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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Risk Management

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

Lead Auditor for Management Systems, with expertise in information security, artificial intelligence, IT services, quality management, and related domains.

Chairman of the Institute for Artificial Intelligence.

Deputy Manager of the Bulgarian Union of Standardizers.

Active contributor to numerous European and national cybersecurity projects, with a focus on standards, resilience, and digital transformation.

Assistant Professor at UniBIT, teaching:

- Cybersecurity Standards
- Cybersecurity Management
- Cryptography
- Zero Trust Architectures

Workshop 4
Risk Management

- Session 1: From Threats to Impact: Thinking in Risk, not just Security

  Speaker Miroslav Mitev

- Session 2: Embedding Risk Management into the Development Lifecycle

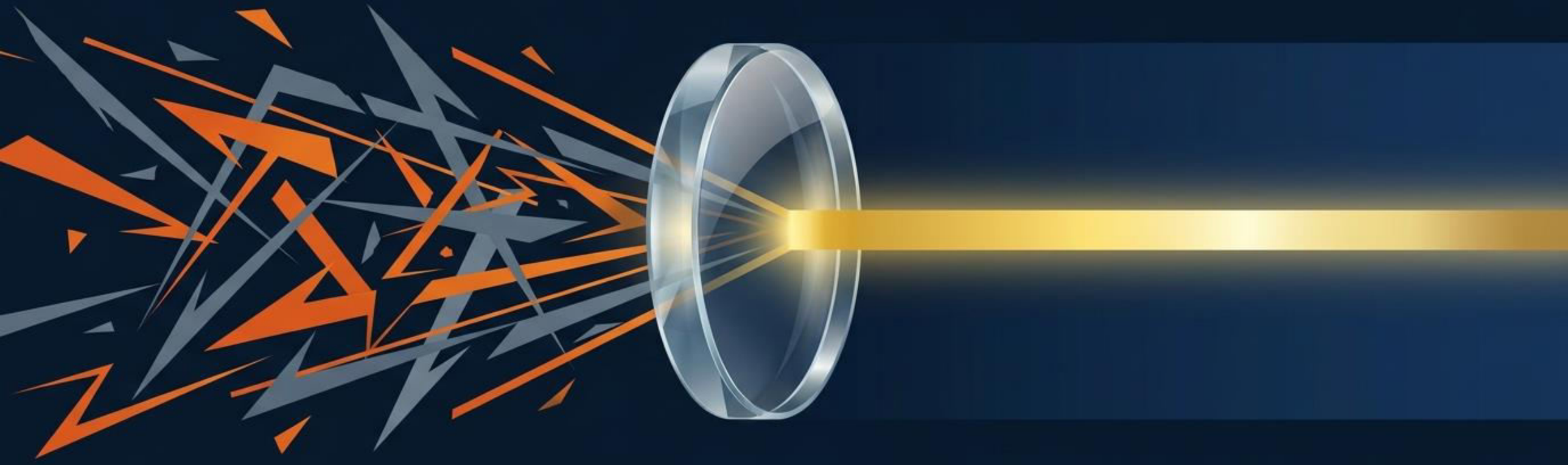
  Speaker Yasen Tanev

- Session 3: From Regulation to Implementation: Managing Risk under CRA

  Speaker Adrian Anghel

FROM THREATS TO IMPACT

THINKING IN RISK, NOT JUST SECURITY



The Illusion of Perfect Security vs. The Reality of Risk

Security Thinking

Goal:
Stop everything.
(An impossible mandate).

Focus:
Cyberspace vectors, malware, and technical perimeters.

Success Metric:
Number of attacks blocked.

Fatal Flaw:
Disconnected from business objectives; treats all assets equally; assumes a perimeter can be fully sealed.

Risk Thinking

Goal:
Manage business outcomes.
(A strategic mandate).

Focus:
The effect of uncertainty on objectives.

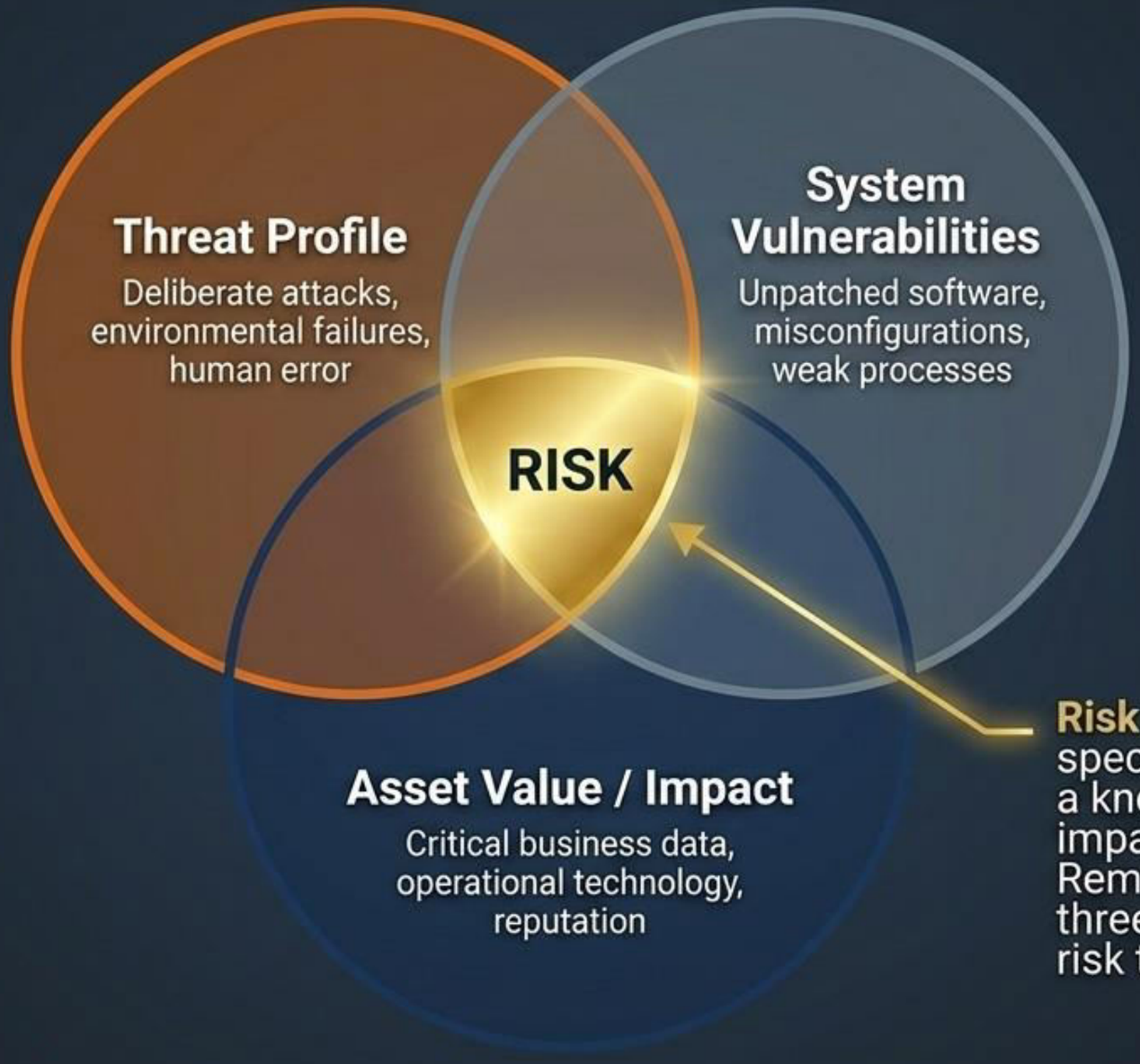
Success Metric:
Keeping cyber risks at a tolerable level aligned with risk appetite.

Strategic Advantage:
Prioritizes high-value assets; acknowledges that operation involves inherent risk; enables informed C-suite decision-making.

Cybersecurity is the safeguarding of organizations from cyber risks. Safeguarding means keeping risks at a tolerable level, not eliminating them.

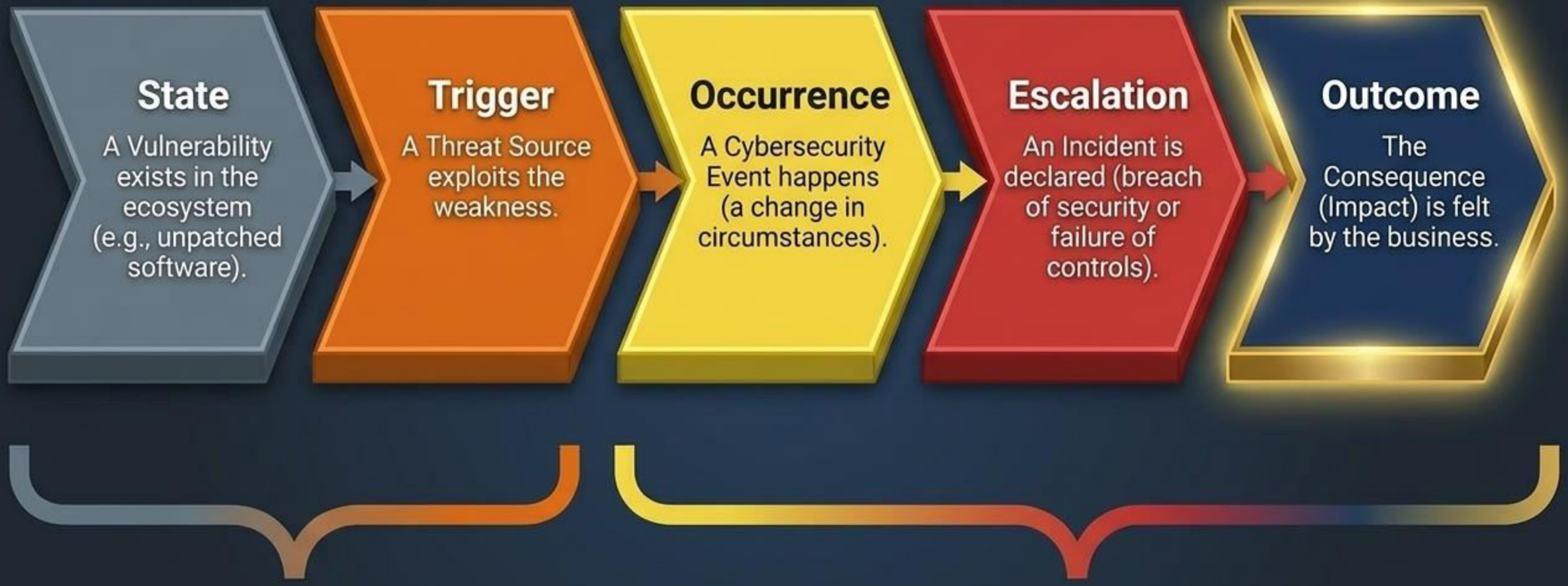
Precision in Language: The Core Lexicon

The Anatomy of Cyber Risk



Risk only exists where a specific Threat can exploit a known Vulnerability to impact an Asset of Value. Removing any one of these three elements reduces the risk to zero.

The Cascade: How Technical Flaws Become Business Problems



Security manages the left side of the timeline (Vulnerabilities & Threats).

Risk Management governs the entire continuum to control the right side (Consequences).

The Core Model: Calculating the Effect of Uncertainty

Likelihood
(The Probability Engine)

Based on experience, applicable statistics, attacker motivation (cost/benefit), and capability.

Impact
(The Consequence Engine)

Extent of damage or harm to an organization resulting from the loss of confidentiality, integrity, or availability.

Risk Level
(The Output)

Can be qualitative (Very High to Low) or quantitative (Annual Loss Expectancy in monetary value).

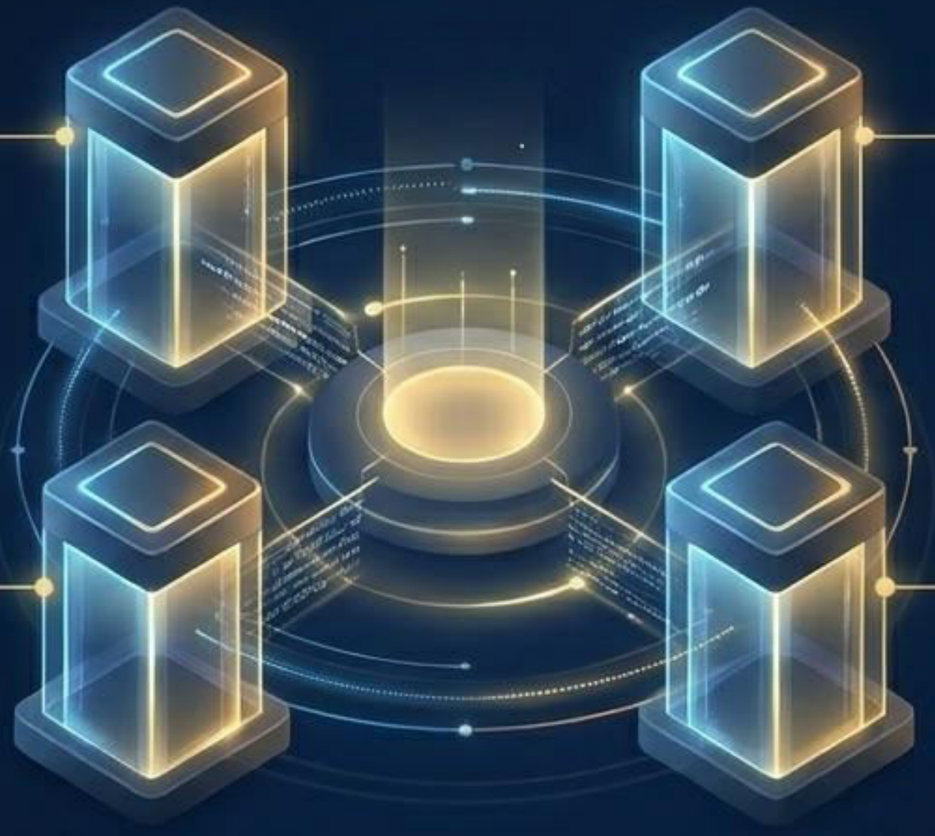
Translating Vectors to Value: The Dimensions of Impact

Financial & Business

Loss of business, financial value, or market share.

Operational

Impaired internal or third-party operations (damage to business functions, delayed deadlines).



Human & Safety

Loss of life, harm to individuals, loss of freedom or privacy.

Reputational & Legal

Damage to public trust, breaches of legal, statutory, or regulatory requirements.

A severe technical breach on a low-value, isolated asset generates low business impact.
A minor technical disruption on a critical financial node generates catastrophic impact.
Impact is defined by the business, not the IT department.

The Engine of Execution: The Risk-Based Approach

The Mandate

Shifting from ad-hoc technical patching to a disciplined, structured, and flexible process for managing security.

The Toolkits

Modern enterprise risk is governed by internationally recognized frameworks. While they use different lexicons, they share a unified objective: driving risk to acceptable levels through continuous, iterative cycles.

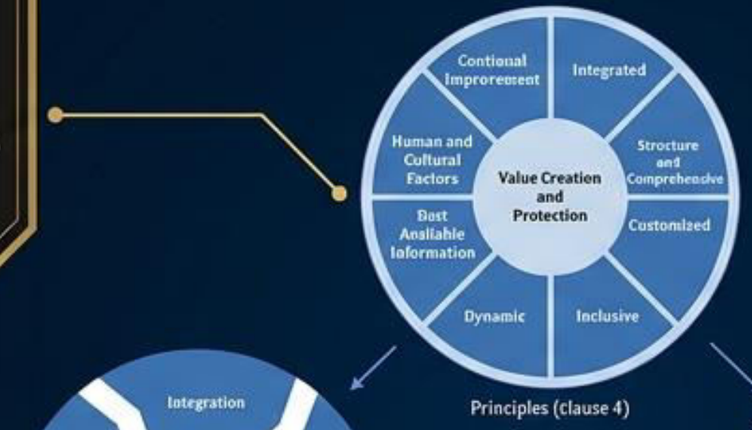
The Core Pillars

Context Establishment, Risk Assessment (Identify, Analyze, Evaluate), Risk Treatment, and Continuous Monitoring.

NIST RMF: The 7-Step Life Cycle

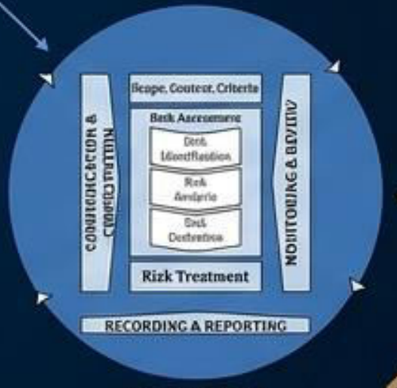
ISO 31000 & 27005: Value Creation and Protection

Principles:
Risk management is integrated, customized, and dynamic. It exists to create and protect value.



Principles (clause 4)

Framework (clause 5)



Process (clause 6)

Iterative Nature:
Risk treatment involves an iterative process: formulating options, implementing treatment, assessing effectiveness, and deciding if residual risk is acceptable.

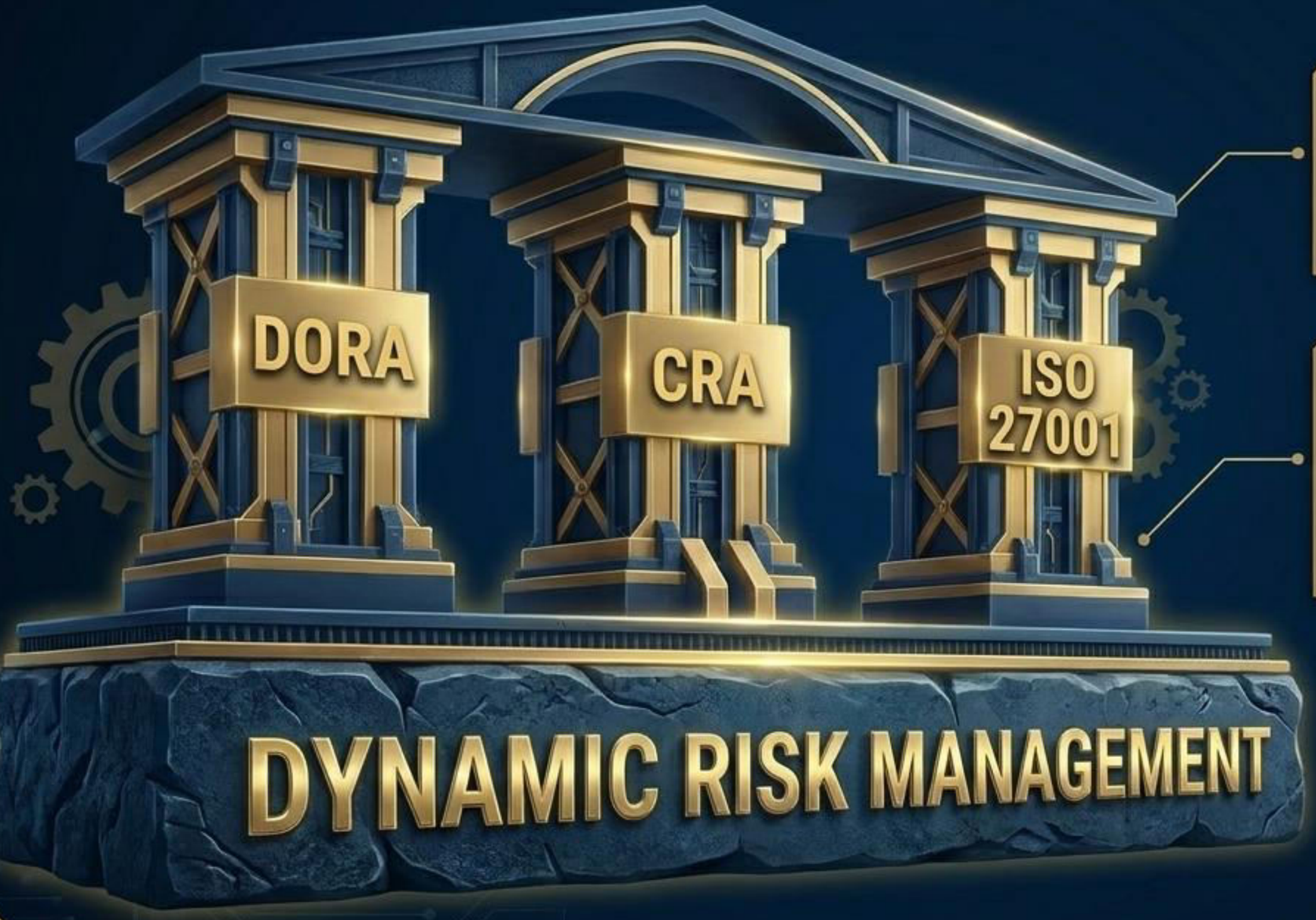
Process Core:
The heart of ISO 27005 is Risk Assessment (Identification, Analysis, Evaluation) followed by Risk Treatment.

Framework Alignment: Two Paths, One Destination

NIST RMF	Phase	ISO 27005/31000
Prepare & Categorize	Context & Foundation	Context Establishment
(Embedded in Prepare/Select)	Risk Assessment	Risk Identification, Analysis, & Evaluation
Select & Implement	Mitigation	Risk Treatment
Assess	Validation	Assessing Effectiveness
Authorize	Governance	Risk Acceptance (Residual Risk)
Monitor	Ongoing Visibility	Monitoring & Review

Both frameworks demand that senior leadership accepts accountability for the residual risk.

Why Risk is the Absolute Bedrock of Compliance



Compliance is no longer a checklist of static technical controls. Modern European and global regulations mandate a risk-based approach.

You cannot comply with modern regulations by simply buying security tools. You must prove you understand your risk exposure, your supply chain, and your impact on the broader ecosystem.

The Strategic Horizon: DORA, CRA, and ISO 27001

Cyber Resilience Act (CRA)

Focus:
Products and software.

Risk Mandate:
Introduces mandatory security requirements for digital products to reduce systemic vulnerabilities via security-by-design and formal vulnerability disclosure.

Digital Operational Resilience Act (DORA)

Focus:
Financial sector and ICT providers.

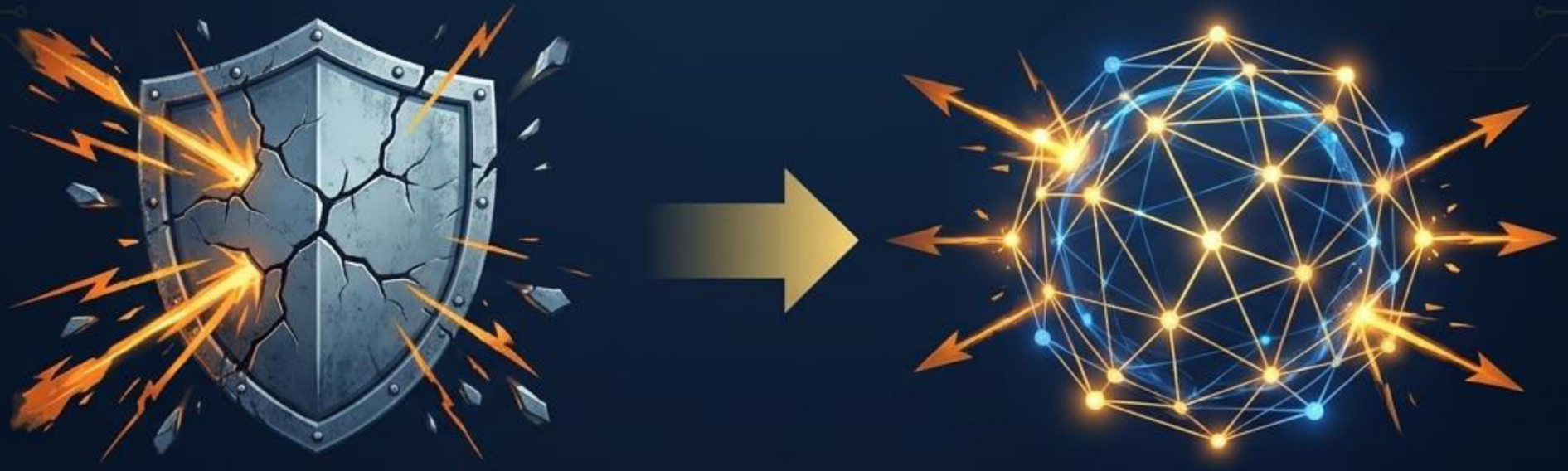
Risk Mandate:
Demands comprehensive management of interconnected digital environments and specifically targets ICT supply chain risk and cross-organizational coordination.

ISO/IEC 27001:2022

Focus:
Information Security Management Systems (ISMS).

Risk Mandate:
Requires an organization to formally assess information security risks (Clause 6.1.2) and treat them based on the organization's unique business drivers.

The Enterprise Advantage: From Reactive to Resilient



Reactive Defense

Resilient Advantage

Key Takeaways (Golden Rules of Risk)

1. Cyberspace is Borderless: You cannot defend everything. Prioritize by business value and consequence.

2. Shared Responsibility: Your risk is inherited by your supply chain, and you inherit theirs. Manage the ecosystem.

3. Continuous Calibration: Risk management is an iterative cycle, not a yearly audit.

4. Value Creation: Good risk management doesn't just prevent loss; it builds the trust required to innovate and accelerate in a digital world.

"The goal is not a perfectly secure system, but a resilient organization capable of operating confidently within defined levels of risk."

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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
phdmitev@gmail.com

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools