Scaling Europe's Regulatory Superpower: From Static Cybersecurity Standards to Semantic Graphs

by Dinis Cruz and ChatGPT Deep Research, 2025/03/31

Introduction

Europe has established itself as a **global regulatory superpower** in the digital realm, exporting its standards and norms well beyond its borders. Landmark frameworks like the GDPR have set **worldwide benchmarks** for data protection, a phenomenon often dubbed the "Brussels effect," where the EU's large single market forces multinational companies to adopt European rules globally.

Now, as Europe rolls out new cybersecurity policies – from network security (NIS2 Directive) to product security (Cyber Resilience Act) to AI governance (EU AI Act) – the challenge is **scaling this regulatory prowess**. Scaling isn't just about enacting more laws; it's about ensuring they can be **implemented, monitored, and updated** effectively in a rapidly evolving threat landscape.

Currently, even Europe's most forward-thinking regulations and standards are published as lengthy PDFs, websites, or spreadsheets – essentially **flat text** documents. Organizations must interpret these static texts and manually map requirements onto their internal controls and processes. This approach is proving **unsustainable**: it's labor-intensive, error-prone, and ill-suited to the **complex, overlapping** nature of modern cybersecurity obligations.

To truly harness its regulatory superpower, Europe needs to transform how regulations are consumed and applied. This white paper argues that the next evolution is to move from static documentation to **semantic, graph-based representations** of cybersecurity standards – a shift that can make Europe's regulations more **granular, context-aware, and machine-consumable** at scale.

We begin by examining Europe's current cybersecurity regulatory landscape and its limitations. We then explore the tension between **regulatory simplicity and implementation detail**, highlighting the need for customization of requirements in context. Next, we introduce semantic knowledge graphs and ontologies as a paradigm to represent regulations in a structured, queryable form.

We discuss practical approaches to building and maintaining regulatory knowledge graphs, and how they enable **granular tailoring** of standards for specific departments, teams, or sectors.

Finally, we consider the broader implications: how **machine-readable standards** can streamline compliance, enhance transparency (especially in third-party risk management), and even **incentivize a market** that rewards security and responsible behavior.

Europe's Cybersecurity Regulatory Landscape: Strengths and Limitations

Europe's strength in cybersecurity lies not in tech giants or defense might, but in its **comprehensive regulatory frameworks**. Over the past decade, the EU and European bodies have produced a suite of laws and standards aiming to bolster cybersecurity and privacy across industries. Some of the prominent ones include:

- **GDPR (General Data Protection Regulation)** – Effective 2018, GDPR is a sweeping data protection law governing personal data handling. It imposes strict requirements (e.g. lawful processing, breach notification, data subject rights) and hefty fines (up to 4% of global revenue) for non-compliance. GDPR's **global influence** is evident – it inspired similar privacy laws worldwide. *Format:* ~88 pages of legal text (PDF); supplementary guidelines from the European Data Protection Board (PDFs). *Customization:* One-size-fits-all rules (although applied proportional to context in practice); organizations must interpret how each article applies to them.
- **NIS2 Directive (Directive (EU) 2022/2555)** – Adopted in 2022, NIS2 updates Europe's network and information security requirements for "essential" and "important" entities across critical sectors (energy, transport, health, finance, etc.). It mandates risk management measures and **incident reporting** to authorities within tight timelines. NIS2 significantly broadens scope (covering medium/large companies in many sectors) and harmonizes security requirements across the EU. *Format:* a directive text with chapters and articles (official PDF) that Member States transpose into national laws. *Overlap:* There are **overlapping obligations** (e.g. incident reporting) with other laws like GDPR and the upcoming

Cyber Resilience Act, which can confuse companies. *Customization:* Some scaling by company size (small orgs are exempted), but within scope, all must meet the same provisions.

- **Cyber Resilience Act (CRA)** – A proposed EU regulation focused on cybersecurity of digital products (software and hardware). It will require manufacturers to ensure products meet certain security requirements and handle vulnerabilities properly throughout the product lifecycle. *Format:* Draft regulation text (PDF); will be directly applicable when in force. *Customization:* Risk-based (e.g. critical products have stricter requirements), but presented as uniform text.
- **DORA (Digital Operational Resilience Act)** – An EU regulation for the financial sector (banks, fintech, insurance) to ensure they can withstand ICT-related disruptions. It demands ICT risk management, reporting of incidents, and oversight of ICT third-party providers. *Overlap:* Aligns with some NIS2 and GDPR principles, but targets financial entities specifically. Financial entities now juggle DORA alongside existing standards (like PCI DSS for payments or ISO 27001 for general security).
- **EU AI Act** – Ambitious upcoming AI regulation creating a tiered risk system for AI systems (banned practices, high-risk systems with strict obligations, etc.). Will be the world's most comprehensive AI law and is expected to be finalized soon. It **delegates technical implementation details to harmonized standards** rather than hard-coding them in the law. For example, providers of high-risk AI must implement risk management, data governance, transparency, etc., but the "how" is deferred to standards by European Standardization Organizations (CEN/CENELEC, ETSI). *Format:* Legal text (multi-chapter regulation); additional standards (likely ISO/IEC) will serve as supporting detail. *Customization:* Risk-based approach, but within "high-risk," detailed requirements are uniform (and complex).
- **ISO 27000 Series** – International standards (widely adopted in Europe) for information security management (ISO 27001 for ISMS, ISO 27002 for security controls, etc.). These are **industry standards** rather than laws, often used to comply with or demonstrate compliance with legal obligations (for instance, implementing ISO 27001 can help meet NIS2 or GDPR security requirements). *Format:* Formal standards documents (available as PDFs for purchase). *Customization:* Intended to be adaptable – organizations choose which controls apply and how – but the standard itself is static text. Researchers have even explored formalizing ISO 27002 controls semantically; one effort created a **semantic decision support system** by formalizing ISO 27002 control descriptions.
- **PCI DSS (Payment Card Industry Data Security Standard)** – A global industry standard (mandated by card networks) for protecting cardholder data, relevant to any European business processing payments. PCI DSS is very prescriptive (12 requirement sections with numerous sub-requirements). *Format:* PDF document (and supplemental spreadsheets) updated periodically. *Overlap:* If an organization deals with payments and personal data, PCI DSS and GDPR both apply, each with separate documentation. Compliance efforts can be siloed, since GDPR is law and

PCI DSS is contractual, but both demand strong security. *Customization:* All entities handling card data must implement all applicable controls, though smaller merchants have some scope reduction – again, defined in text form.

- **OWASP ASVS (Application Security Verification Standard)** – A community-driven standard providing a **checklist of application security requirements** at different verification levels. Although not an EU regulation, it's widely used in Europe as a best-practice for secure software development. Significantly, OWASP ASVS has started providing its requirements in **machine-readable formats (CSV, JSON, etc.)** for programmatic use. This is a noteworthy example of a traditionally PDF-based standard evolving to support automation. (For instance, a development team can pull ASVS JSON data to automatically generate security test cases or checklists).

Limitations of the Status Quo: Europe's comprehensive standards have undoubted benefits – they establish clear baseline expectations and drive security investments. However, delivering these standards as long text documents (PDFs or websites) creates several pain points:

- **Human Effort and Error:** Regulations in pure text **"require significant human time and effort to ensure compliance"**, as found by researchers integrating GDPR and PCI DSS. Compliance officers must manually parse requirements, interpret them, and map them to the organization's own policies and systems. This is laborious and can lead to inconsistent interpretation. Small and mid-size enterprises (SMEs) are especially **overwhelmed**, as they have limited staff to read and track ever-changing policies.
- **Siloed & Overlapping Requirements:** Because each law or standard is a standalone document, organizations face overlaps and sometimes contradictions. For example, an incident affecting personal data might trigger GDPR breach notification to data protection authorities and also NIS2 reporting to cyber authorities. Each regime has different forms and timelines. "Companies in the EU are facing difficulties in understanding the complex, sometimes overlapping requirements" of various cybersecurity policies. Without a unified view, compliance efforts duplicate work or miss subtle differences. It's hard to "see the forest for the trees" in the *"forest of laws, regulations, standards,"* as one study put it.
- **Flat, Non-Contextual Documentation:** A static PDF treats all organizations and scenarios uniformly. In practice, a given requirement might not apply equally to all departments or systems, but the document doesn't adjust to context. There's **no easy way to customize or filter** the text for relevance. Every reader must mentally filter what applies to, say, their department or project. The result: lengthy internal checklists derived from the same source, duplicated and tailored in ad-hoc ways.
- **Lack of Granularity for Automation:** Text documents are not **machine-readable** in a useful way. While a human can read a control like "implement a vulnerability disclosure policy," a software tool cannot inherently understand this from a PDF. Organizations often resort to creating

spreadsheets of requirements as an intermediate form so they can track compliance status. Those spreadsheets are essentially a **bespoke, manual "database"** of the regulation. This manual translation step is inefficient and can introduce errors or omissions.

- **Slow to Update and Difficult to Version:** When a standard updates (e.g., ISO 27002 had a major update in 2022, PCI DSS in 2023), organizations must painstakingly do a **gap analysis** between old and new PDFs. There's no inherent version control or diff in the text – it's up to the reader or consultants to figure out what changed. This slows down adaptation to new rules. With cybersecurity threats evolving, regulators are updating requirements more frequently; static documents don't lend themselves to agile updates.

In summary, Europe's cybersecurity regulations and standards are **rich in substance but poor in format**. The static format limits their accessibility, **customizability**, and **machine integration**. This gap between Europe's *"regulatory superpower"* vision and on-the-ground implementation calls for a new approach. The next section examines one of the key challenges that any new approach must address: the balance between **simplified, principle-based rules** and the **need for implementation-level detail** that varies by context.

The Compliance Challenge: Balancing Simplicity with Detail

Regulators often walk a tightrope between making rules **simple and broadly applicable** versus providing the **detailed guidance** needed for real-world implementation. Europe's approach has generally been to legislate **principles and high-level requirements**, and leave specifics to be figured out by industry or supplemental standards. This avoids tying laws to particular technologies (which might become obsolete) and gives flexibility. However, it also pushes the complexity onto those implementing the rules, who must interpret how to meet these broad mandates in practice.

For example, the EU's AI Act consciously separates concerns: it **provides broad obligations** (e.g. "ensure high-risk AI systems are transparent and subject to human oversight") but **defers the exact methodology to technical standards**. As noted, the Act's authors didn't include the *Trustworthy AI Guidelines* (which are principle-based) in the law itself, recognizing that those guidelines are high-level. Instead, **"detailed rulemaking on implementing the Act…[is] delegated to technical standards"** to be developed by European and international standards organizations. The intent is to let experts define the nitty-gritty and to allow those technical norms to evolve more easily than legislation.

The downside: companies now have to **navigate multiple documents** – the law *and* a host of standards – to know what to do. In the AI Act case, a provider of a high-risk AI system might need to consult a forthcoming CEN/CENELEC standard on AI risk management, an ISO/IEC standard like ISO

42001 (AI management system) or ISO 23894 (AI risk management guidance), etc., all *"interrelated standards, many of which are still under development"*. As a recent analysis put it, *"one of the key challenges for high-risk AI providers is navigating a sea of standards… The lack of common terminology and detailed mapping of requirements adds to the complexity"*. In other words, principle-based regulation can lead to an **implementation puzzle**, where the pieces are in different places and use different language.

We see this pattern in cybersecurity broadly: **laws vs. frameworks vs. controls.** A law (like NIS2 or GDPR) states *"what"* outcomes must be achieved (e.g. protect personal data with appropriate security, ensure network resilience, report incidents, etc.), often without stating *"how."* The *"how"* is found in frameworks like ISO 27002 (which lists security controls) or industry best practices (like OWASP ASVS for secure coding). Organizations then write internal policies or procedures translating those controls to their environment. Each layer – law, standard, internal policy – is typically a **separate static document**, and aligning them is non-trivial. Misalignment can occur; for instance, a company's policy might meet ISO 27002 control guidance but still fall short of a stricter legal requirement, or vice versa, simply due to interpretation gaps.

Over- and Under-Shooting: Another challenge is that broad regulations can be **overly generic** for some contexts and not specific enough for others. A small SaaS startup and a multinational bank both must follow GDPR's mandate for "appropriate technical and organizational measures" for security – but what is appropriate differs vastly. The flat text doesn't tell you that nuance; it's up to each to decide (often by consulting further guidance). Conversely, a very detailed standard (like PCI DSS, which specifies technical settings down to password complexity rules) can be **too prescriptive** in ways that might not fit an unconventional IT environment, yet must be followed to the letter for compliance. Balancing these extremes is difficult when using static documents; regulators tend to err on the side of generality in laws and leave detail to secondary material.

Contextual Relevance: In practice, compliance teams **filter and tailor** requirements to different internal contexts. For example: an enterprise may categorize its business units by risk profile – say, one unit handles only public data, another handles sensitive personal data. The security controls and regulatory obligations differ accordingly. Yet GDPR or ISO 27002 will list *all* possible requirements. It's left to practitioners to mark "not applicable" where needed, or to create separate checklists for each department. This manual contextualization is effortful and can become outdated if the context changes (e.g. a department starts a new high-risk project but their compliance checklist wasn't updated).

What's needed is a way to preserve the **simplicity of universal principles** (so the rules remain understandable and technology-neutral) while enabling **implementation-level detail and filtering** to make them relevant in each context. Essentially, a multi-layered model where the *core requirements* are linked to *detailed controls* and *contextual information* about applicability.

Static documents struggle to achieve this balance because they present one linear narrative. A promising solution is to introduce **structure and semantics** into how regulations are represented. By structuring regulatory knowledge in a machine-readable graph with semantic links, we can embed context and layers of detail in a single, navigable model. The next section introduces this concept – representing regulations and standards as **semantic knowledge graphs** – and how it addresses the challenges of complexity and customization without sacrificing the clarity of high-level rules.

Semantic Knowledge Graphs: A New Paradigm for Cybersecurity Standards

Instead of publishing cybersecurity standards as prose and checklists, imagine representing them as an **interactive map of knowledge**. In this map, each rule or control is a node, and relationships link these nodes to other concepts: to broader principles, to specific technical measures, to responsible roles, even to related requirements in other regulations. This is the essence of a **semantic knowledge graph** approach. Using technologies from the Semantic Web (like RDF – Resource Description Framework, and OWL – Web Ontology Language), we can encode regulatory content in a way that is **both human-readable and machine-processable**.

At its core, a knowledge graph is a set of **triples**: subject–predicate–object statements that form a network. For example, a fragment of a compliance graph might say:

- `Article 32 GDPR` – *requires* – `Encryption of Personal Data`;
- `Encryption of Personal Data` – *is a* – `Security Control`;
- `Encryption of Personal Data` – *mitigates* – `Confidentiality Risk`.

Here, “Article 32 GDPR” and “Encryption of Personal Data” are nodes, and “requires” is a semantic relationship. In a graph, one can then attach more detail: **Article 32** (on security of processing) could be linked to multiple specific controls (encryption, access control, etc.), each of which might link to industry standards or guidelines (say, ISO 27002 control 10.1 on cryptography). The graph can also capture **context** – e.g., attach a condition that “Encryption of Personal Data” is relevant *if* sensitive personal data is processed.

This contrasts with a PDF that might say *“Appropriate technical and organizational measures, such as encryption…”* in a paragraph. In the PDF, the onus is on the reader to interpret that encryption is required in certain scenarios. In the graph, **encryption** becomes a first-class object that can be queried, related, and tagged (e.g. marked as “technical measure” with certain scope).

Benefits of a Semantic Graph-based Approach:

- **Machine Readability and Automation:** By converting "laws as text" into **data with meaning**, we enable software to work with compliance requirements directly. A knowledge graph of regulations can be loaded into compliance management tools, rule engines, or AI systems. For instance, an automated tool could query the graph: "What are all the obligations applicable to a data processor handling financial information?" and get a precise list of requirements spanning GDPR, NIS2, etc., something that would take a human hours of cross-referencing. ClauseMatch, a RegTech firm, demonstrated this by training AI models on regulatory text and generating a **queryable knowledge graph of regulatory requirements**. In their prototype with the Abu Dhabi Global Market regulator, clicking on a node in the graph brings up the exact paragraph of the regulation on that topic. This shows how a graph allows *"within seconds"* what used to require carefully skimming a document's table of contents or index.
- **Transformation into Machine-Readable Format:** Knowledge graphs are *"an essential mechanism to transform regulation into a machine-readable format"*. Unlike a static document, which software sees as just a blob of text, a graph has **structured nodes and relationships** that a computer can traverse. This is foundational for what some call *"Regulation 2.0"* or even *"Regulation-as-a-Service"*, where up-to-date requirements can be served via APIs or data feeds rather than PDF downloads.
- **Deeper Insight and Querying:** A graph format can reveal **relationships and patterns** not obvious in linear text. As ClauseMatch noted, graph representations *"enable us to infer new relationships, gain a deeper understanding and realize patterns within the regulation that we would not have spotted otherwise"*. For example, one could query for all requirements across different laws pertaining to "incident response" and discover overlaps or gaps. In a static approach, one might miss that connection unless actively searching each document. Researchers building a GDPR knowledge graph similarly found that a semantically rich model helps identify *"potential contradictory policies"* within an organization's compliance documentation, so they can be rectified.
- **Continuous Compliance and Automated Reasoning:** Perhaps the biggest advantage is enabling **automated compliance checking and monitoring**. When rules are in a formalized, computable form, you can build rule-checking systems that reason over them. A knowledge graph can integrate with real-time data – for instance, ingest signals about security controls status and automatically flag non-compliance. In the academic effort *NIS2Onto*, which created an ontology for the EU NIS2 Directive, the authors highlight that this approach *"reduces time and effort required for verification by enabling continuous monitoring of any modification… and minimizing the risk of human error"*. With machine reasoning, *"automatic*

compliance verification makes the audit process fast, easy, and detailed", helping companies prove to regulators that they meet requirements. In other words, compliance moves from a periodic, manual audit to an **ongoing, automated process** – a huge leap in efficiency.

- **Version Control and Evolution:** A semantic model can be designed to handle versions, much like software code. Each requirement node can carry a version tag or effective date. Updates to regulations can be incorporated as new nodes/relationships while keeping the old ones (for historical traceability or comparison). This **version-controlled approach** means that when "GDPR 2.0" or a NIS3 directive comes out, the changes can be layered onto the graph and instantly reflected in queries and compliance checks. Compare this to the current situation of reading "GDPR recitals and amendments" and manually reconciling changes. The knowledge graph can even encode **temporal logic** – e.g., an obligation is only in force after a certain date, etc., allowing systems to automatically switch to new requirements when they kick in.
- **Integration of Multiple Standards:** Because knowledge graphs are inherently about linking data, they are ideal for bridging across different frameworks. A single graph can include nodes from GDPR, PCI DSS, ISO 27001, OWASP ASVS, etc. If two standards address the same concept (say "access control"), the graph can link them to a common concept node. The University of Maryland's researchers who built an integrated GDPR + PCI DSS ontology did exactly this: they *"identified the obligations defined in these regulations and related them with corresponding Cloud Security Alliance (CSA) controls."*. The result was a unified knowledge base where one can check compliance against both GDPR and PCI simultaneously. For example, a control like *"Maintain an access control policy"* might satisfy a PCI DSS requirement and also map to GDPR's requirement for restricting data access – the graph would capture that one control covers both. This cross-standard mapping is immensely valuable to reduce duplication in compliance efforts.
- **Inherent Customizability:** We will expand on this later, but it bears noting that when regulations are in a graph format, **custom views** or extra layers can be built on top easily. Because the data is **granular (down to each requirement or clause)**, one can assemble subsets relevant to a context without rewriting content. It's analogous to how a database can be queried to produce different reports from the same data. A graph can be queried to produce a tailored *"compliance checklist"* for a particular team or a specific regulation scope. This is something flat documents cannot do on their own.

Several **real-world and experimental efforts** illustrate the power of semantic regulation:

- *Case: ClauseMatch & ADGM.* In a pioneering 2024 pilot, the Abu Dhabi Global Market's Financial Services Regulatory Authority worked with ClauseMatch to convert its regulatory rulebook into a structured knowledge graph. They used an AI-driven approach: training NLP models on the regulation's taxonomy, **extracting entities and linking content at a granular paragraph level** based on themes. The outcome was a graph of

regulatory requirements – users could visually explore connections and instantly jump to relevant sections by clicking graph nodes. This allowed detecting overlapping obligations by simple queries. ClauseMatch described it as *"the first step before such graphs are created for internal documentation like policies, procedures, controls to map them with the requirements in a visualised dynamic form."* In effect, it lays the groundwork for an end-to-end mapped compliance system: external regs to internal controls in one graph. ClauseMatch reported that their AI models achieved over 90% accuracy in recognizing concepts and obligations, even finding instances of requirements not explicitly seen during training. This indicates that with proper taxonomy and training, much of the grunt work of building a reg knowledge graph can be automated.

- *Case: GDPR Knowledge Graphs.* Several research projects have tackled making GDPR machine-readable. One recent work, *PrivComp-KG (2024)*, created a **GDPR Compliance Verification Knowledge Graph** that *"formalizes GDPR rules and guidelines using Semantic Web technologies"*. This knowledge graph facilitates automated compliance checking by aligning privacy policy texts from companies to the GDPR's articles. It even supports **granular consent management** by mapping GDPR consent requirements to policy statements. The researchers used **ontology rules and inference** (via Semantic Web Rule Language, SWRL) to automatically reason over the graph and identify gaps in a vendor's privacy policy relative to GDPR. Another study integrated GDPR and PCI DSS into a single ontology (as mentioned), and their vision was that such a graph *"will significantly help in automating an organization's data compliance processes"* – not only saving resources but also *"proactively identifying data breaches"* by checking if any practice violates the encoded rules. These projects demonstrate that even complex legal text like GDPR can be systematically broken down into ontology classes (data subject rights, legal bases, obligations on controllers vs processors, etc.) and linked to real-world data processing activities for compliance checks.
- *Case: NIS2Onto.* Recognizing the complexity of the new NIS2 Directive, a group of researchers developed **NIS2Onto**, an OWL ontology to model NIS2's security requirements. Their ontological representation *"explains the structure of the document and enhances it with automatic reasoning capabilities"*. In practice, NIS2Onto allows a company to check whether their measures meet NIS2 requirements much faster. The authors highlight that NIS2Onto *"reduces time and effort required for verification… by enabling continuous monitoring of modifications…and minimizing the risk of human error"*, while covering a wide range of requirements so that no aspect is overlooked. Critically, as requirements change over time, those changes are *"handled automatically without human effort"* by the ontology-driven system. This points to **built-in adaptability** – an ontology can be updated once (e.g., if NIS2 gets amended or interpreted) and all connected compliance checks update immediately. The result is faster audits and easier demonstration of adherence to regulators. This project even applied the ontology to a real company as a case study, showing the approach's practical viability.

- *Case: OWASP ASVS JSON & OSCAL:* On the industry side, OWASP's provision of ASVS in JSON format and similar efforts (such as the U.S. NIST's OSCAL – Open Security Controls Assessment Language – which provides JSON/XML formats for control catalogs) show a trend toward **machine-readable standards**. While JSON or XML aren't semantic graphs per se, they similarly break down requirements into structured data that tools can ingest. For example, a security testing tool could take ASVS JSON and automatically know the list of verification requirements to test for a Level 2 application. The existence of ASVS in JSON has enabled platforms to incorporate it; one compliance tool has even converted ASVS into the NIST OSCAL format, aligning with a broader compliance data model. These efforts reinforce the demand for **programmatically accessible standards**, which knowledge graphs would elevate by adding rich semantic linkages (JSON is just a list, whereas a graph can link items to concepts or to each other).

Given these compelling benefits and early successes, semantic knowledge graphs appear to be a powerful solution to the limitations of static cybersecurity standards. However, moving to this paradigm requires a methodology for **capturing, structuring, and maintaining** regulatory knowledge in graph form. In the next section, we delve into how such a semantic model can be built and kept up to date, and the practical steps for linking regulatory content into a coherent knowledge graph.

Building and Maintaining Regulatory Knowledge Graphs

Transforming regulations from paper (or PDF) into a semantic graph is a non-trivial task – it combines legal analysis, information architecture, and technical tooling. Nonetheless, a structured approach can make it feasible. Here we outline a **practical roadmap** for capturing, linking, and maintaining regulatory content as a knowledge graph:

1. Define the Ontology (Schema) for the Domain:
Before inserting any specific regulation text, we need an ontology – a formal schema that defines the types of entities and relationships in this domain. For cybersecurity regulations, typical **ontology components** might include: **Requirements/Controls**, **Objectives** (the high-level goals or principles), **Actors** (e.g., Data Controller, Service Provider, Device Manufacturer – who must comply), **Assets** or **Data types** (what is being protected, e.g., personal data, networks), **Actions** (e.g., must encrypt, must notify, must authenticate), and **Relationships** like *requires*, *prohibits*, *isPartOf*, *appliesTo*, etc.

A well-designed ontology can mirror the structure of the law. For example, NIS2Onto took NIS2's measures and *"deconstruct[ed] the agents, actions, and objects of such measures, associating them with appropriate ontological commitments."* In plain terms, they identified the key elements in each security measure in NIS2 (who needs to do what, and to what). Their ontology thus could represent sentences like "Entity *X* must implement *Y measure* on *Z asset*" in a structured way. Similarly, a GDPR ontology might have classes for "Consent", "Legal Basis", "Personal Data", "Processing Activity", etc., and relationships encoding which processing requires which legal basis, etc.

It's often useful to reuse or reference **existing ontologies** to avoid reinventing the wheel. For instance, the *Unified Cybersecurity Ontology (UCO)* provides concepts for cyber defense, the *Privacy Ontology (PrOnto)* was developed to capture privacy/legal concepts (including some GDPR aspects), and various standards (like ISO 27002 controls) have been modeled by researchers. A strong ontology is extensible – one can add new classes for new regulations – and interoperable with others (leveraging standards like SKOS for taxonomies or Dublin Core for general metadata).

2. Text Mining and Initial Knowledge Extraction:
With a schema in hand, the next step is to ingest the regulatory documents. Natural Language Processing (NLP) techniques can greatly accelerate this. Modern NLP, including **large language models (LLMs)**, can help identify specific elements in text: section headings, requirement statements (often signaled by keywords like "shall" or "must"), references to other laws, etc. The goal is to tag pieces of text with ontology concepts. For example, an NLP pipeline might read the GDPR and label each article or paragraph with the relevant ontology classes (e.g., Article 33 is a "BreachNotification" obligation on the "Controller" actor, with a time requirement of 72 hours).

ClauseMatch's approach was to train AI models on a regulatory taxonomy and then automatically **extract entities and link content** at the paragraph level. They achieved high accuracy, suggesting that a well-trained model can parse even complicated regulatory language and correctly slot provisions into a structured form. Similarly, the PrivComp-KG project used an LLM in a **retrieval-augmented generation (RAG)** setup to align chunks of GDPR text with segments of companies' privacy policies. This kind of technique can be repurposed to align chunks of regulatory text with the ontology classes we've defined, effectively classifying text and extracting key relationships.

In practice, a combination of **automated extraction and expert review** works best. NLP might draft the graph content, and human experts (lawyers, compliance officers, ontologists) validate and refine it. Over time, as the system learns from corrections, the extraction improves. The output of this stage is that each regulatory requirement (down to sub-paragraph granularity) becomes an **instance in the knowledge graph**, with initial links (e.g., an obligation instance "notify data breach" is linked to actor "Data Controller" and to concept "incident reporting").

3. Linking and Mapping Across Documents:
Once individual regulations are represented, the next powerful step is to **establish links between equivalent or related requirements** across different standards. This is where the **"graph of graphs"** emerges, creating a unified compliance knowledge base.

Some linkages are straightforward: many standards share common control concepts (e.g., both ISO 27001 and NIS2 require an access control policy, GDPR and ISO 27001 both require some form of risk assessment, etc.). Using the ontology, we can assert that "ISO27002: Section 9.2 – User Access Management" *correspondsTo* "NIS2: Article 21(c) – Policies on access controls" (hypothetically). Or we might link both to a common node like "Access Control Policy" as an abstract concept. The integrated GDPR/PCI ontology explicitly did this by relating rules from both sources to the Cloud Security Alliance's control framework as a common reference point.

Other linkages involve **hierarchies**: for example, a high-level principle in one framework might encompass several detailed controls in another. GDPR's mandate for "appropriate measures" is fleshed out by more specific security controls in ISO 27002 or NIST frameworks. A knowledge graph can capture that *Article 32 GDPR has sub-controls encryption, pseudonymization, etc.* and each of those can link to a detailed standard (like ISO or OWASP guidance on encryption).

This crosswalk mapping is crucial to eliminate the **redundancy in compliance**. It ensures that when a company implements one control, they automatically see credit for compliance in multiple areas if applicable. It also helps identify **inconsistencies**: if two regulations have similar goals but slightly different thresholds (say one requires reporting an incident in 72 hours, another in 24 hours), the graph makes that difference explicit by a property on each "incident reporting" node.

Researchers mapping the AI Act to standards noted that any such mappings should use **"flexible, extensible, transparent, and auditable solutions"**, advocating for **open knowledge graphs** as the means to do it. In their work, they built an Open Knowledge Graph (the "TAIR" ontology for Trustworthy AI Requirements) to map AI Act concepts to ISO AI management standards. They published it as a resource that *"allows links between defined terms, concepts, and the requirements to be published in a traceable, queryable, and navigable manner."*. The emphasis on traceable and queryable links underscores how stakeholders can inspect and trust the mapping – something that black-box mappings or proprietary spreadsheets don't offer. Indeed, using open W3C semantic standards ensures **interoperability** and *"increases third-party inspection and confidence in the completeness and accuracy of mapping"*.

4. Implement Governance and Change Management:
A regulatory knowledge graph will evolve – both as regulations change and as our understanding or scope of the model grows. It's critical to establish a **governance process** for maintaining the graph. This might involve:

- **Authority and Validation:** Deciding who approves changes to the knowledge graph (e.g., a multi-stakeholder committee with regulatory experts). For instance, if a new interpretation of a law emerges (through a court decision or regulator guidance), the graph might need an update (perhaps a new relationship or annotation). Such changes should be validated by domain experts before being applied.
- **Versioning:** As mentioned, the graph can hold multiple versions of requirements. Best practice is to **never simply delete or overwrite** nodes representing regulations; instead mark old ones as superseded or time-bound, and add new ones. Consumers of the graph can then filter by date or version. For example, a query could specify "use NIS2 as of 2025" versus "NIS2 as originally adopted in 2022" if amendments happen.
- **Tooling for Updates:** Changes in law (new regulations, amendments) should trigger an update workflow. Some of this could be automated (e.g., monitor official EU law publications for updates, then run NLP to ingest the changes into the graph). The Norwegian Maritime Authority (NMA) provides an inspiring example: since 2020, they have an **automated pipeline to convert new regulatory texts into a semantic knowledge graph**. Using tools like SHACL (Shapes Constraint Language) for describing compliance rules, the NMA pipeline takes plain text regulations and turns them into RDF nodes systematically. This kind of pipeline ensures the graph is never out of sync with the current law. Notably, NMA is enriching their regulatory graph by connecting it "to all aspects of the maritime domain", showing how a base regulatory graph can be expanded with domain-specific data over time.
- **Continuous Alignment with Reality:** The knowledge graph isn't just for the text of laws; it should ideally link to the actual *controls and policies within an organization*. Maintaining those links (which might be proprietary to each company) is part of internal governance. For example, if a company changes its access control policy, it should update the link in their internal compliance graph indicating that policy covers XYZ requirements. This is analogous to keeping an inventory of controls mapped to requirements, but in a far more dynamic way.
- **Security and Privacy of the Graph:** Since the regulatory graph could contain sensitive info (especially when linking to an organization's internal controls or compliance status), maintaining proper access control to the graph data is important. Portions might be public (the regulation ontology itself could be open), while the company's instantiation (with their compliance evidence) is kept internal or shared selectively.

With these steps, the outcome is a **living knowledge base of compliance**. Rather than a bookshelf of binders and PDFs, an organization (or a regulator, or an industry group) has a **queryable, up-to-date graph** that anyone (or any system) can consult to understand obligations, controls, and their relationships. The heavy upfront work of modeling and populating the graph pays off in the **agility and clarity** it provides going forward.

Next, we look at one of the most powerful advantages of this approach: the ability to **slice and customize** the vast body of regulations to fit the needs of specific sub-entities, teams, or contexts within an organization, addressing the long-standing challenge of one-size-fits-all standards.

Granular Customization of Standards in Context

Every organization is different – and within organizations, every department or project can face a different risk profile and regulatory focus. Static regulations can't capture these nuances, but a semantic approach can. By leveraging the rich structure of a knowledge graph, we can achieve **contextual and granular customization** of compliance requirements, tailoring the view of the "rules" to the relevant subset for each audience or use-case.

How Graphs Enable Custom Views: In a regulatory knowledge graph, each requirement or control is an individual node that can carry attributes (metadata) and relationships. By tagging nodes with certain attributes or linking them to contextual nodes, we effectively annotate the conditions under which that node is relevant. This means we can query or filter the graph based on those attributes to produce a custom subset.

For example, consider a large enterprise that has multiple departments: HR, IT, R&D, Finance, etc., and operates in multiple jurisdictions. The enterprise's compliance knowledge graph could include tags like `Department:HR` or `Region:EU` on certain requirements or controls. Suppose GDPR's obligations around handling personal data are tagged `Department:HR` (since HR handles a lot of employee data) and maybe `Region:EU` (if it applies specifically to EU data). Meanwhile, a requirement from a U.S. law (like CCPA in California) might be tagged `Region:US`. If the HR team in Europe wants to see what they need to comply with, a query like "requirements where Department=HR and Region=EU" would yield GDPR's relevant obligations, any HR-specific security policies, etc., without showing them, say, technical server requirements meant for IT.

At a more fine-grained level, one could tag **each requirement with applicability conditions from the text of the law**. Many regulations have scoping statements – e.g., NIS2 might say certain requirements apply only to "essential entities" vs "important entities"; GDPR has some exemptions for SMEs in documentation. In the graph, a requirement node can have a property `applicability: EssentialEntitiesOnly` or an object property linking it to

an “Essential Entity” class. Thus, if you know your organization is categorized as an “important entity” under NIS2, you could filter out those nodes (or mark them as not mandatory). This is far more efficient than footnotes in a PDF – it’s an active filter on the knowledge base.

Department and Team Level Views: Internally, organizations can create **sub-graphs or dashboards** for each team. For instance:

- The **DevSecOps team** could have a view generated from the graph that focuses on secure development requirements: it would pull in relevant controls from OWASP ASVS, any secure coding mandates from internal policy, and relevant legal requirements (like under the EU Cyber Resilience Act, if any, about software development practices). The knowledge graph can link those ASVS controls to the broader regulatory obligations they satisfy (e.g. “input validation” control links to the principle of preventing exploitation of software, which ties to a general duty of care under a law). So the DevSecOps team sees a *practical checklist* with traceability to high-level obligations.
- The **Incident Response team** could query the graph for everything related to incident handling: it would gather requirements from NIS2 (incident reporting duties), GDPR (personal data breach handling), ISO 27001 (incident response controls), etc., in one place. Moreover, it could contextualize by severity – maybe tag which incidents must be reported externally vs just internal. When an incident occurs, the team could use the graph to instantly see “Given this incident type and affected data, which regulators need to be notified and what’s the timeline?” – a question answerable by traversing the graph from the incident node to obligations nodes (NIS2 says report within 24 hours to CSIRT, GDPR says 72 hours to DPA if personal data, etc., each encoded in the graph).
- For **subsidiaries or sub-entities**, if a conglomerate operates different businesses, each business unit could integrate its own context. Say one subsidiary is in healthcare, another in finance – the base regulatory graph can be extended with industry-specific regulations (healthcare has HIPAA in US, finance has PSD2 in EU, etc.) and each subsidiary’s view filters to its industry. The TAIR ontology for the AI Act noted this concept: they suggested the model could be extended by *“subject matter experts in specific high-risk application domains, such as healthcare or education, who may seek to build domain-specific extensions to concepts in this model.”*. In other words, start with a general regulation graph, then plug in domain specifics. In our context, a base cybersecurity ontology can be extended for, say, healthcare privacy or fintech requirements by adding extra nodes and links, without losing the connection to the common core.

Multi-Tier Controls and Assurance Levels: Some standards already have built-in levels (OWASP ASVS has Level 1/2/3, ISO 27001 allows control exclusions based on risk, etc.). A graph can elegantly handle this by treating each level or control applicability as an attribute. For example, ASVS’s JSON data includes which level each requirement is. In the graph, one could mark a control node “ASVS-1” as Level 1 (for all apps), while others are

Level 2 or 3 (for high-security apps). If a particular project is classified as needing Level 2, a query can exclude Level 3 items. This spares developers from wading through unnecessary requirements for their context.

Maintaining Consistency: One might wonder, if everyone has their own custom view, do we risk fragmentation or missing the big picture? The beauty of the knowledge graph approach is that these are **views of the same unified graph**. The underlying data is consistent; you're just not showing all of it to all people at all times. Think of it like different slices of a multidimensional dataset. This actually **improves consistency**, because when a regulation updates, the core graph updates in one place, and *all* the custom views automatically reflect the change (as long as it's within their filtered scope). In contrast, today someone might update a company-wide policy, but an individual team's checklist document might not get the memo immediately.

Example: Let's say the EU updates the incident reporting timeframe in a law from 72 hours to 24 hours. In a graph, you change the property `maxReportTime` of the "Report Incident to Authority" requirement node from 72 to 24. Now, any team view (security operations, management dashboard, etc.) that includes that obligation will now show 24 hours as the requirement. In the old way, you'd have to update the central policy, then make sure every departmental procedure that copied that info updates. It's easy to miss one, causing compliance failures. The graph ensures a **single source of truth**.

Enhancing Relevance and Reducing Noise: By filtering out non-applicable requirements for a given context, employees and implementers face **less clutter**. One common complaint is that compliance checklists are bloated with items that might not apply, causing "checklist fatigue." With contextual queries, a team responsible for, say, cloud infrastructure doesn't need to see requirements that only apply to end-user computing environments, etc. This targeted approach can improve adoption and understanding, since each requirement presented can be accompanied by *why it matters* (the graph might link it upward to a risk or principle, providing rationale).

Tool Support for Custom Views: In practice, user-friendly tools could sit on top of the knowledge graph. For example, a web portal where a user selects their role, department, and maybe specific regulations they care about, and the system dynamically generates a tailored compliance guide from the graph. Even without exposing the complexity of the graph, end users experience a highly relevant, trimmed-down set of guidelines.

This approach aligns with the idea of **modularity in standards** – breaking big standards into modules that can be selected as needed. Semantic graphs provide the ultimate modularization, down to each rule. It's like **Lego blocks** of compliance that can be assembled differently for each scenario, rather than a one-size-fits-all block.

To illustrate briefly, Table 1 provides a conceptual comparison of a static vs. semantic approach to customization:

Aspect	Static Standard (PDF)	Semantic Graph-Based Standard
Applicability Filtering	Reader manually decides what sections apply (often skipping irrelevant parts).	Query can programmatically filter nodes by tags (e.g., by department, risk level, data type). Non-applicable requirements are automatically excluded from view.
Detail vs. Summary	Either one document tries to do both (resulting in a very long document with general and detailed parts interwoven) or separate high-level vs. low-level docs exist with potential gaps between.	Graph can link high-level principles to detailed controls. Users can toggle between summary view (just principles) and detailed view (principles + linked controls) as needed, without losing traceability.
Multiple Frameworks	If using multiple standards (e.g. ISO + internal policy), teams have multiple documents to consult. Tailoring means creating a new merged document or spreadsheet.	Graph already integrates multiple frameworks. A single query can pull relevant nodes from all sources at once (e.g., “show me all controls from either ISO or NIST that our policy uses for Cloud Security”).
Change Propagation	When a central policy or standard changes, each team’s custom documentation must be manually updated. Risk of inconsistency if any are missed.	Change is made in graph once. All contextual views reflect the updated information immediately, ensuring consistency across the board.
Granularity	Typically whole sections or clauses are the smallest unit, which might still bundle multiple requirements. Hard to isolate sub-requirements for specific owners.	Each requirement is a node that can be assigned to a specific owner or context. Granular assignments (even sub-clause level) are possible.

Through semantic customization, organizations can achieve what was previously a dream: **tailored compliance guidance** that is both wholly aligned with enterprise-wide policy and exquisitely relevant to the local context. This significantly lowers the burden on individual teams and increases the

likelihood of proper implementation, because teams get exactly the guidance they need – *no more, no less*.

Having explored internal customization, we now turn to the external dimension: how making standards machine-readable and compliance data structured can improve interactions between organizations – especially for **third-party risk management** and overall market transparency.

Externalizing Compliance Knowledge: Transparency and Trust in the Ecosystem

In today's interconnected digital economy, an organization's cybersecurity risk is deeply tied to its **partners, suppliers, and service providers**. Regulations like NIS2 and DORA explicitly require oversight of third-party risk. Typically, this is managed via contractual requirements and periodic assessments or audits (think of the lengthy security questionnaires companies exchange, or on-site audits for critical vendors). This process is often slow, opaque, and inefficient – much like traditional compliance – because it relies on static reports and manual reviews.

By **externalizing compliance metadata** in a controlled way, organizations can move toward a more transparent and continuous model of third-party assurance. If many organizations adopt semantic compliance graphs (even internally), there's an opportunity to share portions of those graphs (or the insights from them) with partners, customers, and regulators. Here's how that could transform the landscape:

Streamlined Third-Party Risk Assessment:
Imagine a scenario where instead of sending a 200-question security questionnaire to a vendor, you send a *standardized query* or request for their compliance data. The vendor could have an **exported view of their compliance knowledge graph** that they share securely. For example, a cloud provider might share a knowledge graph that shows how its controls map to ISO 27001, CSA Cloud Controls Matrix, and perhaps NIS2 requirements for cloud services. A client's risk assessment system could ingest this graph and automatically identify which required controls are **covered, partially covered, or not covered** by that provider.

This is analogous to how financial data sharing via standards (like XBRL for financial reporting) made analysis easier – here, compliance data is standardized and machine-readable. The outcome is faster, more objective vendor evaluations. One could even envisage regulator-approved **compliance tokens or certificates** that vendors publish in real-time; for instance, an API endpoint that always provides the current compliance status of key controls (with proofs or audit stamps attached).

Some early movements reflect this idea. The EU cybersecurity certification framework (under the Cybersecurity Act) aims to create *common certificates* for products and services (like "ISO 27001 certified" or "Common Criteria EAL certified"). If those certifications were backed by knowledge graphs, a relying party could query the specific criteria the product was certified against and the evidence provided. While currently certifications are static documents, in the future, they could be **dynamic attestations** accessible via a graph.

Transparency and Market Trust:
When compliance information is shareable, it introduces a new level of **market transparency** for security and resilience. Consider **cloud service providers** as an example: they often publish compliance white papers or attestation letters (SOC2 reports, ISO certificates). These are helpful but static and often summary-level. If instead a provider offered a navigable knowledge graph of their controls, customers could explore how the provider meets various regulations and standards. This transparency can become a selling point – companies with strong security postures can *demonstrate* it clearly, not just assert it. It creates a market incentive: those who invest in security and compliance can more easily prove their trustworthiness and potentially win more business.

We already see hints of this in other domains: e.g., **sustainability data** – companies are increasingly pressured to share ESG (Environmental, Social, Governance) metrics. In cybersecurity, sharing metrics or controls is sensitive, but a structured approach allows selective sharing. An organization might choose to publish certain high-level compliance assertions (like "compliant with NIS2 Article X, Y, Z; certified ISO27001 for scope ABC") in an open format. More detailed mappings (like specific control implementations) might be shared under NDA with key partners or regulators.

An important benefit of transparency is **accountability**. If a company publicly states compliance in a machine-readable way, stakeholders (including watchdog groups or investors) could automatically monitor for changes. If that compliance data is found inconsistent or if the company quietly drops a certification, it would be noticeable. This creates gentle pressure to maintain high standards – a company wouldn't want to advertize a strong posture and then have to withdraw it. In other words, it **"incentivizes a market that rewards security and responsible behavior"**: those who maintain robust compliance can be recognized and preferred, while lapses or weaker postures are harder to hide or gloss over.

Example – Third-Party Integration:
Take a bank that relies on a fintech API provider. The bank needs to ensure the fintech company meets certain security requirements. Using the old model, the bank might do an annual audit and hope nothing slips through in between. In a knowledge-graph-driven model, the fintech could grant the bank **access to a live view** of its compliance graph, specifically tailored to the bank's requirements (perhaps the bank shares a template of requirements in graph form, and the fintech aligns its controls to that template). The bank's systems could continuously or periodically query this: "Is

control X implemented? Show evidence or status." If the fintech updates a control (say, improves their encryption standard), they update their graph and the bank sees that update. Conversely, if a control regresses or a new requirement is introduced, it surfaces quickly. This is essentially **continuous compliance monitoring** between entities – a much more dynamic partnership.

One could envisage **marketplaces or repositories** of compliance graphs. For instance, an open repository where standard ontologies for regulations are hosted (maintained maybe by EU institutions or standard bodies), and companies can publish compliance statements linked to those ontologies. ENISA or another body might maintain the official NIS2 ontology, and companies may publish an RDF file stating "we comply with NIS2 requirement X with control Y (see our policy doc reference)". Tools could aggregate these to show, for example, how prepared various sectors are for NIS2 – a level of insight currently gleaned only through surveys and self-reporting.

There is precedent for open data in law: EU regulations themselves are available through EUR-Lex (sometimes even with XML metadata), and efforts like the **EU's machine-readable open data for legislation** are growing. But making compliance implementations open is new ground. It will require careful scoping of what to share (you don't want to reveal your "security recipe" to attackers). Likely, the shared metadata would be high-level (compliance status, not the nitty-gritty technical config). However, even high-level data can be useful, akin to a **"Nutrition label"** for a service's security (an analogy sometimes drawn in policy discussions).

A concrete example on the horizon: The proposed **EU Cybersecurity Label for consumer IoT**. The idea is products will carry a label indicating they meet certain cybersecurity requirements. If those requirements are modeled in a graph, a product manufacturer could publish a reference saying "Product X – conforms to requirements A, B, C of the EU IoT label standard" with maybe a link to evidence. Consumers or regulators could then verify that claim via a digital registry. This is essentially externalizing compliance info to the mass market.

Better Regulatory Oversight and Learning:
If companies share compliance data, regulators themselves gain a powerful tool. They could aggregate compliance graphs to see common gaps. For instance, a regulator might query across all submitted compliance data: "Which NIS2 measures are most often marked not implemented?" and find systemic issues to address via guidance or enforcement. It moves oversight from reactive audits to proactive analysis. Additionally, **regulatory reporting** could be streamlined. Instead of firms writing extensive narrative reports to regulators, they might submit a compliance data model annually (or continuously). The UK and others have explored "RegTech for regulators" where even financial filings become data feeds; similar could happen for cyber compliance.

The emphasis on **market transparency** does not mean all compliance info is public. Rather, it means creating an *option* and *infrastructure* for sharing standardized compliance information with authorized stakeholders. The default today is PDF reports behind NDAs; the future could be consented data sharing via secure APIs or public posting of non-sensitive compliance claims.

One challenge to mention is that **standards organizations (like ISO)** often monetize their standards documents, which could impede open sharing of their content in knowledge graphs (the *paywall fees* issue). For truly open compliance data exchange, either the ontologies would focus on high-level concepts not verbatim text, or there would need to be agreements to allow certain structured representations to be open. The EU can lead here by making the text of its regulations open (which they are), and by possibly providing official mappings to common standards (the AI Act mapping project noted the need for EC and ESO agreement to make harmonized standards more accessible).

In summary, **externalizing compliance knowledge** through semantic graphs can create a more transparent, efficient, and trust-based ecosystem. Companies can more easily trust each other when they can verify security postures; regulators can trust but verify through data; and ultimately, end-users benefit from a market where security is visible and valued.

The final section will consider the **strategic implications** of this transformation – how it affects compliance strategy and what steps policymakers and GRC professionals should consider to foster this evolution.

Implications for Compliance Strategy and Policy

Adopting semantic, graph-based regulatory models is not just a technical tweak – it's a strategic shift in how we approach compliance and regulation. The **impacts span multiple dimensions**:

- **Compliance Management Becomes Proactive:** Organizations that embrace compliance knowledge graphs can move from a reactive stance (checking boxes after the fact, or scrambling when audits loom) to a **proactive, continuous compliance** posture. With automated monitoring against a knowledge graph of obligations, compliance becomes an ongoing activity embedded in business processes. Issues can be flagged and fixed in near real-time. This aligns with emerging best practices of "continuous control monitoring" and gives GRC (Governance, Risk, Compliance) teams a real-time dashboard of risk and compliance status. Fewer surprises during formal audits, and hopefully **no more big gaps** where a

requirement was misunderstood or overlooked – the graph makes it harder to ignore any node, and reasoning rules can catch conflicts or omissions early.

- **Reduced Costs and Burden (Especially for SMEs):** Automation and efficiency directly translate to cost savings. SMEs, which currently are **"disproportionately affected [by compliance burdens] due to limited resources"**, stand to gain significantly. If regulators or industry groups provide ready-made knowledge graph content (e.g., an out-of-the-box NIS2 ontology with guidance), SMEs can plug it in and let tools guide them through what's needed, rather than hiring expensive consultants to interpret the law. Over time, compliance as a data-driven process should cost less than compliance as a manual paperwork process. This also lowers barriers to entry for startups in regulated spaces – they can more quickly understand and meet requirements with the help of machine-readable standards.
- **Enhanced Regulatory Impact:** Regulations achieve their desired impact (better security, privacy, etc.) only if implemented well. By facilitating implementation, semantic standards could **amplify the impact of Europe's regulations**. Instead of rules on paper that companies struggle to follow, we'd have rules in code that can be executed and verified. Regulators might see higher compliance rates and could focus enforcement on truly negligent cases rather than companies that tried but failed due to complexity. Also, regulators could issue **official semantic schemas** alongside laws. For instance, imagine when the EU AI Act goes into effect, the Commission also releases an official OWL ontology for it. This would guide industry implementations and ensure consistency in how the law is interpreted in graphs (preventing divergent ontologies that don't align).
- **Evolving Skill Sets and Roles:** Both regulators and compliance professionals will need to evolve. We'll see demand for **"compliance engineers"** – people with both legal/regulatory knowledge and data/ontology skills. Already, fields like RegTech and LegalTech are merging lawyers with technologists. Policymakers might consider this in capacity building: e.g., ENISA and national authorities might develop internal tools and talent to accept machine-readable reports or to publish machine-readable guidelines. Similarly, companies will invest in GRC tools that support knowledge graphs, and GRC staff will need training to use them (e.g., how to query a SPARQL endpoint for compliance data, or how to update an ontology when a new policy comes out).
- **Public-Private Collaboration:** The creation of standardized regulatory ontologies likely calls for collaboration. **Standards bodies, industry consortia, and regulators** should work together. We might see new working groups specifically for "Digital Regulation" that maintain these models. The EU could fund projects (through Horizon Europe or similar) to develop open ontologies for major regulations (some of this is already happening in academic circles, as we cited). Policymakers can encourage or even mandate that regulatory proposals come with a technical annex that outlines key requirements in a structured form. A modest step could be assigning **unique identifiers to provisions** (some regulations

do this with paragraph IDs), which is a stepping stone to hyperlinking and mapping. The U.S. for example has the Federal Register with some XML structure; EU could expand ELI (European Legislation Identifier) usage for granular citation of rules in data.

- **Technology and Standardization:** On the tech side, if Europe leads in regulatory knowledge graphs, it could also **influence global standards for compliance data**. Just as GDPR influenced global privacy practices, a European push for machine-readable regulation might set a model. We might see the rise of **ontology standards for cybersecurity compliance** that become internationally adopted. This also could create an ecosystem of tools (EU startups or existing firms building compliance graph databases, reg-tech AI, etc.), boosting innovation. It aligns with the EU's goal of digital leadership in governance.
- **Challenges and Considerations:** Of course, this shift won't be without challenges. Data quality and consistency are paramount – a poorly constructed knowledge graph could lead to false assurances (e.g., an incorrectly mapped control might show compliant when it's not… not implemented). Rigorous **validation and testing** of the ontologies and mappings is essential – ideally involving regulators, auditors, and industry experts to vet that the knowledge graph accurately represents the intent of the law. Security of the compliance data is another consideration; shared compliance graphs must be protected against unauthorized modification, since a tampered graph could falsely indicate compliance. These are challenges to be managed with governance and technology (e.g., digital signatures on compliance data, standard validation suites for ontologies), not roadblocks to the overall approach.

Incentivizing Adoption: Policymakers can encourage this shift by endorsing or even providing machine-readable regulatory content. For example, European agencies could publish official **reference ontologies** for major regulations (as a companion to the legal text) and encourage their use. They might also recognize or reward organizations that demonstrate **innovative compliance management**, perhaps through regulatory sandboxes or pilot programs. If regulators signal that machine-readable compliance data will simplify oversight (or reduce audit frequency), companies will have motivation to invest in it. The upcoming generation of cybersecurity frameworks (e.g., future iterations of NIS or GDPR) could bake in requirements or encouragement for **compliance automation** and reporting in standardized formats.

Finally, it's worth noting that this transformation aligns with Europe's broader digital ambitions. The EU has championed **open data, interoperability, and digital innovation** in many arenas – applying those principles to its own regulatory processes is a logical next step. By scaling up its regulatory superpower through technology, Europe can ensure its cybersecurity rules are not only strong on paper but also effectively implemented on the ground, across diverse contexts, with lower cost and friction. This will lead to better security outcomes – the true goal behind any regulation – and will solidify Europe's leadership as not just a rule-maker but an **innovation-maker** in governance.

Conclusion

Europe's bold and comprehensive approach to cybersecurity regulation has set it apart as a global **"regulatory superpower."** The challenge now is to **scale and adapt** that strength to the complexity of the digital age. Static PDFs and one-size-fits-all checklists won't suffice for the dynamic, interconnected, and granular world of modern cybersecurity. The solution lies in marrying Europe's regulatory expertise with the power of **semantic technology** – turning dense rules into living, linkable knowledge.

By evolving standards and regulations into **semantic graph-based structures**, we unlock the ability to **navigate complexity with clarity**. Overlapping laws can be reconciled via links, broad principles can be traced to specific controls, and each organization (or team within it) can get a customized roadmap to compliance. Machine-readable, context-aware regulations mean compliance can be woven into the fabric of business operations, checked by machines, and updated at the speed of change. The burden of compliance can drop, while assurance and security improve – a true win-win for both industry and regulators.

For policymakers and GRC professionals, the message is clear: it's time to **embrace the tools of digital transformation within regulation itself**. This doesn't mean making laws in code instead of words, but supplementing those laws with the **digital infrastructure** to implement them. Europe has an opportunity to lead by example – just as GDPR made the world take notice of privacy, a push for **RegTech innovation** in compliance could become another valuable European export. A collaborative effort to build open compliance ontologies, share best practices, and perhaps establish pilot programs for semantic compliance reporting would pave the way.

In conclusion, scaling Europe's regulatory superpower is not about writing ever more regulations – it's about ensuring the regulations **achieve their purpose** in a scalable way. Semantic knowledge graphs offer a path to do exactly that: **preserve the intent and rigor of European cybersecurity standards, while making them agile, navigable, and fit for a digital world**. By adopting this approach, Europe can strengthen the effectiveness of its cybersecurity regime, ease the compliance journey for organizations of all sizes, and foster a market environment that rewards security and responsibility. In an era of escalating cyber threats, such innovation in regulatory practice is not just desirable, but necessary to keep pace. Europe has led in setting the rules – now it can lead in how those rules are delivered and executed, truly bringing its regulatory superpower into the 21st century.

Sources:

- European regulatory landscape and overlaps – ECSO analysis of compliance challenges; Atlantic Council on EU's regulatory influence; PrivComp-KG on GDPR's global impact.
- Limitations of static compliance documentation – Research noting regulations are only in textual format requiring significant manual effort.
- ClauseMatch & ADGM knowledge graph pilot – demonstrating machine-readable regulation and "Regulation-as-a-Service" vision.
- Integrated GDPR and PCI DSS ontology – example of mapping multiple standards in one knowledge graph.
- NIS2Onto and benefits of ontologies – continuous monitoring, automatic updates, reduced human error in compliance.
- Open Knowledge Graph for AI Act – need for flexible, transparent mappings using W3C standards for interoperability and third-party trust; publishing requirements in a queryable, navigable manner.
- OWASP ASVS in JSON – example of an industry standard providing machine-readable format for programmatic use.
- Norwegian Maritime Authority case – automated pipeline for machine-readable regulations using RDF/SHACL.
- PrivComp-KG – formalizing GDPR with semantic web tech for automated compliance checks.
- Fenz's work on ISO 27002 – formalized controls to enhance automated compliance checking.
- Need for contextualization – EU AI Act separates principles vs. technical standards illustrating challenge of mapping high-level to detailed implementation.
- Importance of open standards for mappings – to allow third-party inspection and confidence in compliance completeness.
- ClauseMatch commentary – on rapidly changing regulations and need for tech to keep up.