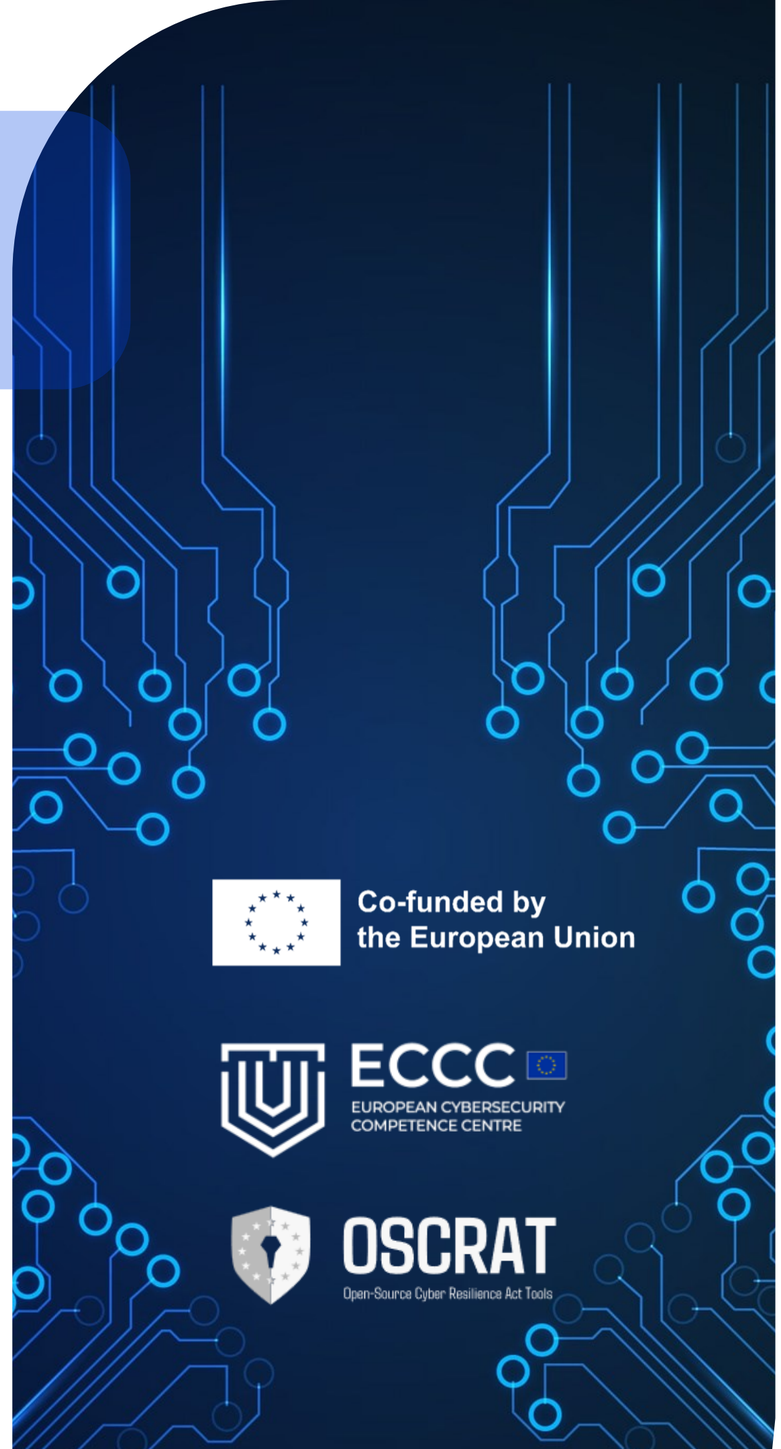
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Regulation (EU) 2024/2847

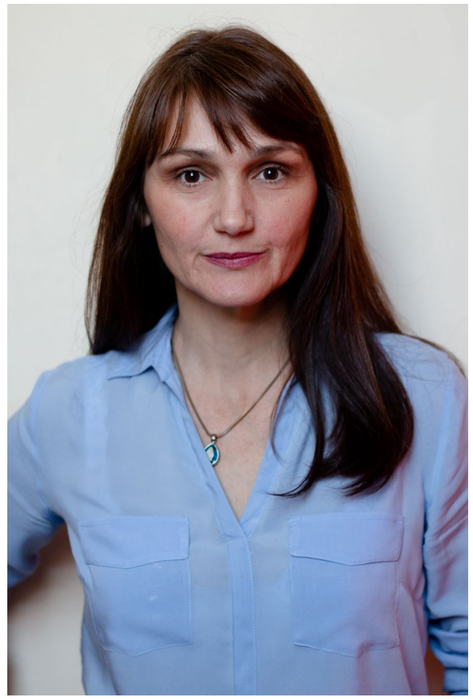
CYBER RESILIENCE ACT

November 2025



Digital Innovation Hub
Trakia

Introduction



Sashka Boncheva

Cybersecurity Expert at EDIH Trakia, Bulgaria

Trainer and Consultant

ISO/IEC 27001 Lead Auditor

Elegant Systems Ltd., Founder

Women4Cyber Bulgaria, Co-founder

s.boncheva@dihtrakia.org

Cyber Resilience Act

Integrating the Cyber Resilience Act with Risk Management Processes

- Bridging compliance, security, and lifecycle risk management

Uncertainty: The New Normal

“We must accept that we live in a world with much more uncertainty. Uncertainty is the new normal.”
— Kristalina Georgieva, Managing Director, IMF

*ISO 31000 defines risk as **“the effect of uncertainty on objectives.”***

Managing risk means navigating uncertainty — not avoiding it.

Defining “Cybersecurity Risk” under the CRA

Term	CRA Definition	Interpretation
Cybersecurity risk - Art. 3 (37)	*“The potential for loss or disruption caused by an incident, expressed as a combination of the **magnitude** of such loss or disruption and the **likelihood** of occurrence of the incident.”*	Quantitative concept: **impact** × **likelihood** — aligns with ISO 31000 / 27005 risk formula.
Significant cybersecurity risk - Art. 3 (38)	*“A cybersecurity risk which, based on its technical characteristics, can be assumed to have a **high likelihood** of an incident that could lead to a **severe negative impact**, including considerable material or non-material loss or disruption.”*	High-impact, high-likelihood scenario; used for prioritization, reporting, and classification.

Why Integration Matters

CRA and Risk Management: Two Sides of the Same Coin

- CRA treats cybersecurity as a business risk, not just a technical issue.
- Integration ensures **vulnerabilities**, **incidents**, and **updates** follow the same cycle as financial and operational risks.
- Builds traceability and accountability across development, compliance, and management.
- Effective integration reduces duplication with ISO 27001 / DORA / NIS2

CRA Risk-Based Provisions

Where the CRA Embeds Risk Thinking

CRA Reference	Focus Area	Risk Relevance
Article 13	Secure design, development, delivery, maintenance	Lifecycle risk minimization
Annex I	Essential cybersecurity requirements	Risk control categories
Annex VII (3)	Cyber risk assessment in technical documentation	Traceability: **Risk → Control → Evidence**

Annex VII, Point 3 Explained

Cyber Risk Assessment as Part of Technical Documentation

- Identify and evaluate cybersecurity risks across the product lifecycle
- Link each risk to specific Annex I controls
- Demonstrate mitigation and residual risk
- Provide traceability: **Risk → Control → Evidence**
- Integrate updates and vulnerability management as continuous risk reassessment

CRA Mapped to ISO 31000 / ISO 27005

CRA Aligned with the ISO Risk Lifecycle

ISO 31000 / 27005 Phase	CRA Equivalent Obligation
Context & Asset Identification	Art. 13 – Design and development context
Risk Identification	Annex VII (3) – Cyber risk assessment
Risk Analysis & Evaluation	Mapping to Annex I controls
Risk Treatment	Secure design, vulnerability management, encryption
Risk Communication	Annex II – User information
Monitoring & Review	Ongoing vulnerability handling, updates and reassessment of residual risk

Documentation and Traceability

What to Document, How, and for Whom

Document type	Audience	Content / Purpose
Technical Documentation	Authorities / auditors	Full risk assessment results, methodology, mapping to Annex I, residual risk levels
Internal Risk Register (ISMS)	Management / Security team	Continuous tracking: detailed risks, treatments, KPIs
User Information (Annex II)	Clients / end users	Summary of security assurances, safe configuration, update policy

Example: SmartTech Software Company

Risk Identification

Risk	Likelihood	Impact	Related CRA Requirement
Unpatched open-source library exploited	Medium	High	Annex I (6) – Vulnerability handling
Insecure API integration with external vendor	High	High	Annex I (2) – Access control
Lack of process to notify ENISA of incidents	Low	Critical	Article 14 – Incident reporting

Example: SmartTech Software Company

Risk Treatment and Traceability

Identified Risk	Annex I Requirement	Mitigation / Control	Evidence
Unpatched open-source library exploited	Annex I (6) – Vulnerability handling	SBOM management, 30-day patch policy integrated into CI/CD	Patch policy, automated scan logs
Insecure API integration with external vendor	Annex I (2) – Access control	Vendor assessment checklist and API authentication hardening	Supplier audit record
Lack of process to notify ENISA of incidents	Annex I (4) – Data protection	Establish a formal Incident Reporting Procedure	Approved Incident Reporting Procedure; notification log

Example: SmartTech Software Company

Documentation under CRA

Document Type	CRA Reference	Content Related to the Example	Audience / Purpose
Technical Documentation	Article 23, Annex VII	– Full cyber risk assessment (risks, controls, evidence) – Mapping to Annex I requirements – Patch management and vulnerability policy – Test results and verification evidence	Authorities / Conformity assessment bodies
Information & Instructions for the User	Article 13, Annex II	– Secure configuration and update procedure – Minimum system requirements – Known limitations or foreseeable misuse – Security support and update period	End users / Integrators

Continuous Integration Workflow

This diagram was generated using ChatGPT (GPT-4o), an AI-powered tool for visual content creation.

Integration Benefits

Why CRA Integration Strengthens the Organization

- Unified risk picture for CRA, DORA, and NIS2 compliance
- Streamlined documentation and audits
- Stronger supplier due diligence and client assurance
- Enhanced trust and market reputation

THANK YOU

FOR YOUR ATTENTION

November 2025

Sashka Boncheva

m: +359 888 800 222

s.boncheva@dihtrakia.org

CYBER
4 ALL STAR

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BULGARIA

Digital Innovation Hub
Trakia