Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27768-cd

The Emerging EU Regulatory Landscape: Risks, Operational Challenges, and Opportunities for Coherent Compliance

Ankur Shukla

Department of Risk and Security, Institute for Energy Technology (IFE), Halden, Norway.
E-mail: ankur.shukla@ife.no

Kanjar De

Department of Kvinnors och barns hälsa, Karolinska Institutet, Stockholm, Sweden. E-mail: kanjar.de@ki.se

The European Union (EU) is rapidly introducing a series of regulatory frameworks to strengthen digital trust, security, and accountability including the Artificial Intelligence Act, NIS2 Directive, Medical Device Regulation (MDR), In Vitro Diagnostic Regulation (IVDR), Cybersecurity Act, Data Act, General Data Protection Regulation (GDPR), Data Governance Act (DGA), Digital Services Act (DSA), Digital Markets Act (DMA), and the forthcoming Cyber Resilience Act (CRA) and standards such as ISO/IEC 27001 and ISO/IEC 42001. These regulations collectively aim to create a secure, resilient and trustworthy digital ecosystem. However, these regulations have evolved simultaneously and often in isolation, creating fragmented compliance framework and making it difficult to maintain consistent regulatory alignment. This paper discusses the potential risks and challenges associated with increasing number of regulations, overlapping governance obligations, duplicative conformity assessments, inconsistent data protection and cybersecurity provisions, increased administrative complexity and other operational challenges. These challenges may increase the risk of non-compliance and may hinder innovation and the practical implementation of emerging technologies. This paper identifies conceptual solutions and potential harmonizing strategies to improve alignment and reduce duplication of efforts. The recommendations of this paper can help to support policymakers, regulators, industry leaders, and compliance professionals to enhance both regulatory efficiency and technological innovation.

Keywords: EU Digital Regulations, regulatory compliance, compliance Challenges, Governance Fragmentation, Regulatory Harmonization, Digital Ecosystem Trust.

1. Introduction

The European Union (EU) has introduced various regulations and acts in the past decade to regulate the emerging technologies, digital economy, and balancing innovation with robust protections for fundamental rights, data privacy, cybersecurity, and consumer trust (Mariniello, 2022; Andraško et al., 2021). Some of the key regulations and act include the General Data Protection Regulation (GDPR) , the Digital Services Act (DSA) and Digital Markets Act (DMA), the Data Governance Act (DGA) (2023), the Data Act, the Network and Information Systems Directive 2 (NIS2), the Cybersecurity Act, the Artificial Intelligence Act (AI Act), and the Cyber Resilience Act (CRA). Complementing these there are several sector-specific regulations and international standards such as the Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR) like ISO/IEC 27001, ISO/IEC 42001, and IEC 62443.

The existing and emerging regulatory environment reflects the EU's commitment to ethical, secure, and human-centric digital transformation. These regulatory frameworks address critical concerns associated with emerging technologies and digitalization such as reducing risks (e.g., fundamental rights and safety of AI), enhancing cyber resilience across critical sectors, enabling fair data use, protecting personal data, and securing digital products throughout their lifecycle (Jørgensen and Ma, 2025; Graux et al., 2025; Andraško et al., 2021). However, the rapid and parallel development of these regulations may create several challenges for organizations to adopt and implement (OECD, 2021). Some of these challenges include duplicative requirements, inconsistent def-

initions and timelines, and varying enforcement mechanisms. Particularly, the organizations that are operating in the critical infrastructure such as healthcare, finance, nuclear energy, and transport face increased administrative pressure, legal uncertainty, expertise, resource strain, and risks of unintentional non-compliance (Grima et al., 2019; Pelkmans and Renda, 2014; Irbe, 2024). These challenges can deter investment, slow innovation deployment, and undermine the EU's competitive goals, as highlighted in recent high-level reports emphasizing the need for simplification.

In this paper, we discuss the risks and operational challenges because of the current European multifaceted regulatory environment, overlapping governance obligations, non-compliance exposure, innovation hurdles, enforcement disparities, and practical implementation barriers. This paper also discusses the potential opportunities and solutions to overcome these risks and challenges such as the Digital Omnibus, an integrated approach for standards adoption, unified governance frameworks, and collaborative strategies that sustain high standards of trust and security while enabling technological advancement in the EU digital market. Overall, this paper is structured around the following research questions:

- RQ1. What are the potential overlaps and inconsistencies across major EU regulations, act and standards?
- RQ2. What are operational and governance challenges to achieve the coherent compliance?
- RQ3. What are the risks and barriers to effective implementation?
- RQ4. What are the potential solutions and harmonization strategies that can improve regulatory alignment without compromising regulatory intent?

The remainder of this paper is organized as follows: Section 2 provides an overview of key EU digital regulations and international standards; Section 3 analyzes the risk and challenges associated with the regulatory landscape. Section 4 presents opportunities and solutions for coherent compliance. Section 5 concludes with limitations and future research work.

2. Overview of Key EU Digital Regulations and International Standards

The overview and analysis presented in this paper are based on a desk-based review of key EU digital regulations and acts, relevant international standards, selected reports and literature.

2.1. *EU Digital Regulations*

2.1.1. *EU AI Act*

The EU AI Act (EU Parliament & Council, 2024a) establishes the world's first comprehensive legal framework for artificial intelligence, regulating AI systems based on risk levels from prohibited to minimal risk. The regulation addresses risks including fundamental rights violations, discriminatory decision-making, safety hazards from high-risk AI systems, and lack of transparency in AI-generated content.

2.1.2. *NIS2 Directive*

NIS2 (EU Parliament & Council, 2022a) mandates cybersecurity measures for essential and important entities across 18 critical sectors to strengthen EU-wide cyber resilience. The directive addresses risks including cyberattacks on critical infrastructure, supply chain vulnerabilities, inadequate incident response capabilities, and operational disruptions from security breaches.

2.1.3. *MDR/IVDR*

The Medical Device Regulation (EU Parliament & Council, 2017) (MDR) and In Vitro Diagnostic Regulation(European Parliament and Council of the European Union, 2017) (IVDR) establish stringent safety and performance requirements for medical devices and diagnostic tests marketed in the EU. These regulations address risks of unsafe or ineffective medical products, insufficient clinical evidence, inadequate post-market surveillance, and supply chain transparency failures.

2.1.4. *Cybersecurity Act*

The EU Cybersecurity Act (EU Parliament & Council, 2019) established ENISA's permanent mandate and created a voluntary EU-wide cybersecurity certification framework for ICT products,

services, and processes. The regulation addresses risks of insecure ICT products, inconsistent security evaluation across Member States, lack of consumer trust in digital products, and inadequate cybersecurity baseline standards.

2.1.5. *Data Act*

The Data Act (EU Parliament & Council, 2023) creates harmonized rules enabling users to access and share data generated by connected products and IoT devices across all sectors. The regulation addresses risks of data lock-in by manufacturers, unfair B2B data sharing terms, inability to switch cloud providers, and inadequate access to data for innovation and public interest purposes.

2.1.6. *Data Governance Act (DGA)*

The Data Governance Act (EU Parliament & Council, 2022b) establishes governance mechanisms for public sector data re-use, data intermediation services, and data altruism to facilitate trusted data sharing. This addresses risks of unfair access to public sector data, untrusted data intermediaries, insufficient safeguards for sensitive data sharing, and lack of infrastructure for voluntary data sharing.

2.1.7. *GDPR*

The General Data Protection Regulation (EU Parliament & Council, 2016) establishes comprehensive rules for processing personal data of EU individuals, creating fundamental data protection rights and controller obligations. GDPR addresses risks including unauthorized data processing, privacy violations, data breaches exposing personal information, inadequate security measures, and lack of individual control over personal data.

2.1.8. *The EU's Cyber Resilience Act*

The Cyber Resilience Act (EU Parliament & Council, 2024b) establishes mandatory cybersecurity requirements for all products with digital elements, from consumer electronics to industrial systems, ensuring products are secure throughout their lifecycle. The regulation addresses risks of insecure connected products, unpatched vulnerabilities, lack of security updates, inadequate vulnerability disclosure processes, and cybersecurity incidents from compromised products.

2.2. *International Standards*

2.2.1. *ISO/IEC 27001*

(ISO/IEC, 2022) is an international standard specifying requirements for establishing, implementing, and maintaining an Information Security Management System (ISMS) to protect organizational information assets. The standard addresses risks including unauthorized access to information, data breaches, loss of data integrity and availability, inadequate security controls, and failure to demonstrate security compliance. The latest version (ISO/IEC 27001:2022) was published October 2022, with organizations having until October 31, 2025, to transition from the 2013 version.

2.2.2. *ISO/IEC 42001*

(ISO/IEC, 2023) is the world's first international standard for AI management systems, providing a framework for responsible development, deployment, and use of artificial intelligence. The standard addresses risks including AI bias and discrimination, lack of AI transparency and explainability, inadequate AI risk management, absence of AI governance structures, and ethical concerns in AI deployment. The standard was published December 2023, with accredited certification available from September 2024.

2.2.3. *IEC 62443*

(IEC, 2009) is a comprehensive series of standards addressing cybersecurity for industrial automation and control systems (IACS) across all industrial sectors. The standard addresses risks including cyberattacks on operational technology, industrial process disruptions, safety incidents from compromised control systems, inadequate security in legacy industrial equipment, and supply chain vulnerabilities in industrial components.

3. Risk and Challenges Associated with the Regulatory Landscape Operational Challenges

The emerging EU regulatory landscape can create substantial operational challenges for organiza-

tions particularly in critical sectors. Some of these challenges include

3.1. *Non-Compliance Risk*

The EU regulatory landscape for AI, cybersecurity, data governance, and related areas comes with different levels of risk due to non-compliance. Such risks includes the cyber threats, fundamental rights violations, data misuse, and insecure products for organizations. EU also poses substantial financial penalties for non-compliance under mandatory frameworks. Table 1 provides a summary of the main non-compliance risks and associated penalties (where applicable).

3.2. *Innovation and Competitiveness Hindrance*

The extensive and fragmented EU digital regulatory framework including the AI Act, NIS2, CRA, GDPR, Data Act, and others has also been criticized for hindering innovation and eroding EU competitiveness (Pelkmans and Renda, 2014). For example, the 2024 Draghi Report (Draghi, 2024) on the Future of European Competitiveness explicitly pointed out the administrative burdens, regulatory fragmentation, and obstacle to scaling innovation, particularly in digital and AI sectors. This is being discussed as one of the key reasons why the EU lags behind the U.S. and China. Moreover, high compliance costs, duplicative obligations, and legal uncertainty contribites to slow AI adoption, delay product launches, and deter investment.

3.3. *Overlapping Obligations*

Many organizations have obligations to comply with multiple frameworks simultaneously that leads to duplicated or conflicting requirements (Graux et al., 2025; Gonçalves, Gonçalves). For example, AI systems classified as high-risk under the EU AI Act often requires cybersecurity mandates in the NIS2 Directive for essential/important entities and the Cyber Resilience Act (CRA) for products with digital elements.

3.4. *Administrative Burden*

The cumulative impact of these regulations imposes significant administrative loads on the organizations, including separate risk assessments, documentation, audits, and reporting channels (BusinessEurope, 2025a). This burden can be significant specially for SMEs, which lack resources to maintain parallel compliance programs. This can be also challenging for global firms navigating EU-specific rules alongside other jurisdictions (van der Horst et al., 2017).

3.5. *Inconsistencies*

Variations in definitions, thresholds, and enforcement create legal uncertainty (BusinessEurope, 2025a; Tridimas, 2019) . Key examples include differing approaches to data processing for AI training (GDPR restrictions vs. Data Act access rights) and incident severity classifications. IT/OT conflicts persist, such as patching requirements clashing with operational uptime needs in industrial systems governed by IEC 62443 alongside NIS2 or CRA.

3.6. *Supply Chain and Implementation Issues*

Supply chain transparency and third-party risk management are one of the most important requirements across these regulations and standards (Felbermayr et al., 2025; Parlov, Akrap, and Esterhajer, Parlov et al.). However, fragmented oversight often leaves gaps, with risks undetected until a crisis emerges. The implementation of these requirements are also challenges such as legacy system upgrades, and coordination across IT, OT, legal, and compliance teams.

The key operational and governance challenges include overlapping and inconsistent regulatory obligations, fragmented governance structures, and increased administrative and coordination burdens across different technologies. The main risks and barriers to implementation are increased exposure to non-compliance, legal uncertainty, high compliance costs that can hinder innovation, and supply chain-related vulnerabilities under fragmented regulatory oversight.

4. Opportunities and Potential Solutions for Coherent Compliance

The fragmented EU digital regulatory landscape provides protection of rights, security, and trust,

Table 1.: Overview of non-compliance risks and penalties across key EU regulations and international standards

Regulation / Standard	**Fines or Penalties**	**Key Organizational Risks**
EU AI Act	Up to €35M or 7% of global turnover for prohibited practices; €15M or 3% for provider obligations; €7.5M or 1% for information violations (whichever is higher, but whichever is lower for SMEs/startups).	Fundamental rights violations; discriminatory decision-making; safety hazards from high-risk AI systems; lack of transparency in AI-generated content.
NIS2 Directive	At least €10M or 2% of global turnover (essential entities); €7M or 1.4% (important entities). Member States may set higher maximums.	Cyberattacks on critical infrastructure; supply chain vulnerabilities; weak incident response; operational disruptions.
MDR / IVDR	Penalties determined by Member States (no harmonized EU fines); must be effective, proportionate, and dissuasive.	Unsafe or ineffective medical products; insufficient clinical evidence; weak post-market surveillance; supply chain transparency failures.
EU Cybersecurity Act	No EU-harmonized penalty amounts; Member States must establish national penalties for certification framework violations (Article 65).	Deployment of insecure ICT products; inconsistent evaluation across Member States; loss of consumer trust; lack of cybersecurity baseline standards.
Data Act	Penalties at Member State discretion for general violations. However, GDPR fines apply (up to €20M or 4% of global turnover) for personal-data-related violations of data access, third-party sharing, and B2G sharing provisions (Article 40(4))	Data lock-in by manufacturers; unfair B2B data sharing terms; barriers to cloud provider switching; insufficient access to data for innovation or public interest.
Data Governance Act	Enforcement handled by Member States; no specified fines.	Unfair access to public sector data; misuse by untrusted intermediaries; weak safeguards for sensitive data; lack of infrastructure for voluntary data sharing.
GDPR	Up to €20M or 4% of global turnover (serious breaches); €10M or 2% for other failures (whichever is higher; calculated at group level).	Unauthorized data processing; privacy violations; data breaches; inadequate security controls; loss of individual data control.
Cyber Resilience Act (CRA)	€15M or 2.5% for essential requirement breaches; €10M or 2% for other violations; €5M or 1% for false information (whichever is higher; open-source stewards fully exempt).	Insecure connected products; unpatched vulnerabilities; missing security updates; poor vulnerability disclosure processes.
ISO/IEC 27001	No legal fines; loss or denial of certification.	Unauthorized access to information; data breaches; loss of data integrity or availability; inadequate controls; inability to demonstrate compliance.
ISO/IEC 42001	No legal fines; loss of AI management certification.	AI bias and discrimination; lack of transparency; poor AI risk management; absence of AI governance; ethical deployment concerns.
IEC 62443	No legal fines; voluntary best-practice framework.	Cyberattacks on operational technology; industrial process disruptions; safety incidents from compromised systems; supply chain vulnerabilities.

however it imposes substantial compliance costs and operational friction. Despite these challenges, there are several opportunities and solutions to streamline compliance, foster innovation, and build more resilient digital ecosystems. Recent developments, including the European Commission's Digital Omnibus proposal (European Commission, 2025), signal a shift toward greater harmonization. Some of the opportunities and solutions are as follows:

4.1. *Harmonization Initiatives*

The Europen commision launched Digital Omnibus (European Commission, 2025) which is a comprehensive EU regulatory proposal to streamline and rationalize the EU's digital legal framework to reduce complexity and lower compliance costs for businesses while keeping core protections intact. For example, Digital Omnibus include a set of technical amendments to multiple existing digital laws (such as the GDPR, ePrivacy Directive, Data Act, NIS2 and other cybersecurity rules) to clarify, consolidate and simplify obligations across overlapping legislation and modifications proposed for the EU AI Act to facilitate smoother, proportionate implementation of high-risk AI obligations and adjust practical compliance timelines.

4.2. *Integrated Compliance Frameworks*

One of the solutions for the organizations is to adopt the unified governance models including multiple regulation and standards, such as combining ISO/IEC 27001 (ISMS), ISO/IEC 42001 (AI management systems), and sector-specific controls (e.g., IEC 62443 for OT) (Chellappan,

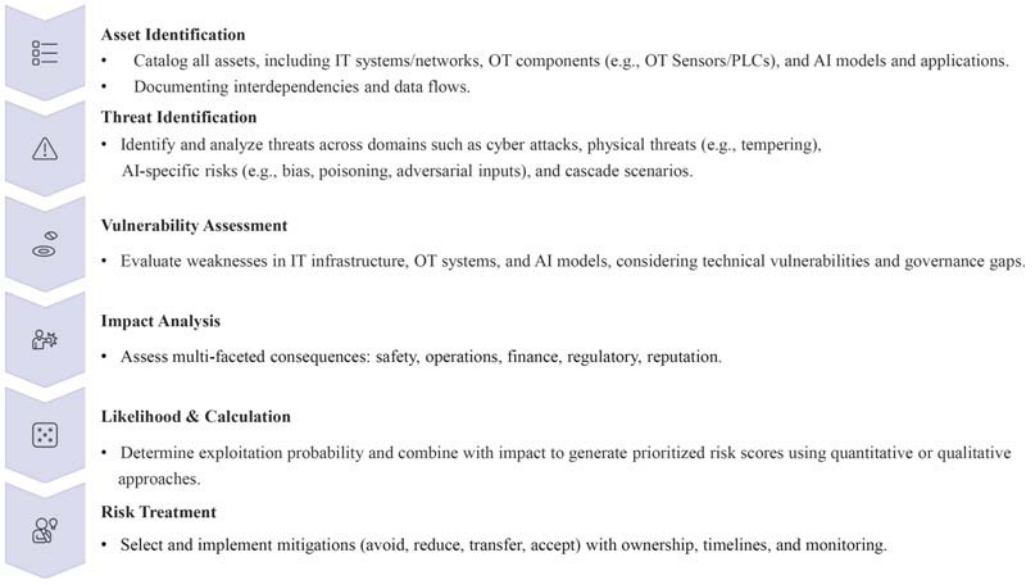

Fig. 1.: Unified risk assessment methodology

Chellappan; ISA Global Cybersecurity Alliance (ISAGCA), 2025). Mapping requirements and controls across these regulations and standards and demonstrating compliance via a common risk register can help to minimize duplication efforts and provide a better overview of the risks. Automated monitoring and AI-driven compliance platforms can hep to enable real-time oversight and evidence collection.

4.3. *Leveraging Standards and Certification*

Harmonized standards can be a practical solution to demonstrate the compliance (Sankaran, 2025). For example, ISO/IEC 42001 supports AI Act governance, while ISO/IEC 27001 certifications aids NIS2 and CRA cybersecurity baselines. In addition, regulatory sandboxes and pilot initiatives can be used by organizations to test integrated governance and compliance models with reduced regulatory risk. For organizations: implement a single cross-regulatory risk register aligned to ISO/IEC 27001 and 42001.

4.4. *Strategic and Collaborative Approaches*

Proactive compliance strategies such as building cross-functional teams (e.g., IT, OT, legal, AI ethics) for unified risk management and fostering dialogue with regulators through industry associations. On the other hand, policymakers can further support coherence by clearifying lex specialis rules and harmonized definitions Graux et al. (2025); BusinessEurope (2025b).

Here, we have given an example of the proposed unified risk assessment method (shown in Figure 1) considering IT, OT, and AI domains. The development of a unified framework for risk assessment that integrates IT, OT, and AI domains. We should consider established guidelines and standards such as the NIST AI Risk Management Framework (AI RMF), which emphasizes mapping, measuring, and managing AI-specific risks, ISO/IEC 42001, ISO/IEC 23894:2023, ISO/IEC 27001, and IEC 62443. This framework is built on traditional risk management processes (e.g., NIST SP 800-30, ISO 31000) and can help to ensure interoperability, incorporating cross-domain

interdependencies, and address threats that span digital, physical, and intelligent systems.

5. Conclusion, Limitations and Future Research Work

The EU's digital regulatory frameworks as well as international standards represents a landmark effort to build a secure, ethical, and trustworthy digital single market. These regulations, act and standards collectively help organiztions to mitigate critical risks to fundamental rights, cybersecurity, data sovereignty, and consumer safety amid rapid technological advancement. However, increasing number of regulatory frameworks and standards and their parallel development has resulted in a fragmented landscape characterized by overlapping obligations, duplicative assessments, inconsistent definitions and enforcement, heightened administrative burdens, and operational complexities. These issues create several risks and challenges such as non-compliance risks with substantial penalities, strain resources, hinder innovation through legal uncertainty and compliance fatigue, and potentially undermine the EU's global competitiveness goals.

However, several initiative have been taken to overcome this for example the Digital Omnibus package that offer promising pathways forward. Other potential solutions can be adopting the unified approach such as unified risk management, incident reporting, timeline adjustments, targeted simplifications, and greater coherence across data, AI, and cybersecurity rules, these efforts aim to reduce fragmentation while preserving high standards of protection. On the other hand, organizations can also adopt strategies such as integrated standards adoption, unified governance models, cross-regulatory mapping, and technology-enabled compliance that can help them to transform challenges into efficiencies. Overall, the paper addresses RQ1 by identifying overlaps and inconsistencies in EU digital regulations, RQ2 and RQ3 by clarifying the main operational challenges and implementation risks, and RQ4 by outlining potential harmonization and integrated compliance strategies.

This paper has several limitations for example the EU regulatory landscape are changing and new rules, guidance, and interpretations are continuing to evolve. Enforcement and application still vary significantly across Member States due to differences in transposition, national priorities, and supervisory practices. Sector-specific experiences also differ considerably between different sectors such as healthcare, finance, transportation or general commercial contexts that limits the universality of the findings. Future research will focus on real-world compliance implementation, cost and outcome analysis over time, and comparative assessment of enforcement practices across Member States, including sector-specific studies in critical infrastructure.

References

Andraško, J., M. Mesarčík, and O. Hamul'ák (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the eu legal framework. *AI & society 36*(2), 623–636.

BusinessEurope (2025a, January). Mapping of regulatory burden. D55.1.

BusinessEurope (2025b, July). Simplification of the digital rulebook. BusinessEurope Policy Paper.

Chellappan, R. B. Responsible innovation in artificial intelligence: A unified risk management approach integrating nist, iso 42001, and the eu ai act.

Draghi, M. (2024). The future of european competitiveness part a: A competitiveness strategy for europe.

EU Parliament & Council (2016, April). Regulation (eu) 2016/679. Entry into force: 24 May 2016; Date of application: 25 May 2018. Corrigendum: OJ L 127, 23.5.2018, p. 2.

EU Parliament & Council (2017, April). Regulation (eu) 2017/745. Entry into force: 25 May 2017; Date of application: 26 May 2021.

EU Parliament & Council (2019, April). Regulation (eu) 2019/881. Entry into force: 27 June 2019.

EU Parliament & Council (2022a, December). Directive (eu) 2022/2555. Entry into force: 16 January 2023; Transposition deadline: 17

October 2024.

EU Parliament & Council (2022b, May). Regulation (eu) 2022/868. Entry into force: 23 June 2022; Date of application: 24 September 2023.

EU Parliament & Council (2023, December). Regulation (eu) 2023/2854. Entry into force: 11 January 2024.

EU Parliament & Council (2024a). Regulation (eu) 2024/1689. Entered into force: 1 Aug. 2024.

EU Parliament & Council (2024b, October). Regulation (eu) 2024/2847. Published: 20 November 2024; Entry into force: 10 December 2024; Full application: 11 December 2027.

European Commission (2025). Digital omnibus proposal.

European Parliament and Council of the European Union (2017). Regulation (EU) 2017/746. Text with EEA relevance.

Felbermayr, G., K. Friesenbichler, M. Gerschberger, B. Meyer, and P. Klimek (2025). Eu supply chain regulations between efficiency and effectiveness. *Intereconomics 60*(3), 165–169.

Gonçalves, A. Regulatory convergence and divergence: A study on the synergies and conflicts among key cybersecurity european legislation.

Graux, H., K. Garstka, N. Murali, J. CAVE, and M. BOTTERMAN (2025). Interplay between the ai act and the eu digital legislative framework. Technical report, Technical Report. Policy Department for Transformation, Innovation and ....

Grima, S., J. Spiteri, and I. Romanova (2019). The challenges for regulation and control in an environment of rapid technological innovations. In *InsurTech: a legal and regulatory view*, pp. 83–98. Springer.

IEC (2009). Industrial communication networks – network and system security. Standard Series IEC 62443, International Electrotechnical Commission.

Irbe, I. (2024). European union regulatory complexity: Challenges and solutions for entrepreneurs. *Available at SSRN 4859007*.

ISA Global Cybersecurity Alliance (ISAGCA) (2025). Applying iso/iec 27001/2 and the isa/iec 62443 series: White paper. White Paper.

ISO/IEC (2022). Information security, cybersecurity and privacy protection – information security management systems – requirements. Standard ISO/IEC 27001:2022, International Organization for Standardization.

ISO/IEC (2023). Information technology – artificial intelligence – management system. Standard ISO/IEC 42001:2023, International Organization for Standardization.

Jørgensen, B. N. and Z. G. Ma (2025). Impact of eu regulations on ai adoption in smart city solutions: A review of regulatory barriers, technological challenges, and societal benefits. *Information 16*(7), 568.

Mariniello, M. (2022). *Digital economic policy: The economics of digital markets from a European Union perspective*. Oxford Uni. Press.

OECD (2021). Case studies on the regulatory challenges raised by innovation and the regulatory responses. Technical report. Accessed: 2026-02-06.

Parlov, N., G. Akrap, and J. Esterhajer. Supply chain security and ai risk governance model for critical infrastructure under nis2, cer, and cra. *Applied Cybersecurity & Internet Governance*.

Pelkmans, J. and A. Renda (2014). Does eu regulation hinder or stimulate innovation?

Sankaran, S. (2025). Enhancing trust through standards: A comparative risk-impact framework for aligning iso ai standards with global ethical and regulatory contexts. *arXiv preprint arXiv:2504.16139*.

Tridimas, P. T. (2019). Indeterminacy and legal uncertainty in eu law. *Takis Tridimas, Indeterminacy and legal uncertainty in EU law in Joana Mendes (Ed), EU Executive Discretion and the Limits of the Law, OUP*.

van der Horst, R., A. Nijsen, and S. Gulhan (2017). Regulatory policies and their impact on smes in europe: The case of administrative burdens. *The Blackwell Handbook of Entrepreneurship*, 128–149.