

Cybersecurity

Field 2 · EPSO/AD/430/26 · grade AD 8

254

successful candidates sought

AD 8

entry grade

30 / 40 min

field-related test

13 Oct 2026

application deadline

eu-now.com

Preparation dossier · 19 study blocks with their official sources

Based on notice of competition OJ C/2026/4668 and the official texts that cover its Annex II

[EU-now.com](https://eu-now.com)

1 · The competition at a glance

EPSO/AD/430/26 is an open competition based on qualifications and tests for **administrators at grade AD 8** in the institutions, bodies, offices and agencies of the Union. Two fields, and **you may apply for only one**: artificial intelligence (240 successful candidates sought) and cybersecurity (254). You are going for cybersecurity: 254 places on the reserve list.



What actually decides: the three reasoning tests and the EUFTE essay are pass-or-out gates. **Only the field-related MCQ score ranks candidates**, and only the highest scorers have their EUFTE marked and their eligibility checked. Two thirds of your study time belong to the field.



The five phases. Only the field MCQ score ranks candidates; everything else is a pass-or-out gate.

2 · The five tests

Test	Language	Questions	Time	Points	Pass mark
Verbal reasoning	1	20	35 min	0-20	10/20
Numerical reasoning	1	10	20 min	0-10	10/20 combined with abstract
Abstract reasoning	1	10	10 min	0-10	10/20 combined with numerical
Field-related MCQ	2	30	40 min	0-30	15/30 and among the highest scorers
EUFTE	2	—	40 min	0-10	5/10

Language 1 is any of the 24 official languages. **Language 2** is the language of the field MCQ and of the EUFTE. You need C1 in one and B2 in the other, and you choose them in the application form. The tests are taken remotely with remote proctoring, and the order of the sittings may differ from the order in the notice.

The EUFTE is neither a language test nor a knowledge test: EPSO publishes documentation on EU matters before the test — the same you receive during it — and you answer an assignment based on it. It is marked against published anchors.

The exam platform

Tests run on TAO, the platform EPSO uses for all its exams. Arrive knowing where everything is: you lose less time and nothing surprises you on the day.

EU Careers - Sample Test / Part I / Verbal Reasoning
Probe 47a

Clock

All cells in the body have a specific structure and perform a specialised function, apart from stem cells. Stem cells have a number of remarkable properties. Unlike most specialised cells they are capable of replicating themselves many times. They can also develop into different types of specialised cells, such as muscle cells or red blood cells. These properties, in theory, mean that stem cells could repair the body, by multiplying and then replacing badly damaged tissue. It is believed that, in time, stem cell research could revolutionise medicine, as stem cells could be used to repair tissues or even to grow replacement organs.

Which of the following statements is correct?

☐ A. The only difference between stem cells and other cells is that stem cells do not perform a specialised function.

☐ B. A muscle cell that originated from a stem cell may transform back into a stem cell.

☐ C. Stem cells are the only cells that have the ability to repair themselves.

☐ D. Stem cells could repair damaged tissues by multiplying and then replacing damaged cells.

1. Elimination tool
2. Calculator
3. Scratchpad

Answered Answered and bookmarked Bookmarked

Back 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OVERVIEW (16) Next

Bookmark tool

Question screen: question navigator at the bottom, bookmark, clock and tools at the top.

Verbal Reasoning

Test Configuration

Set

Showing statements is correct?

Post-traumatic stress disorder is defined as high blood pressure.

Stress from post-traumatic stress disorder can interfere with recovery by themselves.

Stress can trigger memories of distressing events.

Stress is generally ineffective in treating post-traumatic stress disorder.

Calculator

1013x2

2026

AC ± % ÷

Answer elimination: cross out what you have ruled out.

Highlighter and line reader for long stems.

Calculator and scratchpad where the test allows them.

Screenshots of the TAO platform used in EPSO tests.

The reserve list is published in alphabetical order, not by score; everyone tying for the last place goes on it; and being on it guarantees no recruitment.

Sources: notice of competition OJ C/2026/4668, sections 1, 4.2, 4.3.1, 4.3.2 (tables 3 to 5), 4.3.3 and 4.3.4.

3 · What the 30 questions look like

The notice publishes no syllabus and no reading list. The contract is **Annex II, «typical duties»**: everything examinable comes from there, which is why this dossier breaks it down in full. Thirty questions in 40 minutes, in language 2: **80 seconds per question**. There is no time to derive anything from scratch — you answer with what you recognise.

A scenario from your working life
A national authority detects a significant incident in an essential entity...

- ☐ A · Notify the CSIRT within 72 hours
- ☒ B · Early warning to the CSIRT within 24 hours
- ☐ C · Final report to the Commission within a month
- ☐ D · Notify the Cooperation Group

What decides the answer

- 1 WHO is competent
CSIRT, authority, Commission...
- 2 WHICH exact duty
early warning, notification, report
- 3 THE NUMBER
24 h · 72 h · one month

Distractors attack one of the three: the neighbouring deadline, the adjacent the duty from another phase.

Anatomy of a field question: 80 seconds to recognise three facts.

The five traps of the format

- **The longest option.** In official papers the key is the longest option only about 4 times out of 10: picking by length does not pass.
- **The absolute.** «Always», «never», «in all cases» usually mark the false option: EU law lives on exceptions.
- **The swapped actor.** The duty is described correctly but hung on the wrong body. Read the subject before the verb.
- **The neighbouring instrument.** The statement is true, but it belongs to another law that does not govern this case.
- **Superseded law.** Wording from before an amendment. Always study the consolidated text.

The fact sheet that works

Who it applies to	What it requires	Deadlines and figures	Who supervises
entities · products	the exact conduct	24 h · 72 h · threshold	and who sanctions

One fact sheet per instrument: four columns, nothing more. That is what answers a question in 80 seconds.

4 · The syllabus, block by block

Annex II describes duties, not subjects. Here they are turned into study blocks: what is in, what gets confused and where it is written. What is not in an official text is not examined.



Field 2 is about decisions: which control, which deadline and who answers when something happens.

1 - Risk management and security assurance

Risk frameworks (RMF, CSF 2.0)

Controls and monitoring

Vulnerabilities and testing

European certification

2 - Architecture, design and technology

Zero Trust, cloud and virtualisation

Identity and access

Cryptography and post-quantum

Secure development and DevSecOps

Emerging technologies

3 - Security operations and incident response

Operations and detection

Response and forensics

Continuity and sanitisation

4 - Governance, policy and coordination

EU institutions (2023/2841)

NIS2 and implementation

Cyber Resilience Act

Cyber Solidarity Act

DORA

Policy and criminal law

5 - Awareness, skills and advisory

Training and ECSF profiles

Annex II turned into study blocks.

1 Cybersecurity of the EU institutions — Regulation 2023/2841

The framework of the house you will work in. It comes up often and is systematically confused with NIS2.

What is in

- Article 6 framework: approved at the highest level of management by 8 April 2025, covering on-premises, cloud, operational technology and mobile, reviewed at least every four years.
- Article 7 maturity assessment: by 8 July 2025 and at least every two years.
- Article 8 measures and the Article 9 cybersecurity plan, revised every two years.
- The local cybersecurity officer: duties and reporting line.
- Article 21 reporting to CERT-EU: early warning within 24 hours, notification within 72 hours, final report within one month.
- IICB (Articles 10 to 12) decides and issues guidance; CERT-EU (Article 13) provides services.

What gets confused

- CERT-EU does not supervise, sanction, or act as anyone's national CSIRT: it serves Union entities.
- Union entities are NOT under NIS2: if the scenario names an EU institution, the law is Regulation 2023/2841.

- Classified information follows a separate regime, Decision 2015/444, with its markings, zones and registries.

Sources: Regulation (EU, Euratom) 2023/2841, Articles 6 to 13 and 21 · Decision (EU, Euratom) 2015/444

2 NIS2 and Implementing Regulation 2024/2690

The sector's reference law and the richest source of deadline and threshold questions.

What is in

- The ten Article 21(2) measure areas: risk analysis, incident handling, business continuity, supply chain security, acquisition and development, effectiveness assessment, cyber hygiene and training, cryptography, human resources and access control, and multi-factor authentication.
- Entities covered by the Implementing Regulation: DNS, TLD registries, cloud, data centres, content delivery networks, managed and managed security service providers, online marketplaces, search engines, social networks and trust service providers.
- Article 3 significance criteria: direct loss above EUR 500 000 or 5 % of turnover, whichever is lower; trade-secret exfiltration; death or considerable health damage; unauthorised access.
- Article 23 staged reporting: early warning within 24 hours, incident notification within 72 hours, final report within one month.
- Management body responsibility (Article 20) and mandatory training.
- Service-specific thresholds in Articles 5 to 14 of the Implementing Regulation and its thirteen annex sections.

What gets confused

- ENISA does not supervise entities: national competent authorities do.
- Article 21 measures are not the GDPR security duties, however similar they look.
- Essential and important entities differ mainly in supervision and sanctions, not in the measures themselves.

Sources: Directive (EU) 2022/2555, Articles 20, 21 and 23 · Implementing Regulation (EU) 2024/2690 · ENISA technical guidance 2025

3 Cyber Resilience Act — Regulation 2024/2847

Products with digital elements: classification, deadlines and who answers along the chain.

What is in

- Classification: default product, important class I or II (Article 7 and Annex III) and critical (Article 8 and Annex IV).
- Article 32 conformity assessment routes by class.
- Manufacturer duties: vulnerability handling and the Article 13 support period, at least five years unless the product's life is shorter.

- Article 14 reporting of actively exploited vulnerabilities and severe incidents: early warning within 24 hours, notification within 72 hours, final report within 14 days, through the single reporting platform of Article 16.
- The open-source steward role (Article 24).
- Dates: general application on 11 December 2027, reporting duties from 11 September 2026, notified-body provisions from 11 June 2026.

What gets confused

- The CRA final report is due in 14 days; the NIS2 one in a month. That swap is the most common trap.
- The single reporting platform is created by Article 16, but the duty to report sits in Article 14.
- An internal service of an institution is not a product placed on the market.

Sources: Regulation (EU) 2024/2847, Articles 7, 8, 13, 14, 16, 24 and 32; Annexes I, III and IV

4 Cyber Solidarity Act and the EU Cyber Blueprint

European response to large-scale incidents: three parts and three levels.

What is in

- European Cybersecurity Alert System with national and cross-border cyber hubs (Articles 3 to 9).
- Cybersecurity Emergency Mechanism: coordinated preparedness, the EU Cybersecurity Reserve and mutual assistance (Articles 10 to 19).
- European Cybersecurity Incident Review Mechanism, run by ENISA at the request of the Commission or EU-CyCLONe (Article 21).
- Who may request deployment of the Reserve: Member States, Union institutions, bodies, offices and agencies, and DEP-associated third countries.
- Blueprint levels (Recommendation (EU) 2025/3445): technical in the CSIRTs network, operational in EU-CyCLONe, political through IPCR activation by the Council Presidency.

What gets confused

- The political level does not run the technical response: IPCR coordinates decisions, it does not contain incidents.
- EU-CyCLONe is operational, not political, and does not replace the CSIRTs network.

Sources: Regulation (EU) 2025/38 · Council Recommendation (EU) 2025/3445

5 European certification — Cybersecurity Act and EUCC

Certification framework: levels, voluntariness and who does what.

What is in

- The Article 52 assurance levels — basic, substantial and high — and the evaluation each one demands.
- Voluntariness under Article 56, unless Union or national law provides otherwise.
- Roles: ENISA prepares candidate schemes (Article 49), conformity assessment bodies certify (Article 60), national authorities supervise (Article 58) and the ECCG advises (Article 62).
- The EUCC scheme (Implementing Regulation 2024/482): Common Criteria and CEM, substantial equals AVA_VAN 1-2 and high AVA_VAN 3-5, no self-assessment, certificates valid up to five years.
- Holder duties on vulnerability management and the grounds for withdrawal.

What gets confused

- ENISA does not issue certificates: it prepares the schemes.
- Certification is not mandatory by default; saying so is a classic distractor.
- EUCC allows no self-assessment, unlike some basic-level schemes.

Sources: Regulation (EU) 2019/881, Articles 49, 52, 56, 58, 60 and 62 · Implementing Regulation (EU) 2024/482

6 DORA and the financial sector

It appears as a sectoral framework: learn the map and the border with NIS2, not the fine print.

What is in

- The five pillars: ICT risk management (Chapter II), incident management and reporting (III), digital operational resilience testing including threat-led penetration testing (IV), third-party risk with Lead Overseers for critical providers (V) and information sharing (VI).
- Management body responsibility under Article 5.
- Delegated Regulation 2024/1774 details the ICT risk management framework.
- Relation with NIS2: DORA is *lex specialis* for financial entities.

What gets confused

- The European Supervisory Authorities do not supervise an individual bank: national competent authorities do.
- A DORA major-incident report is not a NIS2 notification, and the deadlines differ.

Sources: Regulation (EU) 2022/2554, Article 5 and Chapters II to VI · Delegated Regulation (EU) 2024/1774

7 EU policy and criminal law

Attribution questions: what each instrument says and whose competence it is.

What is in

- The 2020 Cybersecurity Strategy: resilience and technological sovereignty; operational capacity to prevent, deter and respond; a global and open cyberspace.
- The cyber sanctions regime of Regulation (EU) 2019/796: cyber-attacks with significant effect, listing by the Council, freezing enforced by Member States.
- Directive 2013/40: illegal access, system and data interference, interception, tools; aggravating circumstances such as botnets or critical infrastructure; 24/7 contact points.
- The Cybersecurity Skills Academy (COM(2023) 207) and its four pillars.

What gets confused

- Sanctions are decided by the Council; criminal law is applied by Member States. They do not mix.
- The Academy is not a body with powers: it is a policy initiative.

Sources: JOIN(2020) 18 · Regulation (EU) 2019/796 · Directive 2013/40/EU · COM(2023) 207

8 Risk management frameworks — RMF, SP 800-30 and CSF 2.0

The technical backbone. The exam asks for the order of the steps and the output of each.

What is in

- The seven RMF steps (SP 800-37r2): Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor, with the product of each step.
- Risk assessment per SP 800-30r1: threat sources, threat events, vulnerabilities and predisposing conditions, likelihood and impact; the prepare-conduct-communicate-maintain process; the three organisational tiers.
- CSF 2.0 (CSWP 29): six Functions including Govern, Categories and Subcategories, Current and Target Profiles, and Tiers 1 to 4.
- Maturity models: what they are for and how they differ from a risk assessment.

What gets confused

- CSF Functions are not RMF steps, nor ISO 27001 clauses.
- CSF Tiers describe rigour of governance, not a security score.

Sources: NIST SP 800-37r2 · NIST SP 800-30r1 · NIST CSWP 29

9 Controls, assessment and continuous monitoring

What Annex II calls security assessment operations and metrics.

What is in

- SP 800-53r5 control families and the difference between a base control and an enhancement.
- Baselines and tailoring guidance moved to SP 800-53B; r5 keeps the concepts: scoping, compensating controls and organisation-defined parameters.
- SP 800-53A assessment methods: examine, interview and test, and the evidence each produces.
- Continuous monitoring (SP 800-137): define the strategy, establish, implement, analyse and report, respond, review and update; three tiers; what drives frequency.
- Measurement (SP 800-55): implementation, effectiveness and impact measures.

What gets confused

- An annual audit is not continuous monitoring.
- A metric that triggers no decision is not a security metric, just a number.

Sources: NIST SP 800-53r5 · SP 800-53A r5 · SP 800-137 · SP 800-55

10 Vulnerability management and security testing

Tell the techniques apart by goal, scope and evidence — and know which rule demands them.

What is in

- Scanning, penetration testing and red teaming: what each looks for and what it delivers.
- SP 800-115 phases: planning, discovery, attack and reporting; review techniques, target identification and analysis, and target vulnerability validation.
- Enterprise patch management (SP 800-40r4): risk responses accept, mitigate, transfer or avoid; maintenance groups; the patch life cycle.
- OWASP ASVS 5.0 levels and the WSTG 4.2 test categories.
- The legal trigger: Annexes 6.5 and 6.10 of Implementing Regulation 2024/2690.

What gets confused

- A scan is not a penetration test: the goal and the evidence differ.
- The Implementing Regulation makes testing risk-based, not unconditional.

Sources: NIST SP 800-115 · SP 800-40r4 · OWASP ASVS 5.0 and WSTG 4.2 · IR (EU) 2024/2690

11 Security architecture — Zero Trust, cloud and virtualisation

Architecture concepts with very specific vocabulary.

What is in

- SP 800-207 tenets and logical components: the policy engine decides, the policy administrator establishes and the policy enforcement point enforces.
- Sources feeding the trust algorithm: continuous diagnostics, industry compliance, threat intelligence, activity logs and SIEM.
- Approaches: enhanced identity governance, micro-segmentation and software-defined perimeter; deployed variations: device agent and gateway, enclave gateway, resource portal and device application sandboxing.
- Threats specific to a Zero Trust architecture (Section 5).
- Cloud and virtualisation: SP 800-145 for models, SP 800-144 for shared responsibility and SP 800-125 for the hypervisor.

What gets confused

- Zero Trust is not a product or a network perimeter: it is a per-access decision strategy.
- The transition is incremental and starts with the highest-value assets; replacing everything at once is the typical false option.

Sources: NIST SP 800-207 · SP 800-145, 800-144 and 800-125

12 Identity and access management

Assurance levels are the distractors' favourite ground.

What is in

- IAL, AAL and FAL, each from 1 to 3: what each level demands in identity proofing, authentication and federation.
- SP 800-63B-4 authenticator rules: multi-factor, phishing-resistant and syncable authenticators, and re-authentication.
- Privileged access with SP 800-53r5: AC-2 account management, AC-5 separation of duties and AC-6 least privilege; Annex 11.3 of Implementing Regulation 2024/2690.
- eIDAS trust services: advanced versus qualified electronic signature, qualified seal and timestamp, the European Digital Identity Wallet, and their legal effects.

What gets confused

- AAL2 is not AAL3: phishing resistance and the authenticator type change.
- An advanced signature is not a qualified one: only the qualified has the effect of a handwritten signature.

Sources: NIST SP 800-63-4 (A, B and C) · SP 800-53r5 · Regulation (EU) 910/2014 consolidated

13 Cryptography, key management and the post-quantum transition

Figures, states and processes: highly examinable and easy to get wrong.

What is in

- Key lifecycle and key states; the factors that set a cryptoperiod (SP 800-57 Part 1, Section 5.3).
- Key types and the protection each needs.
- Security strength and algorithm-transition guidance (Section 5.6).
- Post-quantum standards: FIPS 203 ML-KEM for key encapsulation, FIPS 204 ML-DSA and FIPS 205 SLH-DSA for signatures.
- What Recommendation (EU) 2024/1101 actually asks for: a sub-group of the NIS Cooperation Group, a Coordinated Implementation Roadmap within two years, national transition plans, hybrid schemes and a review within three years.

What gets confused

- A key encapsulation mechanism is not a signature scheme: ML-KEM and ML-DSA are not interchangeable.
- The EU recommendation sets no migration deadlines: inventing them is the most repeated error.

Sources: NIST SP 800-57 Part 1 r5 · FIPS 203, 204 and 205 · Recommendation (EU) 2024/1101

14 Secure development and DevSecOps

Annex II calls it secure development; the source is the SSDF.

What is in

- The four SSDF groups (SP 800-218): Prepare the Organization, Protect Software, Produce Well-Secured Software and Respond to Vulnerabilities.
- Security in the CI/CD pipeline (SP 800-204C) and the five code types: application, application services, infrastructure as code, policy as code and observability as code.
- Service-mesh controls and where they sit.
- Systems security engineering (SP 800-160 vol. 1 r1): ISO 15288 processes, trustworthiness and the assurance case.
- Legal hooks: Annexes 6.2 and 6.3 of Implementing Regulation 2024/2690 and the CRA requirements.

What gets confused

- A single late-stage scan is not DevSecOps.
- Infrastructure as code and policy as code are code to protect too: that is the usual omission.

Sources: NIST SP 800-218 · SP 800-204C · SP 800-160 vol. 1 r1

15 Security operations — logs, detection and threat intelligence

SOC, monitoring and the threat landscape.

What is in

- Log management (SP 800-92): generation, storage and analysis; the roles of syslog and the SIEM; policies per environment; common challenges.
- Threat information sharing (SP 800-150): indicators versus tactics, techniques and procedures; consume, use, organise and produce; validation and prioritisation.
- Traffic Light Protocol for dissemination: red, amber, green and white.
- The ENISA threat landscape and its methodology: actors, techniques and the sectors most affected.

What gets confused

- An indicator of compromise is not a tactic: the first expires, the second describes behaviour.
- The SIEM does not generate the logs: it receives them. Confusing this changes the answer.

Sources: NIST SP 800-92 · SP 800-150 · ENISA Threat Landscape 2025 and CTL methodology

16 Incident response and digital forensics

Where phases and order of action are most often confused.

What is in

- The SP 800-61r3 life cycle built on CSF 2.0: preparation (Govern, Identify, Protect) and lessons learned versus the response phases (Detect, Respond, Recover), with the table mapping the earlier four-phase model.
- The SP 800-86 forensic process: collection, examination, analysis and reporting; volatile data first; integrity and chain of custody.
- Data sources: files, operating systems, network traffic and applications.
- CERT-EU reporting deadlines under Article 21 of Regulation 2023/2841 and coordination under Article 22.

What gets confused

- Eradicating before capturing evidence destroys the case: the order matters and is examined.
- Recovery is not closure: lessons learned are part of preparing for the next incident.

Sources: NIST SP 800-61r3 · SP 800-86 · Regulation (EU, Euratom) 2023/2841

17 Continuity, contingency and media sanitisation

Closed lists and parameters: quick marks if you know them.

What is in

- SP 800-34r1 plan types: business continuity, continuity of operations, crisis communications, critical infrastructure protection, cyber incident response, disaster recovery, information system contingency and occupant emergency.
- RTO, RPO and maximum tolerable downtime, derived from the business impact analysis.
- Recovery strategies: backup methods and cold, warm, hot, mobile and mirrored sites.
- Media sanitisation (SP 800-88r2): clear, purge and destroy; cryptographic erase and its preconditions; the Section 4.3 decision flow by media type, reuse and FIPS 199 confidentiality categorisation.

What gets confused

- RTO is not RPO: one measures time to return, the other how much data you can afford to lose.
- Clearing is not purging, and degaussing does not work on flash memory, which stores no data magnetically.

Sources: NIST SP 800-34r1 · SP 800-88r2

18 Awareness, training and the cybersecurity workforce

It closes Annex II and answers quickly if you know the lists.

What is in

- SP 800-50r1 learning programme: needs assessment; plan and strategy; analysis and design; development and implementation; assessment and improvement.
- Awareness versus role-based training: different goal, different measurement.
- The twelve ENISA ECSF role profiles and the NICE framework (SP 800-181r1) with its work roles and task, knowledge and skill statements.
- Legal triggers: NIS2 Article 20(2), Annex 8 of Implementing Regulation 2024/2690 and Article 8(1) (p) of Regulation 2023/2841.

What gets confused

- A yearly e-learning is not a programme: the needs assessment and the measurement are missing.
- Do not invent ECSF profiles: the list is closed and distractors usually add a fake one.

Sources: NIST SP 800-50r1 · SP 800-181r1 · ENISA ECSF

19 Emerging technologies — AI in security and quantum readiness

The bridge to the other field of this competition.

What is in

- The three layers of the ENISA multilayer framework: cybersecurity foundations, AI fundamentals and the sector-specific layer.
- NIST AI 100-2 attack classes that matter when a SOC adopts machine learning or LLM tooling.
- The OWASP LLM Top 10 items to control first in an organisation.
- Quantum readiness: cryptographic inventory, agility, hybrid schemes and the process of Recommendation (EU) 2024/1101.

What gets confused

- A machine-learning tool does not replace a control: it complements it.
- There are no EU post-quantum migration deadlines: there is a process with planning milestones.

Sources: ENISA multilayer framework · NIST AI 100-2 · OWASP LLM Top 10 · Recommendation (EU) 2024/1101

5 · How to study it in eight weeks



Eight weeks allow two passes over the syllabus if you answer questions from day one.

week	1	2	3	4	5	6	7	8	
Map and fact sheets									
Block-by-block study									
Weak blocks and figures									
Timed mock tests									
Review and reasoning									

Split: two thirds on the field, one third on reasoning. The field ranks you; reasoning only eliminates. And from week 3, answer questions the same day you study the block: reading without answering fixes nothing.

6 · Official library

Everything below is public and citable. No serious preparation needs more, and no commercial manual replaces the consolidated text.

Document	What for
Regulation (EU, Euratom) 2023/2841 and Decision 2015/444	Cybersecurity of Union entities and EU classified information.
Directive (EU) 2022/2555 and Implementing Regulation 2024/2690	Measures, significance thresholds and reporting deadlines.
Regulation (EU) 2024/2847 — Cyber Resilience Act	Products with digital elements, classes and reporting.
Regulation (EU) 2025/38 and Recommendation (EU) 2025/3445	Cybersecurity Reserve and crisis management.
Regulation (EU) 2019/881 and Implementing Regulation 2024/482	European certification and the EUCC scheme.
Regulation (EU) 2022/2554 and Delegated Regulation 2024/1774	DORA and the ICT risk management framework.
JOIN(2020) 18 · Regulation 2019/796 · Directive 2013/40 · COM(2023) 207	Strategy, sanctions, criminal law and skills.
NIST SP 800-37r2 · SP 800-30r1 · CSWP 29	Risk management framework, assessment and CSF 2.0.
NIST SP 800-53r5 · 800-53A r5 · 800-137 · 800-55	Controls, assessment, continuous monitoring and metrics.
NIST SP 800-115 · 800-40r4 · OWASP ASVS and WSTG	Security testing and patch management.
NIST SP 800-207 · 800-144/145/146 · 800-125	Zero Trust, cloud and virtualisation.
NIST SP 800-63-4 (A, B, C) and Regulation 910/2014	Identity, authentication and trust services.
NIST SP 800-57 Pt.1 r5 · FIPS 203/204/205 · Recommendation 2024/1101	Keys, post-quantum and the EU roadmap.
NIST SP 800-218 · 800-204C · 800-160 v1r1	Secure development, CI/CD and systems security engineering.
NIST SP 800-92 · 800-150 · ENISA Threat Landscape 2025	Logs, threat intelligence and the landscape.
NIST SP 800-61r3 · 800-86 · 800-34r1 · 800-88r2	Incidents, forensics, continuity and sanitisation.
NIST SP 800-50r1 · SP 800-181r1 · ENISA ECSF	Awareness, training and workforce profiles.

7 · Before you call yourself ready

- Do you keep the NIS2, CRA and 2023/2841 deadlines apart, final report included?
- Do you know who supervises, who certifies and who assists in each European framework?
- Can you recite the seven RMF steps and the six CSF 2.0 Functions with their output?
- Can you tell scanning, penetration testing and red teaming apart by goal and evidence?
- Are IAL, AAL and FAL clear, and the three post-quantum standards with their function?
- Do you know why degaussing does not sanitise flash memory, and what cryptographic erase needs?
- Have you done three mock tests of 30 questions in 40 minutes, in your language 2?

Practise with questions from this field, in the five languages of the exam.

EPSO/AD/430/26 cybersecurity bank, with the explanation and the article behind every answer: eu-now.com/specialist/cybersecurity



And when something does not click, ask. In EU-now, EUgenio answers with the law in front of it and cites the article the answer comes from: the difference between knowing you got it wrong and knowing why.

Figures and deadlines come from the notice published in the Official Journal (C/2026/4668) and from the official texts cited. If EPSO publishes a corrigendum, the Official Journal prevails.