ISO, NIST and the European Regulatory Perspective

Rahim Hahimov – 17 February, 2026

***Abstract*—Abstract—This paper presents standards (NIST, ISO/IEC) and EU regulations (NIS2, GDPR, DORA, CRA, CER) for SOC analyst projects. Using a German hospital scenario, we demonstrate a 4-step implementation: CSF structure → incident lifecycle → SIEM rules → regulatory compliance.**

***Index Terms*—SOC, NIST CSF, ISO 27001, NIS2, GDPR, DORA, Cyber Resilience Act, CER Directive, Incident Response, Cybersecurity Frameworks**

I. Introduction

Designing or documenting a Security Operations Center (SOC) analyst project requires alignment with internationally recognized cybersecurity standards and regulatory frameworks. The most influential frameworks fall into three major categories: U.S. standards (NIST), international management standards (ISO/IEC), and European Union regulatory frameworks (NIS2, GDPR, DORA, CRA, CER). Together, these frameworks define how cybersecurity risk is structured, managed, monitored, and reported within an organization.

II. NIST Perspective (United States)

The National Institute of Standards and Technology (NIST), founded in 1901 and part of the U.S. Department of Commerce, provides foundational cybersecurity guidance widely adopted globally [21].

A. NIST Cybersecurity Framework (CSF) v2.0

The NIST Cybersecurity Framework (CSF 2.0) provides a high-level, outcome-based structure for managing cybersecurity risk. It consists of six interconnected Functions [1]:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

For a SOC project:

- SOC monitoring aligns primarily with Detect
- Incident handling aligns with Respond
- Post-incident activities align with Recover
- Governance integration aligns with Govern

Because CSF is flexible and technology-agnostic, it is well suited as the structural backbone of SOC documentation: policies, process diagrams, runbooks and KPIs can be mapped to the relevant Functions and Categories, which in turn helps demonstrate coverage to management and regulators [20].

B. NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide

NIST SP 800-61 defines the canonical incident response lifecycle [2]:

1) Preparation
2) Detection & Analysis
3) Containment, Eradication & Recovery
4) Post-Incident Activity

This publication is essential for SOC runbooks, playbooks, escalation procedures, and lessons learned processes.

C. NIST SP 800-53 – Security Controls

NIST SP 800-53 Rev. 5 [3] includes 395 controls across 20 families (AC, IR, AU, SI) with Low/Moderate/High baseline and integrated privacy controls. It supports detection engineering, logging requirements, access control monitoring, and supply chain risk management. SP 800-53 feeds SOC use-case design by mapping controls (e.g., AC, IR, AU, SI) to monitoring logic.

III. ISO Perspective (International / Management-Oriented)

As one of the oldest non-governmental international organizations since 1947, ISO provides management-system requirements rather than technical prescriptions [**?**].

A. ISO/IEC 27001:2022

ISO/IEC 27001:2022 defines requirements for establishing an Information Security Management System (ISMS). Relevant to SOC [4]:

- Logging
- Access control
- Incident management
- Continuous improvement (PDCA cycle)

B. ISO/IEC 27002:2022

Provides detailed control guidance. Useful for translating controls into detection rules, defining logging requirements, and supporting SOC monitoring coverage [5].

C. ISO/IEC 27035 (Parts 1–3):2016 – Incident Management

ISO/IEC 27035 defines a five-phase model for incident management [6]:

1) Prepare
2) Identify
3) Assess
4) Respond
5) Learn

This model is closely aligned with NIST SP 800-61.

4. European Regulatory Perspective

Unlike NIST and ISO (voluntary standards), EU frameworks are legally binding.

4.1 NIS2 Directive (Directive (EU) 2022/2555)

Effective: October 2024
Applies to: Essential and Important entities, critical infrastructure sectors

Key SOC implications [7]:

- 24-hour incident notification
- Supply chain oversight
- Logging maturity
- Governance accountability

NIS2 elevates SOC capabilities from best practice to legal obligation.

4.2 General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) [8]

Applies whenever personal data is processed. SOC relevance: log retention limitations, data minimization, breach notification (72 hours), monitoring proportionality. GDPR operates alongside all other cybersecurity regulations.

4.3 DORA – Financial Sector [9]

Digital Operational Resilience Act
Effective: January 2025
Applies to: Banks, insurance companies, financial ICT providers

Requirements:

- 4-hour major ICT incident reporting
- Resilience testing
- Third-party attestation

DORA overrides NIS2 for financial institutions (sector-specific precedence).

4.4 Cyber Resilience Act (CRA) [10]

Effective: December 2027 (phased)
Applies to: Manufacturers of digital products

Requirements:

- Secure-by-design development
- Vulnerability disclosure
- Software Bill of Materials (SBOM)

CRA focuses on product security, unlike NIS2 and DORA (operational security).

4.5 CER Directive

Critical Entities Resilience Directive [11]

Focuses on:

- Physical resilience
- Infrastructure continuity
- Cross-sector crisis coordination

Complements NIS2.

TABLE I: Framework Nature and Focus Comparison

Framework	Nature	Focus
NIST CSF	Voluntary, risk structure	Common taxonomy via 6 functions, categories, subcategories [13]
ISO 27001	Certifiable management system	ISMS requirements (policy, risk assessment, continual improvement) [19]
NIS2	Mandatory operational cybersecurity	Risk management, incident reporting for critical entities [14]
GDPR	Mandatory personal data protection	Applies whenever EU personal data processed [8]
DORA	Mandatory financial resilience	Digital operational resilience (lex specialis) for financial entities [19]
CRA	Mandatory product security	Digital products lifecycle security [14]
CER	Mandatory physical resilience	All-hazards resilience of critical infrastructure [17]

IV. Nature and Focus of Each Framework

Key Distinctions regarding Table I

- DORA overrides NIS2 for financial entities (lex specialis) [15]
- GDPR applies horizontally whenever personal data is involved [8]
- NIS2 + CER overlap in critical sectors [16]
- CRA regulates products; NIS2 regulates services [19]

V. Applying These Frameworks in a SOC Project

A Security Operations Center (SOC) is like a 24/7 control room that watches for cyberattacks and handles them—like the "cybersecurity fire department" for a company. This section shows exactly how to build one using the 4-step approach through a realistic scenario: a German hospital building its first SOC.

A. The Hospital Scenario: Why They Need a SOC

Hospital "MediKlinik" (500 beds, Düsseldorf) handles patient records, medical devices, and emergency services. It's critical infrastructure, so EU laws apply. Hackers could:

- Steal patient data → lawsuits
- Shut down ventilators → lives lost
- Disrupt emergency systems → chaos

Current state: No central monitoring. IT gets alerts randomly. No process for "is this an attack?"

Goal: Build a SOC that watches 24/7, handles incidents, and satisfies all laws.

B. What Each Policy/Standard Actually Does (Simple Definitions)

TABLE II: American Standards (Voluntary "Best Practices")

Standard	What it does	Hospital Goal
NIST CSF 2.0	Big-picture map of cybersecurity jobs (6 functions: Govern→Identify→Protect→Detect→Respond→Recover)	Says "our SOC watches (Detect), fights (Respond), fixes (Recover), reports (Govern)" [1]
NIST SP 800-61	Step-by-step "how to handle a cyber incident" (4 phases: Prep→Detect/Analyze →Contain/Recover →Lessons)	Playbook template for "patient records hacked!" [2]
NIST SP 800-53	400+ checklist items ("log all logins", "monitor privileged users") grouped in 20 families	"What exactly should we watch in SIEM?" [3]

TABLE III: International Standards (Certifiable "Management Systems")

Standard	What it does	Hospital Goal
ISO 27035	Incident management process (5 phases: Prepare→Identify→Assess→Respond→Learn) [6]	Same as NIST 800-61 but international wording for auditors
ISO 27002	90+ practical controls ("log failed logins", "check vendors") [5] Turns vague "watch threats" into specific SIEM rules	

TABLE IV: EU Laws (MANDATORY - Fines up to 10M€ or 2% revenue)

Law	Applies when	SOC Requirements
NIS2 (2022/2555)	Critical infrastructure (hospitals, energy, transport) [22]	24-hour "significant incident" reports to BSI; supply chain monitoring; management accountability
GDPR (2016/679)	ANY personal data (patient records) [23]	72-hour breach notification; logs can't keep data forever; monitoring must be "proportional"
CER (2022/2557)	Physical resilience for critical entities [24]	Watch physical threats too (camera feeds, facility access); infrastructure continuity
DORA	Financial sector only (skip for hospital) [25]	4-hour ICT reports + stress tests (N/A here)
CRA	Software makers only (skip for hospital) [26]	Vulnerability tracking + SBOM (N/A here)

C. WRONG ORDER: "Laws First" Disaster (Step 4 → Steps 1-3)

Week 1: Boss reads NIS2: "24-hour reporting! GDPR logs! CER threats! Buy SIEM now!"

Team panic-buys:

- SIEM: €200k/year
- Rules: "Alert EVERYTHING!" (10,000 alerts/day)
- Excel: "NIS2 Incident Report v1"
- Logs: Everything forever → GDPR violation

Week 4 - Total failure:

- ■ Analysts quit: "Can't triage 10k alerts!"
- ■ NIS2 audit fails: No governance, no playbooks
- ■ GDPR fine: Patient logs kept 2 years (illegal)
- ■ CER ignored: No camera monitoring
- ■ Cost: €300k wasted

Why? Laws say **WHAT**, not **HOW**. No structure (Step 1), no process (Step 2), random alerts (Step 3).

D. CORRECT ORDER: Operations First (4 Steps)

Step 1 – NIST CSF 2.0 (Week 1) ✓
What: Map hospital SOC to 4 functions:

```
Detect  ← Daily monitoring (SIEM, logs)
Respond ← Incident handling (on-call team)
Recover ← Backup tests, lessons learned
Govern  ← Monthly reports to director
```

Why first? Creates "buckets" for everything else. Hospital result: Director approves: "Clear 4 jobs. Budget OK."

Step 2 – Incident Lifecycle (Week 2) ✓

What: Unified process blending NIST 800-61 + ISO 27035

```
NIST 800-61: Prep →
Detect/Analyze → Contain/Recover →
Lessons

ISO 27035:  Prep → Identify → Assess
→ Respond → Learn

↓ Combined playbook:

1. Alert arrives → Triage (30min)
2. Escalate if ransomware/breach
3. Contain → Backup restore → Boss
notification
4. Write lessons learned
```

Why after Step 1? "Respond" function now has process.
Result: Analysts train on 1 template. No confusion.

Step 3 – Monitoring Use Cases (Week 3) ✓
What: Turn controls into specific SIEM rules

```
ISO 27002 "Log failed logins"
→ SIEM Rule #1 → Detect function
NIST 800-53 "Privileged users"
→ SIEM Rule #2 → Detect function

ISO 27002 "Vendor access"
→ SIEM Rule #3 → Detect function

Result: 50 SMART alerts/day (not 10,000)
```

Why after Step 2? Alerts need predefined "Triage→Escalate" process.
Result: SIEM configured correctly. Analysts triage in 15min.

TABLE V: ISO vs NIST Comparison

Standard	Simple Explanation	Hospital Example	Why Different from NIST
ISO 27035 [12]	5-phase process: Prepare→Identify→Assess →Respond→Learn. Focuses on management/roles (”Who decides? Who documents?”)	”CEO must approve ransomware payment. Document EVERY decision for court.”	NIST 800-61 = technical steps (”run this command”). ISO 27035 = management process (”CISO owns this”).
ISO 27002 [5]	93 practical controls (2022). Recipe book: ”Log failed logins→check every 24h→alert if >5 tries”	SIEM: ”Alert if vendor logs in from Russia” (control 5.10)	NIST 800-53 = 1,100 detailed controls. ISO 27002 = 93 practical examples. Easier for non-US companies.

TABLE VI: NIST CSF 2.0 vs NIST SP 800-61 vs NIST SP 800-53

Document	Level	Purpose	Content	Hospital Use	Key Difference
NIST CSF 2.0	HIGH-LEVEL (like a map)	Organize ALL cybersecurity work into 6 buckets	6 Functions: Govern→Identify→Protect →Detect→Respond →Recover No specific actions, just categories [1]	“SOC does 4 jobs: Watch(Detect), Fight(Respond), Fix(Recover), Report(Govern)”	BIG PICTURE – Says WHAT (functions), not HOW. Flexible for any company.
NIST SP 800-61	MEDIUM-LEVEL (like a playbook)	Handle ONE incident step-by-step	4 Phases: Preparation→Detection/ Analysis→Containment/ Recovery→Post-Incident Only for incidents, not daily work [18]	“Patient records hacked? Follow these 4 steps exactly.”	INCIDENT ONLY – Detailed process for one attack. Lives inside CSF’s ”Respond” function.
NIST SP 800-53	LOW-LEVEL (like a checklist)	Technical controls for systems	1,100+ rules in 20 families: AC-2: “Log all logins” IR-4: “Incident team” AU-6: “Audit review” Every Tiny Detail [3]	“SIEM Rule #47: Alert if nurse uses CEO password”	DETAILED CONTROLS – Every screw and nail. Feeds CSF’s ”Detect” function.

E. TOTAL RESULT: €50k Well Spent

- ✓ 224/7 monitoring (Step 1 Detect)
- ✓ Incidents $<$ 2h (Step 2)
- ✓ 50 alerts/day (Step 3)
- ✓ Laws satisfied (Step 4)
- ✓ Analysts happy, director happy

F. Why Order CANNOT Change (Visual)

```
WRONG:   Laws → ? → ? → ?
         "NIS2 says report! HOW???"

RIGHT:   Functions → Process → Content
       → Laws
Step1     → Step2   → Step3  → Step4
```

Each step is a brick:

- Step 1 = **Foundation** (where SOC lives)
- Step 2 = **Walls** (how handle incidents)
- Step 3 = **Wiring** (what generates alerts)
- Step 4 = **Inspection** (passes code?)

G. NIST CSF 2.0 vs NIST SP 800-61 vs NIST SP 800-53 (Table VI)

Think of NIST documents like kitchen tools:

CSF 2.0 = **MENU** (what dishes to make)
800-61 = **RECIPE** (how to cook one dish)
800-53 = **INGREDIENTS LIST** (every spice, measurement)

Hospital Example – Ransomware hits!

- CSF 2.0: “This goes in **RESPOND** function”
- 800-61: “Step 2: Isolate server. Step 3: Call CISO”
- 800-53: “IR-4: You need incident response team. AU-6: Review logs”

NIST-only: “Great technical process! But who approved actions? No management evidence.” → Fail audit.

NIST + ISO: “Perfect! NIST playbooks + ISO management roles = full coverage.” → Pass audit + certification.

VI. Conclusion

The modern SOC navigates a complementary ecosystem of standards and regulations.

NIST provides technical structure:

- CSF 2.0 organizes functions
- SP 800-61 delivers incident playbooks
- SP 800-53 supplies SIEM controls

ISO ensures management discipline:

- 27035 defines incident roles
- 27002 translates controls into auditable use cases

EU regulations make compliance mandatory:

- **CRA**: Product security (SBOM)

- **NIS2**: Operational cybersecurity (24h reporting)
- **DORA**: Financial resilience
- **GDPR**: Data protection (72h notification)
- **CER**: Physical resilience

The **4-step approach** (CSF→lifecycle→use cases→regulations) delivers operational SOCs that satisfy auditors and regulators.

REFERENCES

[1] NIST, "Cybersecurity Framework (CSF) v2.0," [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.

[2] NIST, "Computer Security Incident Handling Guide (SP 800-61 Rev. 2)," [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2.

[3] NIST, "Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[4] ISO/IEC, "Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)," [Online]. Available: https://www.iso.org/standard/82875.html.

[5] ISO/IEC, "Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022)," [Online]. Available: https://www.iso.org/standard/75652.html.

[6] ISO/IEC, "Information technology – Security techniques – Information security incident management (ISO/IEC 27035 Parts 1-3:2016)," [Online]. Available: https://www.iso.org/standard/60803.html.

[7] European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[8] European Union, "Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679.

[9] European Union, "Digital Operational Resilience Act (DORA)," [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[10] European Commission, "Cyber Resilience Act (CRA)," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[11] European Union, "Critical Entities Resilience Directive (CER)," [Online]. Available: https://www.critical-entities-resilience-directive.com/.

[12] ISO/IEC, "Information security incident management (ISO/IEC 27035)," [Online]. Available: https://www.iso.org/standard/78973.html.

[13] TrustBuilder, "NIS2 DORA Regulations Compliance," [Online]. Available: https://www.trustbuilder.com/en/nis2-dora-regulations-compliance/.

[14] ISACA, "DORA and NIS2: Connection Points and Key Differences," [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/dora-and-nis2-connection-points-and-key-differences.

[15] PayTechLaw, "NIS2 meets DORA: Changes for financial institutions," [Online]. Available: https://paytechlaw.com/en/nis2-meets-dora-changes-for-financial-institutions/.

[16] Key2XS, "The overlap between NIS2 and CER," [Online]. Available: https://key2xs.com/news/the-overlap-between-nis2-and-cer-what-critical-entities-need-to-know.

[17] Ahmad Science, "NIS vs NIS2 vs CER," [Online]. Available: https://ahmad.science/2024/06/28/nis-vs-nis2-vs-cer/.

[18] NIST CSRC, "SP 800-61 Rev. 2," [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final.

[19] activeMind.legal, "NIS2 vs. DORA [Online]. Available: https://www.activemind.legal/guides/nis2-dora/.

[20] Ramboll, "The EU CER Directive: Understand the basics," [Online]. Available: https://www.ramboll.com/insights/resilient-societies-and-liveability/the-eu-cer-directive-understand-the-basics.

[21] NIST, "About NIST," [Online]. Available: https://www.nist.gov/about-nist.

[22] European Union, "NIS2 Directive (EUR-Lex)," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[23] European Union, "GDPR Regulation (EUR-Lex)," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[24] European Union, "Critical Entities Resilience Directive (EUR-Lex)," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[25] European Union, "Digital Operational Resilience Act DORA (EUR-Lex)," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

[26] European Union, "Cyber Resilience Act CRA (EUR-Lex)," [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2353/oj.