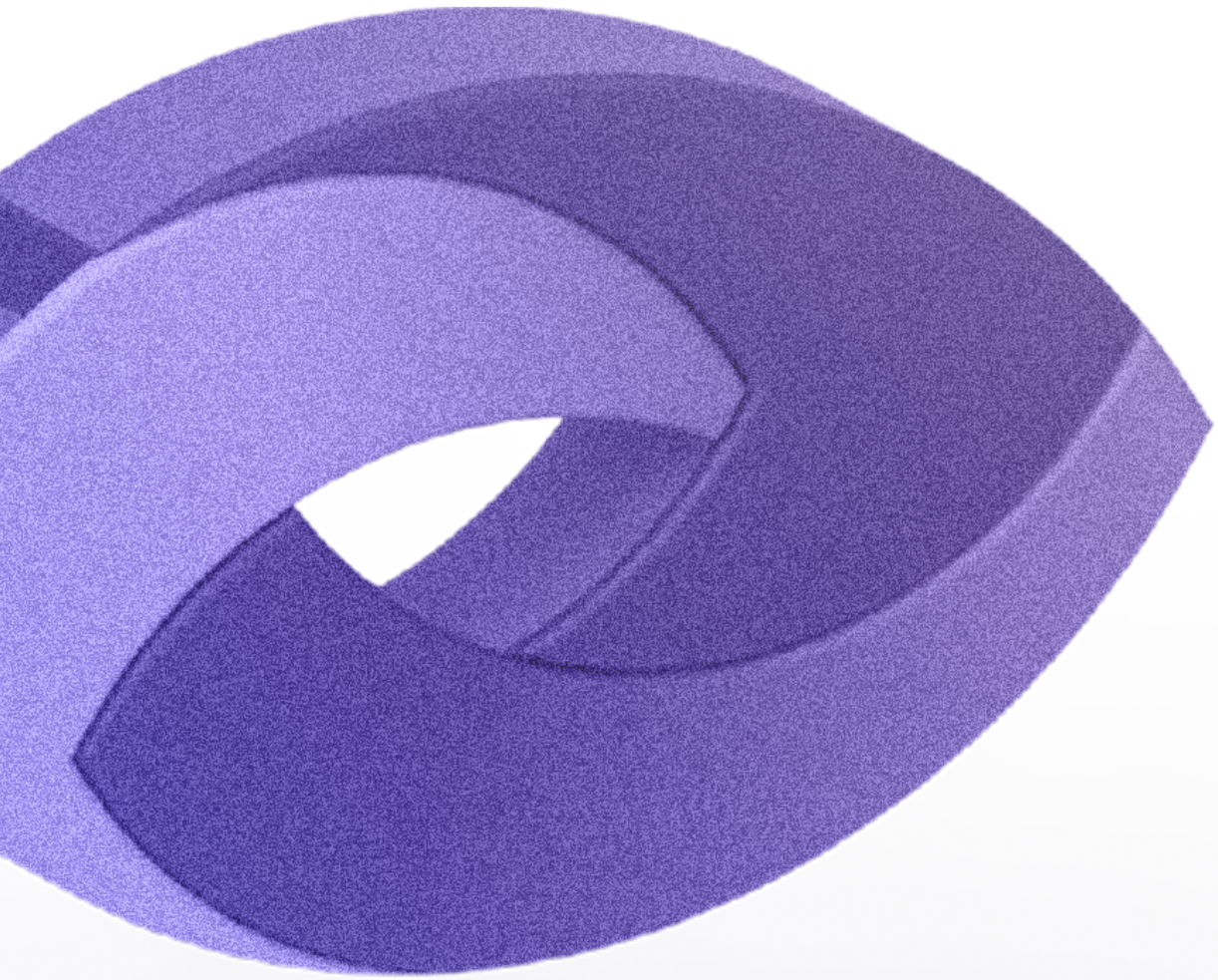
FS-ISAC

DORA Information Sharing Requirements and FS-ISAC Membership



September 2024

The European Union Parliament's Digital Operational Resilience Act (DORA)[1] aims to harmonize digital resilience regulations in five key areas throughout the EU. Each EU nation's financial services regulators apply the DORA regulation, and most financial services institutions will have to be in compliance by 17 January 2025.

One of the five areas of DORA regulation concerns sharing cyberthreat information and intelligence. This regulation – Article 45, "Information sharing arrangements" – requires European financial institutions to share indicators of compromise, adversaries' tactics, techniques, and procedures, cybersecurity alerts, and configuration tools in a safe, secure, and trusted manner.

Membership in FS-ISAC – the only global cyber-intelligence sharing community with a secure platform solely focused on financial services – enables members to meet those requirements and fulfill the conditions set out in DORA Article 45 if they use FS-ISAC offerings to share information and intelligence.

The following table shows how FS-ISAC membership meets Article 45 requirements. Importantly, members can use this table and other pertinent membership details to demonstrate to competent authorities and regulators how they meet the requirements of Article 45.

DORA Pillars

ICT risk management	Articles 5-16
ICT-related incident management, classification, and reporting	Articles 17-23
Digital operational resilience testing	Articles 24-27
Management of ICT third-party risk and Oversight Framework of critical ICT third-party service providers	Articles 28-44
Information sharing arrangements	Article 45

1 https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Table 1 - DORA Article 45 and FS-ISAC Membership

DORA clause	DORA requirement	FS-ISAC Offering
Article 45.1	Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:	The exchange of cyberthreat information and intelligence is a key aim and role of FS-ISAC. FS-ISAC is a non-profit financial services industry consortium and is the only global cyber-intelligence sharing community solely focused on financial services.
45.1a	aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;	▶ FS-ISAC, its members, and financial services critical infrastructure strategic partners developed the voluntary FS-ISAC All-Hazards Framework to guide how the financial sector uses trusted information sharing to evaluate and respond to all-hazards events, share situational awareness and analysis, and coordinate with government and other partners. The overall goal is to enhance financial sector resilience. ▶ Regular Threat Briefing calls curated by FS-ISAC intelligence analysts, leading security experts, and public-private partners that provide members with information about regional and global threats and trends applying to the financial services sector. ▶ Threat reports, including: > STIX/TAXII and MISP Automated Feeds > Daily Reports > Weekly Watch Report > Bi-Monthly Threat Trends Report > Technical Analysis Reports > Spotlight Reports > Generic Threat Landscape Report > Cyber Threat Review for Security Testers > Annual Review > Monthly Member Sharing Metrics

45.1b	takes places within trusted communities of financial entities;	FS-ISAC is a global community from the private and public sectors that shares best practices in a trusted environment. Members connect with industry experts, build stronger relationships, and receive original, curated thought leadership through live events, communities of interest, member viewpoints, and webinars on current topics.
45.1c	is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy.	FS-ISAC uses a trust model that includes the Traffic Light Protocol (TLP) to share information. Unless otherwise specified, this strict information handling procedure treats all information as confidential and will not disclose it to parties outside of FS-ISAC without the permission of the originator.
45.2	For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which they may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.	The FS-ISAC trust model defines conditions for information-sharing arrangements, conditions for participation, involvement of public authorities, and ICT third-party service providers. Dedicated and protected IT platforms are used for information-sharing, including: ▶ **Share,** a member intelligence sharing application that focuses on customization, automation, and three levels of intelligence: tactical, operational, and strategic. ▶ **Connect,** an encrypted chat platform that provides a secure closed environment for members to collaborate.
45.3	Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once it takes effect.	FS-ISAC membership details can be submitted to competent authorities to show that Article 45 requirements are being met.

Beyond fulfilling DORA Article 45 requirements, FS-ISAC helps and supports members with its DORA Working Group. Members exchange advice and best practices to address DORA and its challenges, and understand and comply with its requirements. The Working Group also releases publications that help the entire financial sector become compliant with DORA. If an FS-ISAC member firm wishes to join the DORA Working Group, please email FS-ISAC Member Services at memberquestions@fsisac.com.

Contact

fsisac.com

For media requests, please contact
media@fsisac.com