Publication date : 04/12/2024

Course : EBIOS Risk Manager, preparation for LSTI certification

APT cyber risk analysis and ecosystem

Seminar - 2d - 14h - Ref. IVH

Price : 2170 CHF E.T.

The EBIOS RM (2018) method enables you to assess and deal with IS security risks, particularly cyber risks, based on proven experience in IS consulting and project management assistance. This seminar will provide you with all the knowledge you need to implement it in a real-life situation.

Teaching objectives

At the end of the training, the participant will be able to:

- Understanding cyber risk issues: cyber defense through risk
- Evaluate how the new EBIOS fits (or doesn't fit) current safety issues
- Understanding the proposed risk management approach
- Understand the vocabulary and concepts developed by ANSSI
- Carry out a complete study using all the workshops on offer

Intended audience

CISOs or security correspondents, security architects, IT directors or managers, engineers, project managers (MOE, MOA) who have to integrate security requirements.

Prerequisites

Basic knowledge of risk management and cybersecurity, or knowledge equivalent to that provided by the BYR and ASE or BYR and AIR courses.

Certification

Remote certifications

See the certifier's official documentation for the list of prerequisites for completing the online certification exam.

PARTICIPANTS

CISOs or security correspondents, security architects, IT directors or managers, engineers, project managers (MOE, MOA) who have to integrate security requirements.

PREREQUISITES

Basic knowledge of risk management and cybersecurity, or knowledge equivalent to that provided by the BYR and ASE or BYR and AIR courses.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

Practical details

Example

Case studies in industrial and tertiary contexts will help you understand and apply the method.

Course schedule

1 Cyberthreats in the news

- Cyber theft and cyber espionage of sensitive data.
- Towards a new East-West Cold War, USA-China.
- Denials of service on a global scale.
- Organized hacker groups, the role of intelligence agencies.
- Phishing/social engineering, Spear phishing: well-honed scenarios.
- APTs: persistence and depth of attacks.
- Theft of sensitive data, network intrusions, malware, bots/botnets and ransomware.

2 Cyber threat identification and analysis

- The military approach applied to the cyber world.
- The US approach with Find, Fix, Track, Target, Engage, Assess.
- The cyber kill chain as a basis for description. Typical example: Lockheed Martin.
- Reconnaissance, Weaponization, Delivery, Exploit, Installation, Control (C2) phases. Actions on Objectives.
- ANSSI's portrait of a targeted attack.
- Process phases (Know, Enter, Find, Exploit).
- Identification of direct and indirect attack paths.

3 The EBIOS method

- Role of ANSSI and the EBIOS Club.
- EBIOS and the challenges of the LPM.
- Contribution of the new EBIOS RM method (2018) and EBIOS 2010.
- RM EBIOS compatibility versus ISO 31000 and ISO 27005.

4 The fundamentals of the method

- Business value, well supported, ecosystem, stakeholder.
- Compliance approach versus risk scenario approach.
- Sophisticated intentional threats such as APTs are taken into account.
- Assessment of its ecosystem and critical tier 1, 2 and 3 stakeholders.
- EBIOS RM to the LPM and NIS Directive approval process.
- Safety rules for the compliance approach (hygiene guide, LPM/NIS measures, etc.).
- Risk Management Process as a measure of ISS governance.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 RM EBIOS objectives

- Identify the security foundation best suited to the purpose of the study.
- Comply with safety regulations (trade/legal/contractual).
- Identify and analyze high-level scenarios by integrating the ecosystem and stakeholders.
- Identify and implement safety measures for critical stakeholders.
- Conduct a preliminary risk assessment to identify priority areas for improvement.
- Priority areas for improvement: security and weak points that can be exploited by attackers.
- Carry out a detailed risk assessment, with the aim of obtaining ANSSI certification, for example.

6 Method activities (1 and 2)

- 1. Workshop - Framework and security base :
- What business values, assets and media should be mapped?
- What events should be feared, as seen from a business perspective?
- Which security base should be integrated? ANSSI, internal PSSI...?
- Which regulatory standards should be identified as mandatory?
- 2. Workshop - Sources of risk and objectives :
- How attractive are cyber attackers' business values?
- What role do the professions play in identifying sources of risk?
- What criteria should be used to assess SR-OV pairs? Assessing the resources and motivation of attacking groups.

Case study

Presentation of workshops 1 and 2.

7 Method activities (3, 4 and 5)

- 3.4. Workshop - Strategic and operational scenarios :
- Who are the stakeholders in the ecosystem?
- What are the scenarios as seen from the business side and then from the technical side?
- What direct and indirect attack paths should be described?
- How to calculate scenario likelihoods: from the express method to the advanced method.
- 5. Workshop - Risk management :
- What risks are considered unacceptable in this context?
- What are the deliverables for an RM EBIOS study?
- ISO 27001 declaration of applicability, LPM/NIS risk assessment report, etc.

Case study

Presentation of workshops 3, 4 and 5.

8 EBIOS case study

- 1 The context of the study: involvement of the professions in identifying business values and perceived impacts.
- Identify sources of risk and potential attack targets.
- Determination of regulatory and legal obligations, and identification of critical Tier 1 stakeholders.
- Building a digital threat map of the ecosystem in context.
- 2. The workshop activities required to build the strategic and then operational scenarios.
- Risk assessment in terms of severity and likelihood.
- Development of a method for calculating cyber maturity and stakeholder dependency.
- 3. Development of a risk management plan.
- Drawing up an action plan.
- Technical (protection, defense) and organizational (governance, resilience) security measures.
- Choice of security measures from LPM/NIS, ISO or other standards.
- Choose ANSSI-certified software (currently being certified: ARIMES, EGERIE, AGILE RM, FENCE, IBM OpenPages, etc.).
- The provisional construction of its spreadsheet-based "software".

Dates and locations

REMOTE CLASS
2026 : 2 Apr., 23 June, 29 Sep., 15 Dec.