NIS 2 Directive scheme have the following requirements:

Credential	Education	Exam	Professional experience	MS project experience	Other requirements
PECB Certified NIS 2 Directive Provisional Implementer	At least secondary education	PECB Certified NIS 2 Directive Lead Implementer exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified NIS 2 Directive Implementer			Two years: One year of work experience in cybersecurity management	Project activities: A total of 200 hours	
PECB Certified NIS 2 Directive Lead Implementer			Five years: Two years of work experience in cybersecurity management	Project activities: A total of 300 hours	
PECB Certified NIS 2 Directive Senior Lead Implementer			Ten years: Seven years of work experience in cybersecurity management	Project activities: A total of 1,000 hours	

To be considered valid, the implementation activities should follow best implementation and management practices and include the following:

1. Conducting comprehensive risk assessments specific to critical infrastructure systems
2. Managing incident response plans tailored to the requirements of the NIS 2 Directive
3. Implementing appropriate security measures and controls
4. Implementing metrics and performance indicators
5. Managing and responding to cybersecurity incidents
6. Conducting management reviews
7. Managing a cybersecurity team

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB account), including contact details of individuals who

will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

The online certification application process is very simple and takes only a few minutes:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

PECB provides support both in English and French.

Professional experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Professional references

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their cybersecurity management experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

Cybersecurity project experience

The candidate's cybersecurity project log will be checked to ensure that the candidate has the required number of project activity hours.

Evaluation of certification applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

PECB

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

The application payment for the certification/certificate program is nonrefundable.

Certification status options

Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

- PECB receives excessive or serious complaints by interested parties (suspension will be applied until the investigation has been completed.)
- The logos of PECB or accreditation bodies are willfully misused.
- The candidate fails to correct the misuse of a certification mark within the determined time by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals. Additional reasons for revoking certification can be if the candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

Other statuses
Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to Certification Status Options.

Upgrade and downgrade of credentials

Upgrade of credentials
Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the "My Certifications" tab, and click on "Upgrade." The upgrade application fee is $100.

Downgrade of credentials
A PECB Certification can be downgraded to a lower credential due to the following reasons:
- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Renewing the certification
PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee ($120). For more information, go to the Certification Maintenance page on the PECB website.

Closing a case
If candidates do not apply for certification within one year, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification.team@pecb.com and pay the required fee.

Complaint and Appeal Policy
Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click here.

PECB

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Implementer certification).

Non-discrimination and special accommodations

All candidate applications will be evaluated objectively, regardless of the candidates' age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the partner/distributor in order for them to make proper arrangements[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

[4] ADA Amendments Act of 2008 (P.L. 110–325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:

Headquarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
customer@pecb.com

PECB Help Center

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system.

www.pecb.com