Simplify and Automate NIS 2 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 Network and Information Systems Directive (NIS 2) is a comprehensive set of regulations adopted by the European Union (EU) to enhance the cybersecurity resilience of critical sectors in the face of increasing ICT risks. NIS 2 aims to standardize how organizations across essential industries manage ICT-related risks and ensure they have the necessary capabilities to withstand and recover from cyber-attacks, IT disruptions, and other cybersecurity-related incidents. Organizations must comply with NIS 2's requirements by October 17, 2024.

The NIS 2 Directive focuses on strengthening cybersecurity and resilience across essential sectors, including energy, transport, healthcare, and more, with a special emphasis on third-party risk management in network and information systems.

The regulation emphasizes the following areas:

- **Risk Management:** NIS 2 mandates organizations to implement comprehensive cybersecurity risk management frameworks, including identifying and assessing ICT risks, implementing controls to mitigate these risks, and regularly testing the effectiveness of these controls.
- **ICT Cybersecurity Incident Management:** NIS 2 requires organizations to establish robust processes for ICT cybersecurity incident management, including 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:** NIS 2 stresses the importance of regular testing to verify the resilience of network and information systems, including penetration testing, vulnerability assessments, and cybersecurity continuity and disaster recovery exercises.
- **Third-Party Risk Management (TPRM):** NIS 2 places significant emphasis on managing critical third-party suppliers. Organizations must conduct thorough cybersecurity risk assessments, incorporate NIS 2 TPRM requirements into contracts, and continuously monitor the security posture of their third parties.

SecurityScorecard simplifies and streamlines NIS 2 TPRM compliance by automating processes and providing valuable insights. This document outlines key NIS 2 TPRM requirements, along with SecurityScorecard's capabilities, to operationalize SecurityScorecard and support NIS 2 compliance and enhance cybersecurity resilience.

NIS 2 TPRM Requirements

1. Cybersecurity Risk Identification and Management for Third Parties

1.1 Identify all critical third-party suppliers.

NIS 2 requires organizations to identify and maintain a comprehensive inventory of critical third-party suppliers, including those who provide essential services, manage critical infrastructure, or have access to sensitive data. This identification process ensures that organizations can assess the cybersecurity risks posed by these suppliers and ensure their resilience in the face of emerging threats.

SecurityScorecard simplifies and streamlines this process with:

- **Bulk Company Import:** Allows quick addition of companies via CSV files for organizations without available integrations, helping organizations efficiently build a comprehensive third-party inventory from scratch.
- **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 inventories. This is critical for identifying all relevant suppliers, even those that may be indirectly associated with critical services.
- **Pre-Built Integrations and REST API:** Over 90 integrations with popular GRC solutions and a robust REST API to fetch data from existing systems, ensuring seamless data flow and integration with the organization's current risk management processes. This ensures the ongoing accuracy of third-party inventories.

By combining these capabilities, organizations gain a complete and accurate view of their third-party ecosystem, ensuring effective TPRM and NIS 2 compliance. With SecurityScorecard, organizations can continuously identify and monitor critical third-party suppliers, addressing cybersecurity risks and resilience as required by NIS 2.

1.2 Classify critical third-party suppliers based on their criticality to the organization.

NIS 2 requires organizations to classify critical third-party suppliers based on their cybersecurity risk and the criticality of their services to the organization’s resilience and operations. This classification allows organizations to prioritize their cybersecurity risk management efforts and ensure that appropriate controls are applied to suppliers based on the potential impact of their failure or disruption on the organization’s network and information systems.

SecurityScorecard supports this process with a four-factor vendor risk tiering system, enabling classification of third-party suppliers as low, moderate, high, or critical based on their cybersecurity posture and potential risk to the organization.

SecurityScorecard helps with classification through:

- **Seamless Data Integration:** Using data import, API, and integrations with existing GRC or inventory tools, organizations can automate classification based on factors such as business impact, revenue, and the volume or type of data shared with vendors.
- **Security Ratings:** SecurityScorecard's security ratings provide an outside-in view of a third-party's cybersecurity posture, assessing inherent risks without requiring direct access to the supplier's systems. This aligns with NIS 2's emphasis on understanding external risks from third-party suppliers.
- **Portfolio Grouping:** Portfolios can be used to group vendors by criticality or other criteria, allowing organizations to obtain aggregated risk overviews and customized tier-based reporting. This makes it easier to prioritize high-risk suppliers for further cybersecurity scrutiny.
- **Questionnaire Assessments:** Questionnaires can be used to collect evidence and context, helping to assess the cyber maturity of third-party suppliers, their overall risk, and their access to sensitive data or critical services. This ensures that organizations are capturing all relevant factors needed for effective risk management.

Once classified, organizations can tailor their cybersecurity risk management efforts and oversight to focus on critical vendors, ensuring a risk-based approach that aligns with NIS 2's TPRM requirements and strengthens the organization's cybersecurity resilience.

1.3 Conduct Risk Assessments for All Critical Third-Party Suppliers:

NIS 2 requires organizations to conduct thorough cybersecurity risk assessments for all critical third-party suppliers. These assessments should evaluate the cybersecurity controls and resilience measures in place to mitigate the risks posed by the supplier. The assessments must be tailored to the specific cybersecurity risks associated with each supplier, considering their criticality and the potential impact of their failure on the organization's network and information systems.

SecurityScorecard simplifies and streamlines this process with:

1.3.1 Cyber Security Ratings

SecurityScorecard provides a non-intrusive, outside-in methodology for evaluating organizations' cybersecurity profiles. It calculates and updates cybersecurity ratings daily on millions of organizations worldwide, offering an A-F letter grade and a numerical score (0-100) for each organization. This method provides an objective, scalable, and consistent way to assess third-party suppliers' cybersecurity posture.

Key Features of Cyber Security Ratings:

- **Ten Risk Factor Groups:** SecurityScorecard calculates and provides reports on ten different risk factor scores, covering various dimensions of cyber risk.
- **Issue Type Weights:** Issues within each risk factor are weighted based on their relative breach risk, contributing to the total score.
- **Daily Updates:** Regular scoring updates ensure that organizations are assessing the most up-to-date cybersecurity risk in a dynamic threat environment.
- **Industry Comparisons:** By tagging organizations with an industry label, SecurityScorecard enables cross-industry comparisons, allowing you to assess the cybersecurity posture of third-party suppliers relative to others in the same field.

1.3.2 Automatic Compliance Validation

SecurityScorecard allows for automated validation of suppliers against defined cybersecurity criteria, such as their overall score, individual factor scores, and historical scoring stability. This includes comparing suppliers against various industry standards (e.g., ISO, NIST, CIS, SOC 2, PCI, and NIS 2) and customer-specific frameworks (e.g., contractual security requirements).

- **Custom Compliance Frameworks:** You can build custom frameworks to validate suppliers based on specific requirements defined by your organization, ensuring alignment with your cybersecurity posture and NIS 2's third-party risk management requirements.

1.3.3 Evidence Locker

The Evidence Locker enables third-party suppliers to upload evidence, such as certifications, privacy policies, and penetration test results, to support their cybersecurity assessments.

- **Custom Visibility Control:** Suppliers can choose to make evidence publicly visible

or restrict visibility to specific users.

- **Request Evidence:** If a supplier has not uploaded the necessary evidence, SecurityScorecard facilitates evidence requests, ensuring that any gaps in cybersecurity documentation are addressed.

1.3.4 Questionnaire Assessments

SecurityScorecard simplifies and automates the questionnaire assessment process, traditionally used to collect data from suppliers regarding their cybersecurity practices.

Key Features of Questionnaire Assessments:

- **Automated Workflow:** Fully automated workflow for sending, following up, reviewing, assessing, and reporting on questionnaires.
- **Customizable Questionnaires:** Templates and conditional questionnaires can be customized based on industry needs, regulatory requirements, and vendor risk profiles, ensuring relevance and specificity.
- **Smart Mapping Engine:** Validates questionnaire responses against SecurityScorecard's cybersecurity ratings data, delivering comprehensive and objective risk assessments while minimizing manual effort.
- **Smart Answers:** Previously completed questionnaires or certifications can be used to auto-fill responses, accelerating the assessment turnaround time.
- **AI-Assisted Questionnaire Review (Available in 2025):** Leveraging AI to review documentation such as certifications, contracts, and vendor responses to reduce manual review, ensuring a faster and more efficient process.

These capabilities allow organizations to efficiently assess large numbers of suppliers while ensuring accuracy and relevance, crucial for managing cybersecurity risks at scale and in line with NIS 2's TPRM requirements.

1.4 Document the Results of Risk Assessments and Develop Risk Mitigation Plans:

NIS 2 requires organizations to document the results of their cybersecurity risk assessments for all critical third-party suppliers. Based on these assessments, organizations must develop, communicate, and track risk mitigation plans that include the identification and implementation of appropriate cybersecurity controls to address any identified vulnerabilities or risks.

These plans should be tailored to the criticality of the third-party supplier and designed to enhance the organization’s cybersecurity resilience in the event of a failure or disruption.

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

- **Assessment Findings Report:** SecurityScorecard allows organizations to create Assessment Findings Reports to document risks, violations, remediation actions, and other key findings. New assessment reporting functionality (*Available 2025)* will combine ratings, questionnaires, evidence, and policy violations, providing a comprehensive view of third-party risks.
- **Customizable Reporting:** SecurityScorecard offers customizable reports that provide insights into vendors' security posture, including ratings and risk factor scores. These can be exported in PDF, CSV, or JSON formats for easy sharing and tracking, ensuring NIS 2 compliance.
- **Evidence Locker and Document Center:** A centralized repository for storing and managing critical vendor documentation like questionnaires, contracts, and certifications, making it easier to access and comply with NIS 2's documentation requirements.
- **Action Plans:** Organizations can create targeted remediation plans with specific tasks, deadlines, and responsible parties, ensuring efficient collaboration to address security gaps and meet NIS 2's risk mitigation requirements.
- **Risk Mitigation Recommendations:** SecurityScorecard provides automated risk mitigation recommendations based on vulnerabilities, helping prioritize remediation efforts and align third-party suppliers with NIS 2's cybersecurity resilience standards.

2. Contractual Management

2.1 Incorporate NIS 2 TPRM requirements into contracts with critical third-party suppliers.

NIS 2 requires organizations to integrate cybersecurity and resilience standards into contracts with critical third-party suppliers. These contracts must ensure that suppliers are obligated to meet specific cybersecurity controls, including provisions for incident reporting, compliance with security measures, and cybersecurity resilience. Contracts should also include clauses for regular monitoring and reporting of compliance with these obligations.

SecurityScorecard supports this process by providing guidance on the criteria to be included in the contract, which can also be monitored over time. Actionable data through APIs and integrations enable seamless integration with contract management systems, helping organizations streamline compliance and oversight.

2.2 Monitor compliance with contractual requirements.

NIS 2 requires organizations to continuously monitor the compliance of critical third-party suppliers with the cybersecurity and resilience requirements set forth in their contracts. This includes ensuring adherence to security standards, incident response processes, and other obligations related to cybersecurity resilience.

Organizations must implement a framework for ongoing monitoring, which includes regular audits, assessments, and continuous tracking of the cybersecurity posture of suppliers.

SecurityScorecard simplifies and streamlines 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 supplier 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.

NIS 2 mandates that organizations regularly review and update contracts with critical third-party suppliers to ensure they align with evolving cybersecurity and resilience standards, as well as the changing risk landscape. Organizations must ensure that their contracts reflect the latest cybersecurity controls, incident response protocols, and cybersecurity resilience measures, based on the evolving nature of risks.

This process helps ensure that contractual obligations continue to meet the organization's cybersecurity needs and that third-party suppliers are held to the required standards.

SecurityScorecard assists by providing continuous risk insights that can inform the contract update process, ensuring ongoing alignment with NIS 2 requirements.

SecurityScorecard's Document Center, enhanced with AI/LLM-powered contract validation *(available 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 critical third-party suppliers.

NIS 2 requires organizations to continuously monitor the cybersecurity posture of critical third-party suppliers to ensure ongoing compliance with cybersecurity and resilience requirements. This includes tracking emerging risks, vulnerabilities, and incidents that could affect the continuity and security of critical services. The goal is to identify and address potential cybersecurity threats or weaknesses promptly, ensuring that third-party suppliers maintain a security posture aligned with the organization's cybersecurity standards and regulatory obligations.

SecurityScorecard provides robust features to support continuous cybersecurity monitoring and breach management of critical suppliers, 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 NIS 2's focus on cybersecurity resilience and continuous oversight.

3.2 Establish processes for cybersecurity incident management and response.

NIS 2 requires organizations to establish comprehensive processes for cybersecurity incident management and response. These processes should define clear roles and responsibilities, communication protocols, and escalation procedures for addressing cybersecurity incidents, including those involving critical third-party suppliers.

Organizations must ensure that incidents are detected promptly, responded to efficiently, and reported to the appropriate stakeholders and regulatory authorities. Regular testing and updating of incident response plans are also essential to ensure preparedness in managing both internal and third-party-related incidents.

SecurityScorecard aids this process by providing real-time alerts on cybersecurity risks and incidents from third-party suppliers, enabling a rapid and informed response.

3.3 Conduct regular testing of critical third-party suppliers.

NIS 2 requires organizations to conduct regular cybersecurity testing of their critical third-party suppliers. This testing should include vulnerability assessments, penetration testing, and other exercises to evaluate the strength of the supplier's cybersecurity controls and their ability to respond to cybersecurity incidents. The goal is to verify that suppliers can maintain cybersecurity resilience in the face of evolving threats and potential disruptions.

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:** Offers penetration testing and real-world incident simulations to evaluate vendor preparedness for disruptions.

These tools and services help ensure thorough and effective testing of critical third-party suppliers.

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

NIS 2 requires organizations to maintain a centralized repository for all documentation related to critical third-party suppliers, including contracts, cybersecurity risk

assessments, compliance documents, and cybersecurity incident reports.

This repository ensures that organizations can easily access and manage supplier-related information for ongoing monitoring, compliance checks, and incident response. The repository should help demonstrate compliance with NIS 2 requirements and support cybersecurity resilience efforts.

SecurityScorecard provides a centralized platform for managing third-party documentation and risk assessments, aligning with NIS 2's cybersecurity 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 NIS 2-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 NIS 2's TPRM requirements.

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

NIS 2 requires organizations to regularly report on their third-party risk management

(TPRM) activities to senior management and the board of directors. These reports should include updates on the cybersecurity posture of critical third-party suppliers, key cybersecurity risks, ongoing incidents, and mitigation efforts.

The goal is to ensure that senior leaders are well-informed and can make strategic decisions to mitigate third-party risks. Regular reporting provides cybersecurity resilience oversight and helps maintain compliance with NIS 2 requirements.

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 NIS 2's requirements.

1.1 Identify All Critical Third-Parties

1.1.1 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 critical third-parties within the NIS 2 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 Automatic Vendor Detection (AVD)

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 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 critical third-party suppliers based on their criticality to the organization.

1.2.1 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 the following NIS 2-aligned factors:

- **The type of data the supplier can access:** Suppliers with access to sensitive, confidential, or regulated data (e.g., personal data, intellectual property) should be classified as higher risk due to their potential cybersecurity impact.
- **The type of services the supplier manages:** Suppliers providing critical services or infrastructure, such as those in sectors like energy, transport, or healthcare, should be classified based on their role in ensuring the continuity of essential services and the potential impact on the organization's cybersecurity resilience.
- **The criticality of the supplier's role in business operations:** Suppliers whose failure or disruption could significantly impact network and information systems or cybersecurity resilience should be given higher priority in classification.
- **The potential cybersecurity and operational risk in case of disruption:** Assess

the potential impact of a supplier's disruption on business continuity and cybersecurity resilience, including the likelihood and severity of cybersecurity incidents and operational 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 cybersecurity monitoring and breach management.
- Receive alerts and generate reports based on your defined criteria.

1.3 Conduct Risk Assessments for Critical Third-Party Suppliers

1.3.1 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 context 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)
- **Companies *(Filters)***
  - Filters in Companies listing enable you to filter and search third-parties based on recent breaches, specific types of issues, vulnerabilities and more.

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 Automated 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 and 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 Compliance Validation

Once Ratings data points are assessed and validated, the next step is to check the company against required compliance frameworks.

Evidence Locker enables companies to proactively add certifications and other security evidence, demonstrating compliance and cyber maturity. This can help suppliers avoid certification-based questionnaires. If a supplier's Evidence Locker is empty, you can request documents to be uploaded.

In addition to the Evidence Locker artifacts provided by suppliers, SecurityScorecard supports automated compliance validation by mapping automatically collected Ratings signals to common compliance frameworks.

- **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, NIS 2
    - 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.

1.3.2.3 Questionnaire Assessments

While Ratings and Compliance assessments are fully automated and do not involve the supplier, the third step—Questionnaire Assessments—requires supplier participation.

- **When to Use**
    - Send to all suppliers if required by the company policy or selectively (e.g., low ratings or critical suppliers that must be assessed).
- **How to Send**
    - Use standard industry templates, custom questionnaires, or SecurityScorecard's NIS 2 Supplier focused template
    - From the Company Compliance assessment page (click Send Questionnaire).
    - From any Company Ratings page (More → Send Questionnaire).
    - Via Communications → Questionnaires in the top navigation.
- **Configuration Options**

    - Choose a template, recipient(s), sending date, completion deadline, and reminders.
    - Customize the invitation message with additional context.
- **Workflow Management**
    - Suppliers receive an email linking to the questionnaire.
    - Track progress in the questionnaire workflow management page (e.g., who is working on it, how far along they are).
- **Review and Acceptance Process**
    - Validate supplier responses against Ratings data, add notes or request more information.
    - Once complete, generate an assessment report detailing any findings, agreed actions and recommendations.
    - Email notifications keep both parties updated on progress.

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

Once you've completed your supplier assessment (Ratings, Compliance, Questionnaire), you can record findings, outcomes, and action items using the following methods:

1.4.1 Assessment Findings Report

- **Questionnaire-Based:** Currently, findings reports are tied to a sent questionnaire. If no questionnaire has been sent, you can still track notes and findings in *Vendor Details*.
- **Report Content:** Document identified risks, policy or contractual violations, and agreed remediation actions. Add an assessment summary and choose whether to Recommend, Recommend with Conditions, or Not Recommend the vendor.
- **Access & Generation:**
    1. Open the questionnaire sent to the vendor.
    2. Select the Findings tab (existing findings auto-populate; new findings can be added).
    3. Generate and download the report as CSV or PDF for storage or sharing.
- **A combined assessment report template *(Available in 2025)*** that works even if no questionnaire has been sent.

1.4.2 Company-Specific Summary and PDF Reports

- **One-Page Summaries & Detailed Reports:** Generate PDF reports for any vendor, including a concise overview or more in-depth analysis.
- **How to Generate:** Go to the Company Overview → More → Generate a Report.

1.4.3 Reporting Center

- **Location:** Automation → Reporting Center.
- **Templates:** Offers customizable reporting templates for different audiences—from board-level summaries to technical deep dives.
- **Export Options:** PDF, CSV, and more for easy sharing and tracking.
- **Storage:** All created reports remain under Reporting Center → Generated Reports for 30 days.

1.4.4 Document Center *(Available in 2025)*

- **Central Repository:** Will allow storing and managing vendor documentation—e.g., Assessment Findings Reports, questionnaires, contracts, certifications.
- **Until Release:** Store documents externally and reference them via *Vendor Details* notes.

1.4.5 Action Plans

- **Purpose:** Develop targeted remediation plans with tasks, deadlines, and assigned owners.
- **Creation:**
  - Communication → Action Plans, or
  - Create an Action Plan on the scorecard overview page.
- **Setup:** If a supplier fails to meet defined criteria (e.g., minimum B grade), an action plan can be generated with necessary steps to reach the target.
- **Collaboration:** Share action plans with vendors, granting them access to their scorecard, remediation recommendations, and progress updates.
- **Tracking:** The Action Plans page summarizes vendor progress on assigned tasks.

2.1 Incorporate NIS 2 TPRM requirements into contracts with critical third-party suppliers.

Tying contractual clauses to fact-based, continuously monitored data points ensures requirements are clear, actionable, and consistently tracked. SecurityScorecard supports this by offering guidance on criteria to include in contracts, which can be monitored over time. Examples include:

- **SecurityScorecard Rating** of at least B
- **Risk Factor Ratings** of at least C
- **No High Breach Risk Issues**
- **Questionnaire Validation Score** of 75% or higher

- **90-Day Remediation Requirement** for critical findings or violations

Through APIs and integrations, these criteria can seamlessly integrate with contract management systems, streamlining compliance and oversight.

2.2 Monitor Compliance with Contractual Requirements

2.2.1 Custom Compliance Frameworks

- **Purpose:** Create validation frameworks based on contractual security requirements (e.g., scores, findings) alongside industry-standard frameworks.
- **Functionality:** Track, validate, and identify non-compliance. Conflicting findings are flagged for quick reporting and enforcement.
- **Customization:** SecurityScorecard can help define criteria and import them as a custom compliance framework.

2.2.2 Continuous Monitoring

SecurityScorecard continuously monitors all companies in your portfolios, allowing you to define rules that trigger alerts or actions when certain events occur.

- **Accessing Rule Builder:**
  - Automation → Rule Builder, or
  - In a Portfolio, click Rules in the right-side menu.
- **Rule Attributes:**
  - Name: A descriptive rule name shown in alerts.
  - Trigger: Defines the event (e.g., score drop, new breach).
  - Scorecards: Specify which entities the rule applies to (e.g., all monitored companies, a specific portfolio).
  - Action: Determine what happens when the trigger occurs (e.g., email alert, webhook, questionnaire).
- **Scope & Limitations:**
  - All events and actions are available for monitored companies (i.e., in portfolios).
  - For “unmonitored companies” (not in a portfolio), only “score drop” and “new breach reported” triggers are available, and only email alerts can be sent.
- **Supplier Policy Examples:**
  - **Unmonitored Companies:** Alert on overall grade dropping below B, new breach reported.
  - **All Companies in Portfolios:** Alert on overall grade < B, factor grade < C,

new breach reported.
    - **Critical Suppliers:** In addition to above, consider alerts on specific factor score drops (IP Reputation, Hacker Chatter, Info Leak) or new high breach risk findings.
- **Notifications & Integrations:**
    - Start with email alerts, then integrate with SIEM, ITSM, Microsoft Teams, Slack, etc.
    - Upon receiving an alert (e.g., supplier grade drops from B to C), create an action plan (with a "B grade" criterion) and share it with the supplier for resolution.

2.2.3 Portfolio Policies *(Available in 2025)*

- **Overview:** Allows defining supplier tiering policies based on contractual requirements, continuously monitoring security postures, documents, certifications, and assessments.
- **Automation:** Will support direct integration with rules to automate oversight and enforcement once launched.

2.3 Review and update contracts regularly

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

3.1 Continuously monitor the security posture of critical third-party suppliers

SecurityScorecard uses continuous active and passive data collection to track vendors across 200+ cybersecurity issues.

By configuring Rule Builder and alerts as described in Section 2.2.2, you can promptly detect changes in the risk landscape. In addition, creating Action Plans (see Section 1.4.5) allows you to collaborate with suppliers on remediation and track their progress.

3.2 Establish Processes for Incident Management and Response

When configuring alerting rules, include a universal rule to detect breaches or incidents across all suppliers.

To gather the necessary details—such as incident magnitude, data or operational impact, isolation measures, and corrective actions—create a concise questionnaire template.

By setting this questionnaire as the automated action when a breach or incident rule is triggered, you can quickly obtain critical information and streamline your incident response process.

3.3 Conduct Regular Testing of Critical Third-Party Suppliers

- **Continuous Vulnerability Assessments:** SecurityScorecard provides broad, non-intrusive vulnerability scanning for all companies in your portfolios. While not as in-depth as dedicated tools, this automated coverage helps identify issues at scale and guides deeper penetration testing or targeted assessments.
- **Assessment Questionnaires:** A NIS 2-aligned supplier questionnaire should validate disaster recovery, cybersecurity continuity, vulnerability assessment, and cybersecurity incident management practices, including their review and testing frequency.
- **Penetration Testing & Simulations:** SecurityScorecard also offers penetration testing and real-world tabletop exercises to gauge vendor preparedness for potential disruptions.

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

NIS 2 mandates a standardized Register of Information, capturing all contractual agreements with third-parties, including:

- Supplier Identification: Name, unique identifier (e.g., LEI), contact details
- Contractual Details: Contract reference, start/end dates, type of contract, service scope
- Service Information: Description of provided services, supported critical functions, SLAs/performance metrics
- Risk Assessment: Criticality, associated risks, mitigation/contingency plans
- Subcontractor Details: Roles, compliance status of subcontractors
- Compliance/Regulatory Info: Relevant regulations (e.g., NIS 2, GDPR), reporting obligations
- Incident Management: Reporting procedures, incident history, communication protocols
- Exit/Termination Clauses: Termination conditions, exit strategies, data handling, transition plans

By consolidating these details in SecurityScorecard, organizations can align with NIS 2's cybersecurity resilience principles and maintain a comprehensive, up-to-date register of third-party information that can be exported when needed and used as part of the ITS

Register of Information reporting.

Supplier Details (Vendor System of Record):

- Add and update the majority of these required fields during onboarding or afterward.
- The current version includes a fixed field set. Custom fields will be available in 2025, allowing a comprehensive NIS 2-specific field set.

Collecting Additional Info:

- Use NIS 2-aligned questionnaires to gather details on subcontractors, compliance, or cybersecurity incident management.
- Store questionnaires and assessment results to the vendor record via Document Center
- Add important assessment results, findings or other notable comments to the vendor record as notes.

Document Center *(Available in 2025)*:

- Store and manage all supplier-related documents (contracts, assessments, incident reports, certifications, policies) and link them to specific vendors.

Vendor & Portfolio Exports:

- Export supplier information as a CSV via UI or API for easy reporting on supplier status and Register of Information building.

3.5 Report on TPRM Activities to Senior Management and the Board of Directors

NIS 2 requires organizations to regularly report on their third-party risk management (TPRM) activities to senior management and the board of directors. These reports should provide an overview of the organization's TPRM posture, highlight key risks related to third-party suppliers, outline mitigation plans, and evaluate the performance of third-party suppliers, especially those handling critical services or data.

SecurityScorecard helps organizations meet NIS 2 reporting requirements with the following features:

Reporting Center (Automation → Reporting Center):

- Pre-built templates: SecurityScorecard offers pre-built templates for board-level summaries and detailed, technical reports. These templates ensure that reports are tailored to different audiences, from high-level executives to technical teams,

covering both cybersecurity risks and TPRM performance.

- Fully customizable: Reports can be customized to align with NIS 2 reporting requirements, ensuring that they include critical information on cybersecurity resilience, risk mitigation plans, and third-party performance. SecurityScorecard assistance is available to ensure the reports meet NIS 2's compliance standards.

CSV and API Exports:

- CSV Exports: Supplier data can be exported in CSV format, enabling organizations to share and store information for further analysis or reporting purposes, in compliance with NIS 2's ITS (Implemented Technical Standards) Register of Information reporting requirements.
- API Exports: For seamless integration with existing reporting or GRC systems, SecurityScorecard offers a robust API to export data directly into third-party systems, ensuring continuous tracking and reporting of third-party risk and cybersecurity posture.

.