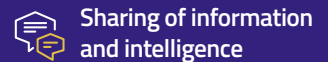
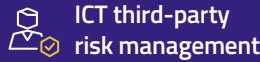


Achieve DORA Compliance with SecurityScorecard

The Digital Operational Resilience Act (DORA) was introduced to protect financial companies and their partners or providers from major information and communication technology (ICT) risks.



SecurityScorecard offers a comprehensive solution for adhering to all major aspects of DORA, enabling your organization to minimize ICT risk exposures, build a resilient digital supply chain, and avoid non-compliance penalties.

ICT Risk Management

REQUIREMENT

Financial entities must have internal governance and control frameworks that ensure effective and prudent management of all ICT risks to bring about a high level of digital operational resilience.

SOLUTION

SecurityScorecard provides the industry's most comprehensive Enterprise Cyber Risk Management solution that allows you to spot vulnerabilities and better prevent cyberattacks from happening.

You can:

- Gain a complete view of how the adversary sees your attack surface
- Investigate vulnerabilities further to drive actionable next steps
- Prioritize remediation by the biggest impact on your business
- Hunt for potential threats like a hacker does
- Demonstrate the ROI of security initiatives to the Board and key stakeholders

ICT-related Incident Reporting

REQUIREMENT

DORA requires financial entities to implement a process for notifying regulators of ICT-related incidents, sometimes within hours of detection, with a set of specific criteria including number of users affected, criticality and impact on systems, and a view of actual costs and loss due to the incident.

SOLUTION

SecurityScorecard offers direct access to highly-skilled and elite incident response experts who are standing by and ready to support your organization with triaging, recovering from, and responding to cyber incidents.

You can:

- Discover indicators of compromise (IOCs) that can trigger reporting requirements
- Quickly identify the cause of incidents to prevent further loss
- Collect, analyze, and preserve evidence to document the events that led to the incident

Digital Operational Resilience Testing

REQUIREMENT

DORA introduces the principles of a comprehensive testing program that assesses and identifies weaknesses, deficiencies, or gaps in your digital operational resilience with requirements that tests be performed by independent evaluators every three years.

SOLUTION

SecurityScorecard helps make your organization cyber resilient with a range of proactive services that battle-test your security controls, identify gaps in your attack surface, and enhance your ability to defend against cyberattacks.

You can:

- Test the effectiveness of your security controls while achieving compliance and protecting your brand
- Practice your incident response skills and identify gaps in your incident response plan
- Perform simulated real-life cyber attacks against your own organization

ICT Third-party Risk Management

REQUIREMENT

DORA mandates management of third-party cyber risks and defines a set of key principles for financial entities to achieve sound management and robust contractual relationships with ICT third-party service providers.

SOLUTION

SecurityScorecard provides the industry's most flexible third-party risk management solution, allowing quick and accurate control of risk across your entire digital ecosystem, including third parties and supply chains.

You can:

- Gain continuous visibility of your entire third-party ecosystem
- Quickly validate a vendor's adherence to security standards
- Prioritize where you need to mitigate risks with your third parties

Information Sharing

REQUIREMENT

DORA promotes information-sharing arrangements among financial entities for raising awareness of cyber threat information and intelligence, including indicators of compromise, tactics, and cyber security alerts.

SOLUTION

SecurityScorecard collaborates with industry groups to help their members understand and secure their environments, the suppliers and vendors they rely on to run their businesses, and the collective supply chains they form.

You can:

- Implement a shared framework for measuring the exposure to ICT risks across an industry

The SecurityScorecard Advantage

Create a stronger ecosystem

12M+ companies rated and the largest security ratings contributory network

Gain visibility of your attack surface

Comprehensive data collection from network data to open source repositories and public cloud infrastructures

Reduce operational costs

Streamlined workflows across the cyber risk lifecycle with rules-based automation and over 90 integrations to extend the value of your existing investments

Make informed decisions

Transparent and accurate security ratings platform with expert-led and proactive incident response services

How SecurityScorecard can help

SecurityScorecard is the trusted, must-have standard for measuring cybersecurity, with over 12 million companies continuously rated. Our platform offers a comprehensive solution covering all major aspects of DORA, including ICT risk management, resilience testing, incident reporting, and third-party risk management. Organizations are empowered to identify and mitigate risks before they become incidents, and with continuous monitoring and vendor risk management, businesses can stay informed about potential threats and vulnerabilities.

Instantly measure your security risks, know what to do next, and who to call.
VISIT SECURITYSCORECARD.COM

GET STARTED



SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166



©2023 SecurityScorecard Inc. All Rights Reserved.