ERMIS

Newsletter

March 2026 - Issue No 6

In this Issue

From Cyber Volatility to Predictability

From Cyber Incidents to Systemic Risk

Europe is entering a decisive phase in its approach to cybersecurity, one in which cyber threats are no longer viewed as isolated technical incidents but as systemic risks with direct implications for economic stability, market confidence and insurability. For the insurance sector in particular, the escalation of ransomware, the growing geopolitical dimension of cyber operations and the increasing dependence on complex digital supply chains have exposed the limits of traditional cyber risk modelling. Correlated losses, opaque dependencies and uneven cybersecurity maturity across sectors have made predictability more difficult precisely at a time when demand for cyber insurance is growing.

CSA2 as Europe's Strategic Reset

The Cybersecurity Act 2 (CSA2) represents a strategic response to this challenge. Rather than introducing another layer of fragmented obligations, CSA2 seeks to modernise Europe's cybersecurity architecture by strengthening governance, reforming certification and addressing ICT supply chain risk at Union level. Its significance for insurers lies not only in its individual provisions, but in how it complements and reinforces the broader regulatory ecosystem shaped by DORA and NIS2. Together, these frameworks reshape the environment in which cyber risk is assessed, priced and transferred. CSA2 emerges against a backdrop of mounting pressure. In recent years, cyber incidents have become more disruptive and more interconnected, with attacks on one organisation cascading across sectors through shared technologies and service providers. For insurers, this has translated into rising loss ratios, reduced diversification benefits and increasing uncertainty around aggregation risk. Actuarial models built on historical data have struggled to keep pace with a threat landscape that evolves faster than reporting cycles and disclosure practices. Policymakers and market participants alike have recognised that greater coherence and stronger institutional coordination are essential to restore confidence.

Building Predictability Through Structure and Convergence

At the core of CSA2 is a shift toward structure and predictability. By reinforcing ENISA's operational role, the regulation strengthens Europe's capacity for coordinated threat intelligence and situational awareness. For insurers, this means access to more credible, centralised insights into systemic cyber risks, supporting better portfolio level analysis and earlier identification of emerging trends. At the same time, CSA2 modernises the European Cybersecurity Certification Framework, transforming it into a lifecycle managed system capable of keeping pace with technological change. The expansion of certification to managed services and organisational cyber posture provides insurers with externally validated indicators of maturity that reduce reliance on self-assessments and inconsistent disclosures.

Perhaps most importantly, CSA2 introduces a coordinated EU level approach to ICT supply chain risk, an area that has long represented one of the greatest blind spots in cyber underwriting. By enabling the identification of critical ICT assets and high-risk suppliers based on non-technical criteria, CSA2 directly addresses the systemic nature of digital dependencies. This development aligns closely with obligations under DORA and NIS2, which already require enhanced oversight of third party providers and supply chain risks within the financial sector and across essential and important entities. Together, the three frameworks transform supply chain risk from a largely hidden variable into a domain that is increasingly assessable, governed and evidence based. For insurers, the intersection of DORA, NIS2 and CSA2 marks a qualitative shift. Cyber maturity becomes more measurable as governance, reporting and certification practices converge across sectors. Information asymmetry narrows as regulated entities adopt more consistent risk management frameworks and supervisory expectations become clearer. Supply chain exposures, historically difficult to quantify, become more visible as EU level mechanisms identify and mitigate systemic dependencies. This convergence improves the quality of data available for underwriting, supports more robust modelling of correlated losses and reduces exposure to unexpected aggregation events.

Beyond compliance, these developments create strategic opportunity. As cyber risk becomes more transparent and structured, insurers are better positioned to refine pricing, develop more nuanced coverage and engage clients on resilience building measures. DORA, NIS2 and CSA2 collectively support a transition toward a more disciplined and insurable cyber risk environment, enabling insurers to move beyond risk absorption and toward a role as strategic partners in Europe's digital resilience. In doing so, they help lay the foundations for a more stable, predictable and sustainable cyber insurance market across the European Union.

By Spyros Chatziloizos, NCSA

4th Plenary Meeting

The DEP-ERMIS consortium convened in Heraklion for its Plenary Meeting on 18 February, followed by an open Workshop on 19 February, bringing together project partners, industry experts, and cybersecurity stakeholders. The Plenary Meeting focused on consolidating current technical progress and defining priorities for the next development phase. Discussions addressed the alignment of the project's technological evolution with real-world insurance use cases, the strengthening of Dynamic Certification Readiness and risk assessment mechanisms, and the continued enhancement of the ERMIS Marketplace to demonstrate iterative security assurance. Partners also coordinated dissemination activities and upcoming implementation milestones as the project advances toward its final stage.

Workshop on Cybersecurity & Insurance Perspectives, Industry Trends, Risk and Resilience

On February 19th, 2026, the ERMIS Project held the open workshop, titled "Cybersecurity & Insurance Perspectives: Industry Trends, Risk and Resilience", examined the evolving relationship between cybersecurity maturity and insurability. Contributions highlighted the role of Security Operations Centers in strengthening organisational resilience, emerging trends in cyber underwriting, and the development of cybersecurity market assurance and insurance-as-a-service models. The discussions reinforced the importance of collaboration between technology providers, insurers, and regulators in fostering transparency, trust, and resilience across Europe's cybersecurity and insurance ecosystem.

ERMIS Dynamic Regulation and Certification Readiness Model (DRCRM) in Action

Introducing DRCRM: A Dynamic Approach to Cybersecurity Readiness

In today's evolving threat landscape, cybersecurity certification and regulatory alignment are no longer one-time milestones — they are continuous responsibilities. Organisations, particularly in critical sectors, must demonstrate ongoing alignment with recognized standards and frameworks such as ISO/IEC 27001, NIS2, and DORA. Within the ERMIS project, this challenge has led to the development of the Dynamic Regulation and Certification Readiness Model (DRCRM).

From Static Compliance to Continuous Readiness

Traditional certification preparation often relies on manual checklists, spreadsheets, and fragmented documentation. This approach is time-consuming and reactive. DRCRM replaces this with a structured, continuous, and evidence-based readiness model. Instead of preparing only when audits approach, organisations can integrate regulatory and certification readiness into their daily operations.

How DRCRM Works

DCRM provides Standard - and regulation-aligned checklists, Customisable assessment instances tailored to each organisation, Manual and automated updates through integration with security tools, Structured and traceable evidence management and Controlled visibility for selected stakeholders. ERMIS plays a central role as the enabler of DRCRM. Through the ERMIS platform, organisations can manage checklists, automate evidence collection, monitor progress via dashboards, and securely share readiness data when needed.

Supporting Cyberinsurance and Transparency

DRCRM also strengthens the link between cybersecurity readiness and cyberinsurance. Organisations can grant insurers-controlled visibility into their readiness status, allowing underwriting decisions to rely on structured, up-to-date evidence rather than static questionnaires. This promotes transparency, supports risk-based pricing, and encourages continuous improvement — while protecting sensitive internal information.

A Community-Driven Approach

DRCRM goes beyond individual assessments. Organisations can voluntarily contribute structured insights on how they address specific checklist items, sharing practical approaches and lessons learned. This community aspect accelerates readiness across sectors and fosters collaborative improvement.

Designed for Critical and Regulated Environments

DRCRM is particularly suited for long-lived and mission-critical systems in sectors such as energy, healthcare, and public administration. By embedding readiness monitoring into system lifecycles, it supports ongoing regulatory alignment, improved audit preparation, and reduced administrative burden.

A Key Result of ERMIS

As a key exploitable result of the ERMIS project, DRCRM combines structured processes, machine-readable models, and controlled information sharing into a scalable framework for continuous cybersecurity readiness. Enabled by ERMIS, DRCRM demonstrates how digital tools can make regulatory and certification readiness more agile, transparent, and sustainable.

By Dr George Alexandris, Nodalpoint Systems Ltd

Contact

Project Coordinator Zelus **Inquiries** info@dep-ermis.eu

Disclaimer

The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cyber Security Authority and is aligned with the Hellenic Cyber Security Strategy.

Consortium Partners