

— EPSO PREPARATION —

AD8 CYBER SECURITY

Technical Expertise & the EU Framework



Study Community Team

EPSOEXAMS
epsoexams.eu

THE PREPARATION APPROACH

Technical depth. European perspective.

Build the knowledge to assess a risk, choose a control and explain your decision.

KNOW THE SYSTEM. UNDERSTAND THE DUTY.

A connected approach to AD8 Cybersecurity preparation

Technical expertise

Architecture, identity, cryptography, cloud, applications, detection and response - explained through mechanisms, limitations and practical choices.

The EU connection

Legislation, institutional responsibilities and security governance sit alongside the technical content, so you can connect a control with the context in which it is used.

Applied judgement

Worked calculations and realistic scenarios develop the reasoning behind an answer: identify the constraint, compare the options and justify the next step.

14 CHAPTERS

Planned technical and EU coverage

500 MCQs

Planned with detailed explanations

Complete edition in development. This brochure presents the planned scope and an illustrative worked example.

WHAT THE BOOK EXPLORES

Foundations to secure architecture

Understand the principles, rules and controls that underpin effective security.

01

Security foundations

Understand confidentiality, integrity, availability, threats, vulnerabilities and attack surfaces. Learn defence in depth, least privilege and how technical choices affect public-service delivery.

02

Risk management and security assurance

Build risk registers and assess inherent and residual risk. Work through quantitative loss estimates, control effectiveness, maturity assessments and evidence-based improvement priorities.

03

EU cybersecurity legislation

Compare NIS2, Regulation 2023/2841, DORA, CRA and complementary rules. Examine scope, responsibilities, reporting and the relationship with data-protection and resilience requirements.

04

EU governance and security frameworks

Understand ENISA, CERT-EU, IICB and coordination arrangements. Connect ISO information-security management, NIST CSF and CIS Controls with practical implementation and assurance.

05

Secure architecture and network security

Read network diagrams and assess segmentation, Zero Trust, secure remote access and lateral-movement controls. Include DNS, DDoS protection and email authentication with SPF, DKIM and DMARC.

06

Identity and access management

Follow identity lifecycles, MFA, authorisation, privileged access and federation. Examine Active Directory, service accounts and access reviews in hybrid environments.

07

Cryptography and data protection

Distinguish encryption, hashing and signatures. Study PKI, TLS, key management, database permissions and auditing, storage protection, retention and secure deletion.

WHAT THE BOOK EXPLORES

Operations to senior judgement

Connect implementation, response and resilience with organisational decisions.

08

Endpoints, cloud and containers

Explore Windows and Linux hardening, device management and secure baselines. Apply shared responsibility, cloud controls, container security and Kubernetes permissions.

09

Application security and DevSecOps

Connect threat modelling with secure development and web/API controls. Evaluate SAST, DAST, dependency analysis, CI/CD protection, SBOMs and software supply-chain security.

10

Vulnerability management and testing

Prioritise vulnerabilities using severity, exploitation, exposure and business impact. Distinguish scanning, penetration testing and red-team exercises; verify remediation and exceptions.

11

SOC, detection and threat intelligence

Interpret logs and correlate network, identity, email and endpoint signals. Study SIEM, EDR/XDR, SOAR, detection metrics, threat hunting, MITRE ATT&CK; and malware behaviour.

12

Incident response and forensics

Work through ransomware, email compromise, DDoS and data-exfiltration scenarios. Balance containment, evidence preservation, service continuity, escalation and communication.

13

Resilience and security leadership

Use BIA, RTO, RPO and availability calculations. Assess backup recovery, physical safeguards, supplier risk, procurement requirements, budgets and communication with management.

14

OT, ICS and integrated cases

Examine industrial and connected systems, safety constraints, segmentation and maintenance. Explore AI security and integrated cases linking technical diagnosis, EU duties and decisions.

INSIDE EVERY CHAPTER

Understand. Apply. Explain.

A repeatable study structure turns a broad syllabus into manageable learning.

01

Build the concept

Start with clear definitions and the distinctions that prevent confusion. Understand the security objective before selecting a mechanism.

02

See how it works

Follow diagrams, comparison tables and architecture examples. Identify the trust boundary, the attack path and the control that changes the outcome.

03

Work through the decision

Study calculations and practical cases with explicit assumptions. Connect the technical choice with risk, governance and relevant European requirements.

04

Test and review

Use MCQs with explanations of the correct answer and the alternatives. Return to the concept behind each mistake and consolidate the reasoning.

BOOK STUDY + ONLINE MOCKS

Study the book first. Then practise under time pressure online, review mistakes and revisit the topics that need reinforcement.

Mock access and package inclusions depend on the selected offer.

A SAMPLE OF THE LEARNING APPROACH

One question. The full reasoning.

An illustrative risk-management MCQ with transparent assumptions and calculations.

A service interruption causes EUR 240,000 in loss per event. Its expected frequency is 0.25 events per year. A control costs EUR 18,000 annually and reduces frequency to 0.08, with unchanged loss per event.

Using expected annual loss and control cost only, what is the net annual benefit?

A EUR 22,800

B EUR 40,800

C EUR 19,200

D EUR 42,000

Correct answer: A

EXPECTED ANNUAL LOSS

Before control		EUR 60,000
After control		EUR 19,200

Before: $\text{EUR } 240,000 \times 0.25 = \text{EUR } 60,000$.

After: $\text{EUR } 240,000 \times 0.08 = \text{EUR } 19,200$.

Gross reduction: $\text{EUR } 60,000 - \text{EUR } 19,200 = \text{EUR } 40,800$.

Net benefit: $\text{EUR } 40,800 - \text{EUR } 18,000 = \text{EUR } 22,800$.

WHY THE OTHER OPTIONS FAIL

B omits the control cost. C gives the residual expected loss. D subtracts the control cost from the initial expected loss but ignores residual risk.

Decision limit: a positive estimate supports the investment under these assumptions; it does not by itself establish compliance or acceptable residual risk.

WHY CHOOSE THIS APPROACH

Go beyond recognising the terminology.

Prepare to explain why a choice is appropriate - and why the alternatives are weaker.

01

Connect the whole picture

Technical knowledge, European responsibilities and operational decisions are brought into one study route.

02

Make difficult ideas visible

Diagrams, structured comparisons and worked applications support understanding of architecture, risk and recovery.

03

Learn from every alternative

The planned 500-question bank goes beyond an answer key, explaining the distinctions and assumptions behind the choices.

04

Move from study to timed practice

Combine focused reading with online mock exams to practise pace, identify gaps and strengthen your preparation.

YOUR NEXT STEP

Explore AD8 Cybersecurity preparation at EPSOEXAMS

epsoexams.eu

Book preview / Complete edition in development. Check the current offer for availability and inclusions. Independent preparation material; not an official EPSO publication.