Simplify and Automate DORA TPRM Requirements with SecurityScorecard

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

140 Avenue of
the Americas, Floor 19,
NY, NY 10036
1.800.682.1707

Executive Summary

The **Digital Operational Resilience Act (DORA)** is a comprehensive set of regulations adopted by the European Union (EU) to enhance the operational resilience of the financial sector in the face of increasing ICT risks. DORA aims to standardize the way financial entities manage ICT-related risks and ensure that they have the necessary capabilities to withstand and recover from cyber-attacks, IT disruptions, and other operational failures. Organizations must comply with DORA's requirements by January 17, 2025.

The regulation focuses on:

- **Risk management:** It mandates organizations to implement comprehensive risk management frameworks, including identifying and assessing ICT risks, implementing controls to mitigate these risks, and regularly testing the effectiveness of these controls.

- **ICT incident management:** DORA requires financial entities to establish robust processes for ICT incident management, encompassing incident detection, response, and reporting. Organizations need to define roles and responsibilities, establish communication protocols, and conduct regular testing to ensure their incident response capabilities are adequate.

- **Testing:** The act emphasizes the importance of regular testing, including penetration testing, vulnerability assessments, and business continuity and disaster recovery exercises, to verify the resilience of systems and processes.

- **Third-Party Risk Management (TPRM):** DORA places significant emphasis on managing third-party ICT service providers. Organizations must conduct thorough risk assessments, incorporate DORA TPRM requirements into contracts, and continuously monitor the security posture of their third parties.

SecurityScorecard simplifies and streamlines DORA TPRM compliance by automating processes and providing valuable insights. This document outlines key DORA TPRM requirements, along with SecurityScorecard's capabilities, to operationalize SecurityScorecard to support DORA compliance and enhance operational resilience.

DORA TPRM Requirements

1. Risk Identification and Assessment

1.1 Identify all third-party ICT service providers.

DORA requires a comprehensive inventory of all third-party ICT service providers, including those that process, store, or access sensitive data or critical services.

SecurityScorecard simplifies this process with:

- **Bulk Company Import**: Allows quick addition of companies via CSV files for organizations without available integrations.
- **Automatic Vendor Detection (AVD)**: AI-driven analytics identify hidden or unknown third- and fourth-party providers, uncovering vendors missed by traditional methods or existing vendor inventory.
- **Pre-Built Integrations and REST API**: Over 90 integrations with popular GRC solutions and a robust REST API to fetch data from existing systems.

By combining these capabilities, organizations gain a complete and accurate view of their third-party ecosystem, ensuring effective TPRM and DORA compliance.

1.2 Classify third-party ICT service providers based on their criticality to the organization.

DORA requires organizations to classify third-party ICT service providers based on their criticality. SecurityScorecard supports this process with a four-factor vendor risk tiering system, enabling classification of third-parties as low, moderate, high, or critical.

SecurityScorecard helps on classification through:

- **Seamless Data Integration:** Using data import, API, and integrations with existing GRC or inventory tools, organizations can automate classification based on factors like business impact, revenue, volume or data types shared.
- **Security Ratings:** An outside-in view of third-party security postures to assess inherent risk.
- **Portfolio Grouping:** Portfolios are used for grouping vendors by criticality or other criteria, enabling aggregated risk overviews and customized tier-based reporting.
- **Questionnaire Assessments:** Questionnaires can be used to collect evidence and context helping to assess vendor's cyber maturity, overall risk or access to sensitive data or services.

Once classified, organizations can tailor risk management and oversight to focus on critical vendors, ensuring a risk-based approach that aligns with DORA's TPRM requirements and bolsters operational resilience.

1.3 Conduct risk assessments for all third-party ICT service providers.

The assessments should evaluate the security controls and processes of third parties, and should be tailored to the specific risks posed by each provider.

SecurityScorecard simplifies this process with:

1.3.1 Cyber Security Ratings

SecurityScorecard provides a non-intrusive, outside-in methodology for evaluating organizations' security profiles, measuring and updating cybersecurity ratings daily on millions of organizations globally. SecurityScorecard assigns an easy-to-understand A-F letter grade and a numerical score (0-100) for each organization.

Key Features of Cyber Security Ratings:

- **Ten Risk Factor Groups:** SecurityScorecard calculates and provides reports on ten different factor scores to describe different aspects of cyber risk.
- **Issue Type Weights:** Issue types within each factor are weighted based on their relative breach risk to calculate the total score.
- **Daily Updates:** Maintaining a regular scoring update cadence enables SecurityScorecard to preserve fair cybersecurity risk ratings in a dynamic threat environment.
- **Industry Comparisons:** SecurityScorecard assigns each scored organization an industry tag, enabling comparisons of security posture within and across industries.

1.3.2 Automatic Compliance Validation

SecurityScorecard can validate companies against defined criteria such as their main score, factor scores, historical scoring stability, and the amount of findings by severity. Companies can also be compared against various industry standards, such as ISO, NIST, CSA, CIS, DORA, SOC and PCI. Custom Compliance frameworks can be built to validate companies against customer's preferred criteria, e.g. contractual security requirements and clauses.

1.3.3 Evidence Locker

Suppliers can upload evidence, such as certifications, privacy policies, and penetration test results, into their Evidence Locker. They can define whether those artifacts are visible to all or selectively to defined users. If a supplier has not yet uploaded the needed evidence, a request can be made to get those included.

1.3.4 Questionnaire Assessments

SecurityScorecard scales up and simplifies the traditional questionnaire assessment process by automating the workflow.

Key Features of Questionnaire Assessments

- **Automated Workflow:** Workflow for sending, following up, reviewing, assessing and reporting on questionnaires.
- **Customizable Questionnaires**: Pre-built and customizable templates and conditional questionnaires allow organizations to tailor assessments to industries, regulations, and risk profiles, ensuring relevance to the vendor's services and risk appetite.
- **Smart Mapping Engine**: Automatically validates questionnaire responses against SecurityScorecard's security ratings data, delivering comprehensive and objective risk assessments while reducing effort and time.
- **Smart Answers:** Use existing documentation such as previously completed questionnaires or certification documents to auto-fill questionnaire responses accelerating the assessment turnaround time.
- **AI Assisted Questionnaire Review** (coming in 2025): Leverage certifications, contracts, and documents to validate assessment responses, minimizing the need for traditional human performed reviews and further streamlining the process.

These capabilities enable organizations to efficiently assess large numbers of vendors while maintaining accuracy and relevance.

1.4 Document the results of risk assessments and develop risk mitigation plans.

DORA requires organizations to document the results of risk assessments and develop, communicate and track risk mitigation plans, including identifying and implementing appropriate controls to address identified risks.

SecurityScorecard supports organizations in documenting risk assessment results and developing effective risk mitigation plans through:

- **Assessment Findings Report:** Assessment findings report can be created to describe any identified risks, policy or contractual violations, remediation actions agreed or other notable findings that may affect the assessment acceptance of the supplier. Currently Assessment Findings reports are tied to sent questionnaires, bu during H1/2025, the service will support a combined assessment report of Ratings, Questionnaires, Evidences, Policy violations etc.
- **Customizable Reporting**: A robust reporting center with customizable templates provides insights into vendor security posture, including ratings, risk factor scores, and

specific findings. Reports can be exported in formats like PDF, CSV and JSON, enabling easy sharing with stakeholders and tracking progress over time.

- **Evidence Locker and Document Center**: Centralized repositories to store and manage vendor documentation, such as questionnaires, contracts, and certifications. This feature streamlines access to relevant information for auditors and regulators.
- **Action Plans**: Create targeted remediation plans with specific tasks, deadlines, and responsible parties. Progress tracking and direct vendor communication ensure efficient collaboration to address security gaps and enhance the third-party ecosystem.
- **Risk Mitigation Recommendations**: Automated recommendations based on identified vulnerabilities help prioritize remediation efforts. These insights can be integrated into action plans to develop comprehensive mitigation strategies.

By leveraging these tools, organizations can effectively document risk assessments, implement actionable mitigation plans, and meet DORA requirements for managing third-party ICT service provider assessments.

2. Contractual Management

2.1 Incorporate DORA TPRM requirements into contracts with third-party ICT service providers.

Integrating DORA TPRM requirements into contracts ensures third-party ICT providers are contractually obligated to meet necessary security and resilience standards.

SecurityScorecard supports this by providing actionable data through APIs and integrations, enabling seamless integration with contract management systems to streamline compliance and oversight.

2.2 Monitor compliance with contractual requirements.

Monitoring third-party ICT providers includes tracking their performance and ensuring adherence to agreed-upon security and resilience standards.

SecurityScorecard simplifies compliance monitoring through:

- **Custom Compliance Frameworks**: Organizations can create frameworks based on contractual security requirements, enabling tracking, validation, and identification of non-compliance. The platform flags conflicting findings for easy reporting and enforcement.
- **Continuous Monitoring**: SecurityScorecard continuously monitors vendor security postures and alerts organizations to changes that may impact compliance, such as

vulnerabilities, breaches, suspicious activity, or shifts in security ratings. This proactive approach helps mitigate potential compliance issues before escalation.

- **Portfolio Policies** *(available in 2025)*: Portfolio Policies allows organizations to define supplier tiering policies based on contractual requirements and continuously monitor security postures, documents, certifications, and assessments to ensure suppliers meet the defined security standards.

These capabilities provide a comprehensive approach to ensuring third-party compliance with contractual obligations and maintaining organizational resilience.

2.3 Review and update contracts regularly.

DORA mandates that contracts stay aligned with evolving TPRM requirements and the changing risk landscape.

SecurityScorecard's Document Center, enhanced with AI/LLM-powered contract validation (launching in 2025), ensures contracts remain up-to-date with current security risks, certifications, and resiliency standards, enabling a proactive compliance approach.

3. Continuous Monitoring and Oversight

3.1 Continuously monitor the security posture of third-party ICT service providers.

DORA requires organizations to continuously monitor the security posture of third-party ICT service providers to ensure ongoing compliance with security and resilience requirements. This includes monitoring for emerging risks, vulnerabilities, and incidents that could impact the continuity and security of critical services. The goal is to identify and address potential threats or weaknesses promptly, ensuring that third-party providers maintain a security posture aligned with the organization's standards and regulatory obligations.

SecurityScorecard provides robust features to support continuous monitoring of third-party ICT providers, including:

- **Continuous Monitoring**: SecurityScorecard leverages continuous active and passive data collection to monitor vendors' cybersecurity postures across more than 200 security issues. This is further enriched by threat intelligence feeds, which provide insights into emerging threats, zero-day vulnerabilities, malware, threat actors, and breaches, ensuring organizations stay ahead of emerging risks.
- **Real-time Alerting**: Customizable alert rules for events like score drops, new findings, CVEs, or breaches or incidents, tailored to organizational needs. Alerts can be seamlessly connected with GRC, SIEM, and ITSM tools to streamline workflows and

centralize alerts.

- **Vendor Collaboration, Remediation and Tracking**: Action Plans and Alerts are used to manage and notify suppliers about identified risks or vulnerabilities, form remediation plans and track the remediation progress to drive timely resolution.

These features enable organizations to proactively monitor third-party security, quickly address risks, and maintain compliance with DORA’s focus on operational resilience and continuous oversight.

3.2 Establish processes for incident management and response.

Incident management requirements of DORA require clear roles, responsibilities, communication protocols, and escalation procedures.

SecurityScorecard supports these processes through continuous monitoring, alerting, and collaboration features. Alerts can be integrated with automated questionnaire workflows to gather additional context and information from vendors during an incident, streamlining communication and escalation efforts.

3.3 Conduct regular testing of third-party ICT service providers.

Regular testing, such as penetration testing, vulnerability assessments, and disaster recovery tests, is essential to ensure third-party resilience.

SecurityScorecard supports these efforts with:

- **Continuous Vulnerability Assessments**: Identify and prioritize remediation efforts while tracking vulnerability management progress. Results can guide deeper penetration testing or targeted assessments.
- **Customizable Assessment Questionnaires**: Collect evidence and assess supplier compliance with security standards, policies, and best practices.
- **Professional Services**: Offer penetration testing and real-world incident simulations to evaluate vendor preparedness for disruptions.

These tools and services help ensure thorough and effective testing of third-party ICT providers.

3.4 Maintain a central repository for all third-party-related documentation.

The register of information under DORA is a standardized central database that records all contractual agreements of a financial company with ICT third-party service providers. It contains detailed information about the ICT services utilized, the providers, and the supported business and operational functions. The register enables systematic monitoring of dependencies and risks arising from the use of ICT third-party providers and serves to provide this information to the relevant supervisory authorities. It encompasses all ICT services; however, particularly critical or important functions must be listed in more detail.

SecurityScorecard provides a centralized platform for managing third-party documentation and risk assessments, aligning with DORA's operational resilience principles.

Key features include:

- **Central Document Repository (Document Center)**: Store and manage vendor contracts, questionnaire assessments, incident reports, due diligence documents, certifications, policies and other relevant documentation with advanced search and tagging capabilities. Documents can be easily shared with the vendors in question. Future versions will enable AI/LLM based document validation, gap analysis and executive summaries.
- **Vendor System of Record**: Add customer specific context to vendor records, such as business impacts, risk levels, data types shared, business units, lifecycle status, contact details and contract dates.
- **Evidence Locker**: A functionality for vendors to add and manage their own compliance documentation ensuring readiness for audits, regulatory requirements and vendor assessments..

Benefits for maintaining a DORA-compliant Register of Information:

- Consolidated access to all vendor-related information as a single source of truth.
- Enhanced visibility into third-party risks and compliance.
- Streamlined audits and regulatory processes.
- Improved collaboration and communication across stakeholders.
- Readily available documentation for incident response and critical activities.

SecurityScorecard's platform reduces the complexity of managing third-party documentation, improving efficiency and effectiveness in meeting DORA's TPRM requirements.

3.5 Report on TPRM activities to senior management and the board of directors.

Reporting to senior management and the board involves updates on the organization's TPRM posture, key risks, mitigation plans, and third-party ICT provider performance.

SecurityScorecard supports these efforts with:

- **Board Trends Reports**: Provide real-time executive insights, compliance tracking, and competitive benchmarking of the organizations themselves as well as their third-party landscape.

- **Customizable Reporting Templates**: Pre-built and customizable templates tailored for Board of Directors, CISOs, Vendor Risk Managers and technical teams, exportable in formats such as PDF, CSV and JSON.
- **Reporting Dashboards**: Track KPIs, monitor trends, and visualize TPRM posture, key risks, and third-party performance.
- **Cyber Risk Quantification:** Cyber Risk Quantification dashboard and reports can also quantify companies' cyber risks in financial terms.

These reporting capabilities help organizations demonstrate TPRM program effectiveness, align with business goals, and prove compliance with DORA's requirements.

1.1 Identify All Third-Party ICT Service Providers

1.1.1 Start with Bulk Company Import in SecurityScorecard

The fastest way to get started with SecurityScorecard is to use the bulk company import feature:

1. **Export Your Supplier List:** Begin by exporting a complete list of your suppliers, or focus specifically on ICT service providers within the DORA scope, from existing sources such as CRM, GRC, or procurement applications.
   - Ensure the export is in a **CSV** or **spreadsheet** format for easy data conversion.
2. **Include Key Information:** The export file should have a column for the company domain or website to reliably import all companies. If domain information isn't available, include at least the company name.
   - You can also add additional attributes, such as internal and supplier contact emails, business impact, risk level, data types shared, business unit, and custom tags.
   - For a full list of available attributes, download the **bulk upload template** from SecurityScorecard (navigate to: *Portfolios → All Companies → Add Companies → Bulk Import → Download Template*).
3. **Prepare the Export File for Upload:** Convert the columns in your exported file to match the template columns in the SecurityScorecard bulk upload file. Once the data has been formatted correctly, you can upload the supplier list into SecurityScorecard by following the steps: *Portfolios → All Companies → Add Companies → Bulk Import*.

1.1.2 Use SecurityScorecard AVD (Automatic Vendor Detection)

SecurityScorecard's Automatic Vendor Detection (AVD) feature helps identify third-party suppliers automatically. Here's how you can use it:

1. **Review the AVD List:** Check the list of third-party suppliers that SecurityScorecard has automatically detected.
2. **Validate the List:** Verify if there are any unknown suppliers or missing companies that weren't included in your imported data set.
3. **Import Remaining Companies:** You can directly import any remaining suppliers from the AVD view to ensure your supplier list is complete.

1.1.3 Explore Integrations and REST API

Once SecurityScorecard is set up and running, consider integrating it with your existing Third-Party Risk Management (TPRM) processes and tools:

1. **Check the SecurityScorecard MarketPlace:** Explore the ready-made integration plugins available in the SecurityScorecard MarketPlace (*Automation → Integrations*). These plugins provide seamless integrations with common tools such as GRC, SIEM, ITSM, and collaboration platforms.

2. **Enhance Your TPRM Process:** By integrating SecurityScorecard with your existing tools, you can automate workflows, streamline risk assessments, and improve overall efficiency in your TPRM processes.
3. **Utilize the REST API:** For more customized integrations, you can leverage the SecurityScorecard REST API to connect with your internal systems and build tailored solutions that fit your organization's needs.

1.2 Classify third-party ICT service providers based on their criticality to the organization.

1.2.1 Use Existing Classification

If you have an existing supplier classification from tools like CRM, GRC, or procurement applications, you can apply it directly in SecurityScorecard by using the **Business Impact** attribute during the bulk upload process.

When determining the business impact classification, consider several factors:

- The type of data the supplier can access.
- The type of services the supplier manages.
- The size of the contract.
- The potential monetary or operational risk in case of business disruptions.

1.2.2 Use SecurityScorecard for Classification

You can also classify suppliers directly within SecurityScorecard by using the following methods:

1. **Questionnaires:** Create and send a short pre-assessment questionnaire to suppliers. The questionnaire can help assess the business impact based on criteria such as data access, service types, cybersecurity policies, certifications, or maturity level.
2. **Security Ratings:** Use SecurityScorecard's rating scores and data points to evaluate suppliers. Factors like recent breaches, significant rating declines, and malware or ransomware findings can serve as classification criteria.
    - You can filter the **All Companies** view by these criteria and assign attributes in bulk to streamline the process.

1.2.3 Group Companies into Portfolios

To better manage your suppliers, group them into **portfolios** within SecurityScorecard. Portfolios allow you to segment suppliers based on different criteria, such as:

- **Business Impact or Tiering:** Classify suppliers based on their criticality to your organization.
- **Supplier Type:** Group suppliers by the type of services they provide.
- **Business Unit Ownership:** Organize suppliers based on the business unit responsible for managing them.

By grouping suppliers into portfolios, you can:

- Get an aggregated risk overview.
- Perform assessments and continuous monitoring.
- Receive alerts and generate reports based on your defined criteria.

1.3 Conduct Risk Assessments for All Third-Party ICT Service Providers

1.3.1 Perform a High-Level Third-Party Landscape Assessment Using Portfolios

Start by reviewing your third-party ecosystem at a high level, using Portfolios to identify overall risk and prioritize further assessments. Key features include:

- **Overview**
  - Displays a consolidated view of the average portfolio risk rating, grade distribution, and the most common or critical issues.
  - Highlights companies with the lowest or declining ratings to guide deeper evaluation.
  - Uses scatter plot chart to visualize the portfolio status
- **Vendor Detection**
  - Leverages Automatic Vendor Detection (AVD) across all portfolio companies to aggregate fourth-party data.
  - Identifies widely used but potentially risky vendors throughout your supply chain.
- **Supply Chain Risk Intelligence (SCRI)**
  - Connects portfolio companies with threat intelligence to assess risk in five scenarios:
    1. **Infections** (e.g., malware, ransomware)
    2. **Vulnerabilities** (critical, weaponized CVEs)
    3. **Breaches**
    4. **High-Risk Products** (critical or zero-day vulnerabilities)
    5. **Cloud Exposure** (cloud providers, regions, countries)

Using these portfolio insights, you can quickly pinpoint areas of concern and direct more comprehensive assessments where they're needed most.

1.3.2 Company-Based Risk Assessment

Access detailed company information by selecting a company in the portfolio view or using the top search bar.

1.3.2.1 Security Ratings-Based Assessment
The **Company Overview** page consolidates key rating criteria into a single view, including:

- **Overall Rating and Trend**: Historical scoring, stability, and improvements or declines
- **Recent Breaches or Incidents**: Indications of security events affecting the company
- **Certifications and Documents**: Items stored in the Evidence Locker
- **Questionnaire Assessments**: Current or completed evaluations
- **High-Risk Score Factors**: Issue types by breach risk

From the overview, or via the right-hand navigation menu, you can dive into each area for more detail. Common validation criteria might include:

- **Minimum Score Requirements** (e.g., a B or better overall and C or better for each factor)
- **No High-Breach Risk Issues**
- **No Recent breaches or incidents**
- **Stable or Improving Scoring History**

Additional considerations include:

- **Vendor Detection**: An AVD-based supply chain assessment of the company
- **Hierarchy**: Ratings of any subsidiaries or parent companies.

1.3.2.2 Automated Compliance Validation

Once Ratings data points are assessed and validated, the next step is to check the company against defined compliance frameworks. SecurityScorecard supports popular frameworks by mapping automatically collected Ratings signals to each framework.

- **Accessing Compliance Validation**:
  - Click **Start Initial Assessment** on the Company Overview page, or
  - Select **Compliance** in the right-hand navigation menu.
- **Selecting Frameworks**:
  - On your first visit, click **Select Framework** to choose the frameworks you want to validate. Ready made frameworks include standards such as CSA, CIS, ISO 27001, PCI, NIST, DORA
  - Future visits will automatically show your previously selected frameworks.
- **Interpreting Compliance Results**:
  - Each framework displays as a series of **dots** (white, blue, or red) representing compliance requirements.
  - **White**: No automatically gathered data or submitted evidence for that requirement.
  - **Blue**: Matching signals exist with **no conflicts**.
  - **Red**: Conflicting findings detected by SecurityScorecard.
- **Detailed View**:
  - Click the framework name to review specific requirements, relevant findings, and any conflicts.

As the compliance validation covers the company's entire attack surface, a conflicting finding may not necessarily mean the company is non-compliant with the selected framework. For instance, the finding could involve an asset or service outside the certified scope. However, the automated validation provides a rapid overall assessment, and a higher number of red (conflicting) signals typically indicates a greater likelihood of non-compliance.