# Flare for EU Cybersecurity Regulations

With the help of European cybersecurity compliance experts, we've mapped Flare's Threat Exposure Management and Intelligence solution to three of the most prominent mandates for European busniesses: NIS2, DORA, and CRA. This document is intended to help you understand how Flare can support your organization’s efforts toward aligning with EU cybersecurity regulations. Flare contributes to compliance initiatives but does not replace a full compliance program or guarantee regulatory compliance.

# Network and Information Security Directive 2

flare

NIS2 is an updated EU directive that raises cybersecurity standards across a broad range of essential industries, including energy, healthcare, transport, and public services. It expands the number of organizations required to meet strict security and incident reporting rules, emphasizes managing risks in the supply chain, and improves cooperation between EU countries. This directive aims to create a stronger and more unified approach to cybersecurity across Europe.

| Regulation | Specific Article/Section | Regulation Summary | Aligned Flare Capabilities | Value to the Client | Degree of Alignment |
|---|---|---|---|---|---|
| NIS2 | **Article 21** – Cybersecurity Risk Management Measures | Entities must implement appropriate and proportionate technical and organizational measures to manage cybersecurity risks. | Attack Surface Management, Vulnerability Prioritization, External Threat Exposure Monitoring. | Enables proactive identification and mitigation of cybersecurity risks. | Direct |
| NIS2 | **Article 23** – Reporting Obligations | Entities are required to report significant cybersecurity incidents to relevant authorities within 24 hours. | Alerting and Reporting, External Threat Exposure Monitoring. | Facilitates timely detection and reporting of incidents to comply with regulatory timelines. | Direct |
| NIS2 | **Article 29** – Cybersecurity Information Sharing Arrangements | Promotes sharing of cybersecurity information among entities to enhance collective security. | Threat Intelligence Sharing, External Threat Exposure Monitoring. | Enables clients to have threat intellgience data to share by monitoring their respective threat perimiter. | Loose |
| NIS2 | **Article 22** – Supply Chain Security | Entities must address cybersecurity risks across their supply chains and service providers. | Third Party Monitoring, Data Leak Identification. | Third party monitoring and wider attack surface assesment enable clients to have higher visibility over their supply chain. | Loose |
| NIS2 | **Article 25** – Supervision and Enforcement | Regulators will have powers to supervise and penalize non-compliant entities. | Alerting and Reporting, Identity Intelligence. | Helps clients demonstrate due diligence and proactive monitoring to supervisory bodies. | Loose |
| NIS2 | **Article 28** – Peer Reviews and Coordinated Risk Assessments | EU member states are encouraged to conduct joint reviews and cross-border risk assessments. | Identity Intelligence, External Threat Exposure Monitoring. | Aids clients in contributing to coordinated assessments with up-to-date intelligence. | Loose |
| NIS2 | **Article 20** – Governance and Accountability | Requires management bodies of essential entities to approve and oversee cybersecurity risk management practices. | Reporting, Identity Intelligence. | Supports strategic oversight and reporting for executive stakeholders. | Loose |
| NIS2 | **Article 11** - Technical Requirements of Computer Security Incident Response Teams (CSIRTS) | Outline of the technical requirements for CSIRTS's | External Threat Exposure Monitoring. | Significantly enhances the external attack surface monitoring capacity of CSIRTS. | Direct |
| NIS2 | **Article 15** - Computer Security Incident Response Teams (CSIRTS) Network | The regulation mandates the formation of a pan European network of national CSIRTS. | Attack Surface Management, Vulnerability Prioritization, External Threat Exposure Monitoring. | In order to be in a position to effectively contribute to the confederation of CSIRTS group entities can have extremely well contextualised threat level data. | Loose |

# Digital Operational Resilience Act

DORA is an EU regulation designed to strengthen the financial sector's ability to handle cyber incidents and technology disruptions. It sets consistent rules for how banks, insurers, and other financial entities manage digital risks, report and recover from incidents, test their resilience, and oversee their critical technology providers. The goal is to keep essential financial services running smoothly, even in the face of major cyber threats.

| Regulation | Specific Article/Section | Regulation Summary | Aligned Flare Capabilities | Value to the Client | Degree of Alignment |
|---|---|---|---|---|---|
| DORA | **Article 16** – Simplified ICT (Information and Communication Technology) Risk Management Framework | Provides a simplified ICT (information and communication technology) risk management framework for smaller entities, focusing on essential elements to ensure digital resilience. | Attack Surface Management, Vulnerability Prioritization. | Assists smaller entities in implementing essential ICT risk management practices efficiently. | Loose |
| DORA | **Article 17 (3)** - ICT Related Incident Management Process | The ICT Related incident management process shall put in place early warning indicators. | Attack Surface Management, Threat Intelligence Alerting and Reporting. | Enables the detection and integration of intelligence-led early warning indicators into the risk management process. | Direct |
| DORA | **Article 7** - Content on the voluntary notification of significant cyber threat | The content required to fill a voluntary significant cyber threat report. | Incident Monitoring & Reporting. | Due to the auditable intelligence chain in Flare IO we can enable our clients to more easily access data required to fill a voluntary cyber threat report. | Loose |
| DORA | **Article 8** - Identification | The article places a requirement on entities to assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions. | External Threat Monitoring, Identity Intelligence Dark Web Monitoring, Data Leak Identification, Attack Surface Management. | Flare can directly meet this requirement. | Direct |
| DORA | **Article 13** - Learning and Evolving | Puts a requirement on financial entity to learn and continuously gather information and intelligence regarding vulnerabilities and cyber threats. | External Threat Surface Monitoring, Dark Web Monitoring, Data Leak Identification, Attack Surface Management. | Flare can enhance the knowledge cycle of relevant organizational staff when it comes to real time threat intelligence. | Direct |
| DORA | **Article 45** - Information sharing arrangements on cyber threat information and intelligence | The article establishes protocols how financial institutions may exchange amongst themselves cyber threat information and intelligence. | External Threat Exposure Monitoring. | Clients will have access to high-fidelity intelligence to aid in information sharing efforts. | Loose |
| DORA - Regulatory Technical Standards on Information and Communication Technology Incident Classification | **Article 20** – Governance and Accountability | The regulation outlines in detail how to designate significant cyber threats essentially drilling down into how cyber threats that have a higher probability of impacting certain critical systems should be mapped and awareness around the likelihood should be. | External Threat Exposure Monitoring, Third Party Monitoring, Dark Web Monitoring. | Flare's one of approach to external threat surface management will enable clients to more accurately assess the likelihood of high material impact to critical services. Application of Flare services can showcase to the regulator the validity of the approach. | Loose |

# Digital Operational Resilience Act

flare

| Regulation | Specific Article/Section | Regulation Summary | Aligned Flare Capabilities | Value to the Client | Degree of Alignment |
|---|---|---|---|---|---|
| DORA - Regulatory Technical Standards on Risk Management Framework | **Article 23** - Anomalous activities detection and criteria for ICT related incidents, detection and response | The article establishes specific criteria on how to detect anomalous behaviour. | External Threat Exposure Monitoring | The regulation stipulates the monitoring of internal and external cyber threats and considering scenarios common used by threat actors based on threat intelligence activity. Flare can contribute to the effectiveness of these threat assessments and scenario analysis. | Loose |
| DORA - Regulatory Technical Standards on Risk Management Framework | **Article 27** - Format and content of the report on the review of ICT Risk Management Framework | Outlines the reporting requirements for executive level reporting and levels of approval required. | External Threat Exposure Monitoring, Third Party Monitoring, Identity Intelligence. | Flare's native reporting capabilities are highly granular and includes the abilty to tailor to specific audiences. | Loose |
| DORA - Regulatory Technical Standards on Risk Management Framework | **Article 34** - ICT Operations Security | Defines requirements to monitor cyber threats and have up to date information on all relevant items. | All capabilities | Flare enables robust external threat exposure monitoring. | Loose |
| DORA - Regulatory Technical Standards on Risk Management Framework | **Article 26** - ICT Response and Recovery Plans | Organizations have an obligation to develop scenarios on information around current threats. | All capabilities | Flare can provide essential intelligence for those scenarios. | Direct |
| DORA - Regulatory Technical Standards on Subcontracting ICT Services | **Article 3** - Due diligence and risk assessment regarding use of subcontractors supporting critical or important functions | Organizations are responsible for a number of third party risk categories and one specific one in the risk assessments is ICT Risk. | Third Party Monitoring Vulnerability Prioritization | Flare can be used to monitor the threat exposure of critical service providers. | Loose |
| DORA - Regulatory Technical Standards on Threat Led Penetration Testing | **Article 8** - Preparation Phase | Describes in detail what preparations need to be undertaken in order for TLPT to take place. | All capabilities | Flare is used by pen testing teams globally to accelerate tesing preparation and OSINT. | Direct |
| DORA - Regulatory Technical Standards on Threat Led Penetration Testing | **Article 10** - Testing Phase: Red Team Test | Describes in detail the sequences of the red teaming tests and how they should take place. | All capabilities | Flare can inform threat-lead red teaming exercises. | Loose |

# Cyber Resilience Act (CRA)

The CRA is an EU regulation that ensures digital products—such as connected devices and software—are designed and maintained with cybersecurity in mind. It requires manufacturers and distributors to follow secure-by-design principles, fix vulnerabilities promptly, and provide long-term security updates. The regulation helps reduce systemic risks from insecure technology products and builds greater trust in the connected devices people and businesses rely on.

| Regulation | Specific Article/Section | Regulation Summary | Aligned Flare Capabilities | Value to the Client | Degree of Alignment |
|---|---|---|---|---|---|
| EU Cyber Resilience Act | **Annex I, Section 1** | Establishes essential cybersecurity requirements for products with digital elements, including secure design and development. | Vulnerability Prioritization, Attack Surface Management. | Enables active vulnerability scanning and maintaining of a comprehensive vulnerability register for the organization at hand. | Direct |
| EU Cyber Resilience Act | **Annex I, Section 2** | Requires manufacturers to have processes for handling vulnerabilities, including coordinated disclosure. | Dark Web Monitoring, Identity Intelligence. | Enables active vulnerability scanning and maintaining of a comprehensive vulnerability register for the organization at hand. | Direct |
| EU Cyber Resilience Act | **Article 11** | Mandates reporting of actively exploited vulnerabilities and incidents within specified timeframes. | Alerting and Reporting, External Threat Exposure Monitoring. | Provides clients with an additional landscape scanning tool in order to develop an intellgience lead threat based understanding of the actively explouted vulnerabilities in a certain perimiter. | Loose |
| EU Cyber Resilience Act | **Article 10** | Requires manufacturers to conduct cybersecurity risk assessments for their products. | Attack Surface Management, Vulnerability Prioritization. | Provides active intellgience in regard to the definition and risk profiling of an threat surface. | Direct |
| EU Cyber Resilience Act | **Article 12** | Obligates manufacturers to provide security updates and inform users about vulnerabilities. | Alerting and Reporting. | Assists clients in maintaining a register of threat awarness in order to in advance inform users about active threats. | Loose |