Simplify and Automate APRA Prudential Standard CPS 230 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 Prudential Standard CPS 230, issued by the Australian Prudential Regulation Authority (APRA), is a regulatory framework designed to strengthen operational risk management, business continuity, and third-party risk management (TPRM) for APRA-regulated entities, including banks, insurers, and superannuation funds. CPS 230 aims to ensure organizations have comprehensive risk management frameworks to identify, assess, and mitigate operational and third-party risks, ensuring business continuity and resilience in the face of potential disruptions. Organizations must comply with CPS 230's requirements by July 1, 2025.

CPS 230 focuses on enhancing operational resilience across financial and insurance sectors, with particular emphasis on third-party risk management to ensure service continuity and reduce risks associated with outsourced providers.

The standard emphasizes the following key areas:

Risk Management:

CPS 230 mandates organizations to establish comprehensive risk management frameworks, requiring:

- Identification and assessment of operational risks across all business functions, including third-party dependencies.
- Implementation of internal controls to mitigate identified risks and ensure regulatory compliance.
- Ongoing risk assessment processes, including continuous monitoring and reporting to senior management.
- Board accountability in overseeing and ensuring the effectiveness of operational risk management strategies.

Business Continuity and Incident Management:

Organizations must implement robust business continuity and incident response frameworks, including:

- Documented business continuity plans (BCPs) with clearly defined recovery strategies.
- Establishment of incident response teams with clearly assigned roles and responsibilities.
- Crisis communication and escalation protocols to ensure timely reporting and resolution of incidents.
- Regular testing of BCPs through scenario-based exercises to validate effectiveness under operational stress conditions.

Testing and Assurance:

CPS 230 underscores the importance of regular resilience testing, requiring:

- Business continuity and disaster recovery (BCDR) testing to ensure organizations can withstand operational disruptions.
- Penetration testing and vulnerability assessments to validate cybersecurity resilience.

- Compliance testing and regulatory audits to ensure adherence to APRA's risk management expectations.

Third-Party Risk Management (TPRM):

CPS 230 places significant emphasis on oversight of third-party and outsourced service providers, requiring:

- Identification and classification of critical third-party vendors based on their impact on business operations.
- Regular cybersecurity and operational risk assessments of third-party providers.
- Incorporation of CPS 230-aligned risk management requirements into vendor contracts.
- Continuous monitoring of vendor security postures and service performance to detect potential risks early.
- Development of contingency and exit strategies in case of third-party failure or contract termination.

SecurityScorecard's Role in CPS 230 Compliance:

SecurityScorecard helps to simplify and streamline CPS 230 Third-Party Risk Management (TPRM) compliance by:

- Automating risk assessment processes for third- and fourth-party vendors.
- Providing real-time security insights into vendor cybersecurity postures.
- Enabling continuous monitoring and early detection of security risks.
- Supporting compliance tracking and reporting to meet APRA requirements.

This document outlines key CPS 230 TPRM requirements and how SecurityScorecard can help organizations operationalize compliance, strengthen cybersecurity resilience, and ensure regulatory adherence.

CPS 230 TPRM Requirements

1. Operational Risk Identification and Management for Third Parties

1.1 Identify All Critical Third-Party Suppliers

CPS 230 mandates that organizations establish a comprehensive inventory of critical third-party suppliers to enhance operational resilience and mitigate risks associated with outsourcing key services. This includes identifying third parties that:

- Provide essential services to business continuity.
- Manage critical infrastructure relevant to financial and operational stability.
- Have access to sensitive data or handle confidential information.

This identification process ensures that organizations can effectively assess, categorize, and mitigate risks introduced by their third-party relationships, supporting compliance with APRA's operational risk and business continuity expectations.

How SecurityScorecard Supports Compliance

- **Pre-Built Integrations:** Supports over 90 industry-leading integrations with GRC platforms, procurement systems, and IT risk management tools.
- **Automatic Vendor Detection (AVD):** AI-powered technology identifies hidden or indirect third- and fourth-party suppliers, uncovering risks that traditional vendor assessments may overlook. This proactive identification helps organizations address supply chain vulnerabilities before they escalate.
- **REST API:** Ensures seamless data exchange with existing governance workflows, enhancing the accuracy and timeliness of third-party risk assessments.
- **Bulk Company Import:** Enables organizations to quickly populate their vendor inventory using CSV uploads. This is particularly useful for institutions without integrated third-party management systems.

By leveraging automated detection and classification, organizations gain a holistic view of their third-party ecosystem, helping to achieve compliance with CPS 230 while proactively mitigating vendor risks. SecurityScorecard enables continuous monitoring, real-time risk intelligence, and integration with operational resilience strategies to help organizations meet APRA's stringent risk management standards.

1.2 Classify Critical Third-Party Suppliers Based on Their Impact on Business Operations

CPS 230 mandates organizations to classify critical third-party suppliers based on their operational impact, regulatory risk, geographic exposure, and resilience requirements. This classification ensures that risk management controls are applied appropriately based on the potential impact of supplier failure on the organization's operational stability, financial security, and regulatory compliance.

Offshoring & Geographic Risk Considerations

CPS 230 expects organizations to assess jurisdictional risks associated with outsourcing critical

operations to third-party vendors operating in foreign or high-risk jurisdictions. This includes:

- **Regulatory & Compliance Risks**: Vendors must comply with local laws, data protection regulations, and APRA-aligned security standards.
- **Geopolitical Stability**: Assessment of potential economic, political, or cybersecurity threats affecting vendor operations.
- **Data Sovereignty Risks**: Ensuring vendor compliance with APRA's data governance and sovereignty requirements.
- **Service Continuity Risks**: Evaluating vendors' ability to maintain operations during cross-border disruptions.

To mitigate offshoring risks, organizations should:

- **Require geographic risk disclosures** as part of vendor onboarding.
- **Include contingency planning provisions** in vendor contracts for vendors in high-risk jurisdictions.
- **Conduct enhanced due diligence** on vendors operating in geopolitically sensitive regions.
- **Monitor compliance with jurisdictional security laws and evolving regulations**.

SecurityScorecard Supports CPS 230 Compliance through:

Seamless Data Integration for Third-Party Classification

- **Automated Data Imports**: Organizations can automatically classify vendors by integrating SecurityScorecard with GRC platforms, procurement systems, and IT risk management tools.
- **REST API and Third-Party Integrations**: Organizations can leverage 90+ integrations with existing inventory management tools, ensuring real-time classification of critical suppliers.

Risk-Based Vendor Classification and Security Ratings

- **Security Ratings**: SecurityScorecard provides a continuous, outside-in assessment of third-party security postures, enabling risk-tiering without requiring direct access to supplier environments.
- **Operational Impact Analysis**: Organizations can align vendor classification with business impact, data sensitivity, regulatory exposure, and geographic risk factors.

Portfolio-Based Risk Grouping and Monitoring

- **Portfolio Management**: SecurityScorecard enables organizations to group vendors by risk category (critical, high, moderate, low) to ensure targeted risk assessments and compliance oversight.
- **Aggregated Risk Reporting**: Organizations gain tier-based risk insights to prioritize high-risk suppliers for further cybersecurity and resilience scrutiny.

Vendor Risk Questionnaires and Cyber Maturity Assessments

- **Customizable Third-Party Questionnaires**: SecurityScorecard enables organizations to capture operational dependencies, compliance evidence, and security certifications via

vendor assessments.

- **Continuous Risk Posture Validation**: Organizations can use automated questionnaire validation to maintain a real-time view of vendor cybersecurity and operational resilience.

By integrating geographic risk assessments, operational impact analysis, and third-party risk classification, organizations can align their supplier risk management strategies with CPS 230, helping to achieve regulatory compliance and enhanced operational resilience.

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

CPS 230 mandates that organizations conduct comprehensive risk assessments for all critical third-party suppliers to evaluate their operational resilience, cybersecurity controls, and business continuity capabilities. These assessments should be tailored based on supplier criticality and the potential impact of failure, ensuring that organizations identify and mitigate risks proactively.

SecurityScorecard simplifies and streamlines this process with:

Third-Party Risk Ratings

SecurityScorecard provides a non-intrusive, outside-in methodology for evaluating organizations' cybersecurity and operational risk postures. Ratings are calculated and updated daily across millions of organizations globally, assigning an A-F letter grade and a numerical score (0-100) to provide a scalable, objective risk assessment.

Key Features of Security Ratings:

- **Comprehensive Risk Factor Analysis:** SecurityScorecard evaluates ten operational and cybersecurity risk factors covering multiple dimensions of third-party risk.
- **Weighted Risk Contributions:** Issue types within each risk category are weighted based on their potential impact on business continuity and regulatory compliance.
- **Real-Time Updates:** Organizations receive daily risk intelligence to track the latest security posture of their third-party ecosystem.
- **Industry Benchmarks:** Companies can benchmark their suppliers against industry-specific cybersecurity standards and best practices, ensuring third-party providers maintain resilience in line with regulatory expectations.

Automated Compliance Validation

SecurityScorecard enables organizations to automate compliance validation against key regulatory and industry frameworks, including ISO, NIST, CIS, SOC 2, PCI, and internal contractual requirements.

Organizations can define and enforce custom supplier compliance requirements, helping vendors align with CPS 230's operational resilience and business continuity mandates.

Automated checks compare third-party security postures against regulatory thresholds, identifying non-compliant suppliers before risks escalate.

Evidence Locker for Regulatory Assurance

The Evidence Locker provides a centralized platform for suppliers to upload and manage compliance documentation, including:

- **Certifications, penetration test reports, and privacy policies** to demonstrate adherence to regulatory standards.
- **Audit trail tracking** to ensure visibility into supplier security measures and regulatory compliance over time.
- **Custom Visibility Controls** allow organizations to restrict document access to relevant internal stakeholders and compliance officers.
- **Streamlined Evidence Collection:** Organizations can request missing documentation directly from suppliers, ensuring that cybersecurity and compliance gaps are proactively addressed.

Advanced Questionnaire Assessments

SecurityScorecard automates and enhances the vendor due diligence process by providing customizable, structured questionnaires that assess third-party risk based on:

- **Operational and cybersecurity resilience**, helping third parties meet CPS 230's business continuity and security requirements.
- **Industry and regulatory mandates**, aligning vendor risk assessments with CPS 230, APRA guidelines, and international security frameworks.
- **Continuous compliance tracking**, enabling organizations to receive real-time insights into supplier vulnerabilities and remediation actions.

Key Features of Smart Questionnaires:

- **Automated Workflow:** Fully integrated with third-party risk management workflows to send, track, and assess questionnaires efficiently.
- **Dynamic Questionnaires:** Customizable based on vendor tiering, industry verticals, and risk exposure, ensuring relevance.
- **AI-Assisted Review (Available 2025):** AI-powered automation for document verification, accelerating compliance validation and reducing manual efforts.

By leveraging automated risk assessments, compliance validation, and AI-powered monitoring, organizations can enhance their third-party risk oversight and work to adhere to CPS 230's operational risk and business continuity mandates. This proactive approach strengthens resilience against third-party failures, mitigating financial, regulatory, and reputational risks for APRA-regulated entities.

1.4 Identify Fourth-Party Aggregated Risk

CPS 230 requires organizations to assess fourth-party risks, ensuring that third-party providers do not introduce excessive reliance on high-risk subcontractors. This approach mitigates cascading supply chain vulnerabilities and strengthens overall operational resilience.

SecurityScorecard's Automatic Vendor Detection (AVD) enhances visibility by:

- **Mapping Supply Chain Relationships:** Identifies third, fourth, and nth-party dependencies to assess systemic risks.
- **Tracing Vendor Linkages:** Uses multiple data sources to uncover hidden subcontractors and indirect dependencies.
- **Enhancing Risk Visibility:** Helps institutions analyze supply chain risks across extended vendor networks, helping to comply with CPS 230 operational resilience mandates.

1.5 Document the Results of Risk Assessments and Develop Risk Mitigation Plans

CPS 230 mandates that organizations document the results of risk assessments for all critical third-party suppliers. These assessments should support the development of comprehensive risk mitigation plans, including:

- Identification of cybersecurity and operational vulnerabilities.
- Implementation of security controls and remediation measures.
- Tracking corrective actions and monitoring vendor compliance.

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

Assessment Findings Report:

- Enables organizations to create structured reports to document risks, violations, and remediation actions.
- New functionality (Available 2025) will combine security ratings, questionnaires, evidence, and policy violations for a holistic view of third-party risks.

Customizable Compliance Reporting:

- Generates detailed insights into vendors' security posture, including risk factor scores and compliance gaps.
- Reports are exportable in PDF, CSV, or JSON formats for tracking and board-level presentations.

Centralized Document Repository (Evidence Locker & Document Center):

- Provides a single repository for vendor documentation, including contracts, security questionnaires, and compliance certifications.
- Delivers easy access and audit readiness in line with CPS 230's third-party risk governance requirements.

Action Plans for Risk Mitigation:

- Organizations can create targeted remediation plans with clearly assigned tasks, deadlines, and accountability measures.
- Facilitates structured collaboration with vendors to address security gaps and ensure timely corrective actions.

Automated Risk Mitigation Recommendations:

- SecurityScorecard provides AI-driven remediation recommendations based on detected vulnerabilities, helping organizations prioritize high-impact security improvements.
- Helps align third-party risk management efforts with CPS 230's cybersecurity resilience framework.

By implementing structured risk documentation, automated compliance tracking, and centralized risk reporting, organizations can proactively enhance third-party risk oversight and work to comply with CPS 230 operational resilience standards.

2. Contractual Management

2.1 Incorporate CPS 230 TPRM Requirements into Contracts with Critical Third-Party Suppliers

CPS 230 requires organizations to embed operational risk management, cybersecurity, and resilience requirements into contracts with critical third-party suppliers. Contracts must ensure suppliers adhere to specific security controls, including provisions for:

- Incident response and reporting obligations.
- Continuous compliance with cybersecurity and operational risk measures.
- Regular resilience testing and business continuity planning.
- Clear accountability for risk management practices.

Additionally, contracts should define ongoing monitoring expectations and provide structured mechanisms for vendors to demonstrate compliance with CPS 230 obligations.

How SecurityScorecard Supports Contractual Compliance:

- **Automated contract compliance tracking** through integrations with governance platforms.
- **Real-time security data** via APIs to monitor third-party compliance with contractual requirements.
- **Centralized contract management (Available 2025)** to streamline regulatory oversight and mitigate risks.

2.2 Monitor Compliance with Contractual Requirements

CPS 230 mandates organizations to continuously monitor compliance of critical third-party suppliers with contractual risk management obligations. This requires:

- **Ongoing audits, assessments, and performance tracking**.
- **Continuous cybersecurity posture monitoring** to identify changes in vendor risk profiles.
- **Ensuring vendor adherence to security standards and incident response protocols**.

To comply with CPS 230, organizations must establish structured audit and assurance processes to validate third-party compliance with security and resilience requirements. This includes:

Internal Audit Reviews

- **Annual internal audits** of third-party risk management policies and procedures.
- **Quarterly compliance spot checks** to ensure ongoing adherence to risk controls.
- **Audit trails** documenting historical risk assessments, remediation actions, and contractual compliance.

Third-Party Control Testing

- Vendors must participate in **regular control testing** to verify the effectiveness of their security and business continuity measures.
- **Simulated security assessments** (e.g., phishing exercises, incident response drills) must be conducted periodically.
- Organizations should require **external validation of vendor security controls** through independent audits or certifications (e.g., ISO 27001, SOC 2).

Escalation & Issue Management Workflows

To comply with CPS 230, organizations must implement structured escalation workflows to manage third-party security incidents, compliance failures, and contractual breaches.

Defined Escalation Triggers

- **Security Rating Drops Below Threshold:** Immediate escalation for vendors whose rating falls below a predefined security threshold (e.g., below a B grade).
- **Repeated Security Violations:** If a vendor is flagged for multiple security or compliance violations, automated escalation is triggered.
- **Failure to Remediate Risks Within SLA:** If a vendor does not resolve identified issues within agreed-upon remediation timelines, formal escalation occurs.
- **Regulatory Compliance Breaches:** Any vendor identified as non-compliant with CPS 230 mandates is escalated for executive and board review.

Enforcement Actions

- **Automated Risk-Based Alerts:** Vendors receive automated notifications for risk deviations.
- **Corrective Action Mandates:** Non-compliant vendors must submit structured remediation plans.
- **Suspension or Contract Termination:** Critical violations may result in immediate supplier suspension.

How SecurityScorecard Enhances Compliance Monitoring:

- **Custom Compliance Frameworks**: Enables organizations to define and enforce supplier security and operational requirements.
- **Continuous Risk Monitoring**: SecurityScorecard tracks vendor cybersecurity postures in real time, providing immediate alerts for security shifts.
- **Audit Reporting Tools**: Supports automated compliance reporting, tracking vendor adherence to CPS 230 mandates.
- **Integrated Escalation Workflows**: Automated routing of security incidents to risk teams.
- **Remediation Tracking Dashboards**: Provides visibility into supplier corrective actions.
- **Portfolio Policies (Available in 2025)**: Allows organizations to set risk-based contract

enforcement policies and ensure vendors comply with resilience and risk mitigation mandates.

2.3 Review and Update Contracts Regularly

CPS 230 mandates organizations to periodically review and update contracts to reflect:

- Evolving cybersecurity risks and threat landscapes.
- New operational resilience and business continuity requirements.
- Updated security policies and regulatory changes from APRA.

By regularly revising contracts, organizations can ensure that third-party vendors maintain compliance with CPS 230 risk standards, mitigating operational and security vulnerabilities introduced through outdated agreements.

How SecurityScorecard Supports Contract Updates:

- **Continuous risk insights** to help with contract update discussions in alignment with CPS 230.
- **Automated contract risk assessments**, ensuring vendors meet resilience standards.
- **AI-driven contract validation (Available in 2025)** to streamline contract audits and enforce up-to-date security and compliance clauses.

By embedding cybersecurity resilience, risk controls, and compliance tracking into contracts, organizations can strengthen their third-party governance frameworks, helping to achieve CPS 230 compliance and robust operational risk management.

3. Continuous Monitoring and Oversight

3.1 Continuously Monitor the Security Posture of Critical Third-Party Suppliers

CPS 230 requires organizations to continuously monitor the operational and cybersecurity risk posture of third-party suppliers to ensure compliance with business continuity and resilience requirements. This includes tracking emerging threats, vulnerabilities, and incidents that may impact service availability and security. The objective is to proactively identify and mitigate risks to maintain operational resilience in line with APRA's standards.

Offshoring & Geographic Risk Monitoring

To comply with CPS 230, organizations must continuously monitor vendor security postures, especially for offshored or jurisdictionally sensitive third-party providers. Key monitoring strategies include:

- **Real-Time Risk Alerts**: Tracking cybersecurity threats, geopolitical instability, and compliance risks affecting vendors in foreign jurisdictions.
- **Continuous Threat Intelligence**: Identifying evolving risks, including cross-border data access vulnerabilities, service continuity threats, and government-imposed restrictions.
- **Automated Compliance Tracking**: Ensuring offshored vendors adhere to APRA's operational risk and security mandates.

How SecurityScorecard Supports CPS 230 Compliance:

- **Continuous Risk Monitoring**: Real-time tracking of third-party security postures across 200+ risk categories, incorporating threat intelligence, breach detection, and security issue remediation.
- **Customizable Alerts & Notifications**: Automated alerts for risk score degradation, critical vulnerabilities, and non-compliance incidents, ensuring rapid risk mitigation.
- **Geographic Risk Assessment Tools**: Provides risk-adjusted supplier monitoring based on operational jurisdiction.
- **Vendor Remediation & Tracking**: Provides action plans, supplier collaboration workflows, and issue tracking to enforce security improvements and ensure continuous compliance.

By integrating jurisdictional risk monitoring, geographic risk assessment, and continuous compliance tracking, organizations ensure full alignment with CPS 230's operational risk mandates, particularly for offshored third-party suppliers.

3.2 Establish Processes for Incident Management and Response

CPS 230 mandates that organizations establish structured cybersecurity incident response processes for third-party suppliers. These processes must define roles and responsibilities, escalation procedures, and regulatory reporting requirements.

Organizations must ensure incidents are:

- **Promptly detected** through real-time monitoring and intelligence feeds.
- **Efficiently addressed** via pre-established response protocols.
- **Reported to senior stakeholders and regulators** as per APRA's incident disclosure mandates.

Structured Escalation Workflows for Third-Party Incidents

Organizations must enforce structured response protocols when handling third-party security breaches:

Step 1: Incident Detection & Initial Triage

- Automated breach detection alerts trigger an internal risk review.
- Initial triage team classifies incident severity based on business impact.

Step 2: Formal Escalation & Risk Mitigation

- High & Critical severity incidents are escalated to executive security teams.
- Vendors must provide formal remediation plans within 24 hours.
- Risk containment actions are executed (e.g., temporary vendor access suspension).

Step 3: Regulatory & Board-Level Disclosure (if applicable)

- For major incidents, organizations must notify APRA within 72 hours.
- The board must receive a detailed post-incident analysis report.

- Third-party contractual reviews are conducted to assess long-term risk.

Incident Type	Notification Deadline	Required Actions
Security Breach	Within 24 hours	Vendor submits preliminary breach report
Major Service Outage	Within 6 hours	Vendor provides root cause analysis (RCA)
Regulatory Violation	Immediate	Incident escalated to board & APRA notified within 72 hours
Data Leak or Breach	Within 24 hours	Vendor submits risk impact assessment

How SecurityScorecard Enhances Incident Response:

- **Real-Time Incident Alerts**: Detects third-party breaches, zero-day vulnerabilities, and compliance violations.
- **Automated Incident Response Workflows**: Supports structured remediation tracking, supplier engagement, and resolution management.
- **Regulatory Compliance Reporting**: Facilitates incident documentation and reporting to help align with APRA's operational risk governance expectations.

By integrating structured escalation workflows and rapid incident management, organizations can achieve compliance with CPS 230's operational risk mandates, mitigating third-party security failures before they escalate.

3.3 Conduct Regular Testing of Critical Third-Party Suppliers

CPS 230 mandates regular cybersecurity and operational resilience testing of critical third-party suppliers, including:

- **Penetration Testing** to identify security weaknesses.
- **Business Continuity Simulations** to assess supplier response capabilities.
- **Cybersecurity Resilience Exercises** to evaluate preparedness against evolving threats.

3.3.1 Defining Tolerance Levels for Disruptions

To align with CPS 230's resilience requirements, organizations must define **Maximum Allowable Downtime (MAD), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO)** for critical third-party suppliers. These benchmarks help ensure that disruptions do not exceed

acceptable levels and allow organizations to enforce contractual business continuity expectations.

Required Tolerance Thresholds:

- **Tier 1 Suppliers (High-Criticality Vendors)**:
  - Maximum Downtime: **4 hours**
  - RTO: **4-6 hours**
  - RPO: **15 minutes - 1 hour**
    - Compliance Requirement: **Annual resilience testing & attestation**
  - **Tier 2 Suppliers (Moderate-Criticality Vendors)**:
    - Maximum Downtime: **12 hours**
    - RTO: **12-24 hours**
    - RPO: **6-12 hours**
    - Compliance Requirement: **Biennial resilience testing & attestation**
  - **Tier 3 Suppliers (Low-Criticality Vendors)**:
    - Maximum Downtime: **24-48 hours**
    - RTO: **48-72 hours**
    - RPO: **24-48 hours**
    - Compliance Requirement: **Risk-based resilience testing**

These thresholds should be embedded into vendor contracts, risk assessment frameworks, and compliance monitoring programs.

How SecurityScorecard Supports Third-Party Resilience Testing:

- **Continuous Vulnerability Assessments**: Identifies and prioritizes remediation for security gaps.
- **Compliance Assessment Tools**: Automates evidence collection to validate supplier adherence to CPS 230 security mandates.
- **Penetration Testing & Tabletop Exercises**: Supports real-world attack simulations to ensure third-party preparedness.

By integrating continuous testing and compliance verification, organizations can strengthen vendor resilience and regulatory compliance, while ensuring disruptions remain within acceptable thresholds.

3.4 Maintain a Central Repository for Third-Party Documentation

CPS 230 requires organizations to maintain a centralized risk documentation repository to store vendor-related information, including:

- **Contracts and security agreements**.
- **Risk assessment reports and compliance records**.
- **Incident response plans and resilience testing results**.

Documenting Disruption Tolerance Levels

To ensure CPS 230 compliance, organizations must maintain structured documentation on

vendor-specific disruption tolerance levels:

- **Service-Level Agreements (SLAs)**: Document vendor compliance with **RTO, RPO, and MAD benchmarks**.
- **Resilience Testing Reports**: Store periodic business continuity simulation results and penetration testing data.
- **Vendor-Specific Disruption Policies**: Maintain detailed records on expected recovery timeframes, fallback mechanisms, and failover testing outcomes.

How SecurityScorecard Enhances Documentation Management:

- **Centralized Document Repository**: Stores and organizes critical third-party documentation with advanced search and tagging.
- **Vendor System of Record**: Maintains supplier-specific risk levels, data access permissions, and lifecycle status.
- **Evidence Locker**: Ensures vendors can upload and manage compliance artifacts to streamline audits and regulatory reporting.

By maintaining a well-structured repository, organizations can have audit readiness, compliance validation, and enhanced risk visibility for CPS 230 compliance while reinforcing business continuity obligations with critical third-party providers.

3.5 Report on TPRM Activities to Senior Management and the Board

CPS 230 requires organizations to regularly report on third-party risk management (TPRM) activities to senior management and the board. These reports must include:

- **Risk posture updates** on critical third-party suppliers.
- **Key operational risks and compliance deviations**.
- **Incident reporting and mitigation status**.
- **Audit & Assurance Findings**: Summary of vendor control testing results, compliance gaps, and remediation progress.

How SecurityScorecard Supports TPRM Reporting:

- **Board-Level Risk Dashboards**: Provides executive insights, compliance tracking, and benchmarking data.
- **Customizable Compliance Reports**: Generates structured board reports, CISO briefings, and vendor risk summaries.
- **Cyber Risk Quantification**: Financially quantifies cyber risk exposure for better risk-informed decision-making.
- **Audit & Compliance Tracking**: Enhances regulatory reporting by centralizing vendor audit documentation and risk analysis.

By integrating continuous monitoring, structured incident response, and board-level reporting, organizations can have full alignment with CPS 230's operational risk and resilience mandates, with enhanced oversight on vendor audit and assurance activities.

SecurityScorecard Implementation Best Practices for CPS 230 Compliance

1.1 Identify All Critical Third-Party Suppliers

1.1.1 Bulk Company Import in SecurityScorecard

To align with CPS 230's third-party risk management (TPRM) requirements, organizations must establish a comprehensive inventory of critical third-party suppliers. The fastest way to achieve this in SecurityScorecard is through the bulk company import feature:

1. **Export Your Supplier List:** Extract a complete list of suppliers from CRM, GRC, or procurement applications. Prioritize critical third parties based on their impact on business operations.
2. **Ensure File Compatibility:** Convert the export to a CSV or spreadsheet format for seamless import into SecurityScorecard.
3. **Include Key Risk Attributes.** Ensure your dataset includes:
    - Company domain or name
    - Supplier contact details
    - Business impact rating
    - Risk level classification
    - Data access permissions and shared data types
    - Business unit ownership
4. **Use Pre-Built Upload Template:** Download the bulk upload template from SecurityScorecard *(Portfolios → All Companies → Add Companies → Bulk Import → Download Template)*.
5. **Format and Upload the Data**: Adjust the exported data to match SecurityScorecard's template and complete the upload *(Portfolios → All Companies → Add Companies → Bulk Import)*.

By structuring third-party data effectively, organizations can enhance operational risk transparency and streamline compliance with CPS 230's supplier risk identification mandates.

1.1.2 Automatic Vendor Detection (AVD)

CPS 230 emphasizes the proactive identification of third-party risks, including fourth-party supplier dependencies. SecurityScorecard's Automatic Vendor Detection (AVD) *(My Organization → My Scorecard → Vendor Detection)* enhances this process by:

1. **Generating an AVD List:** Automatically identifies third-party suppliers based on external internet activity and risk indicators.
2. **Validating the Vendor List:** Organizations can cross-reference detected vendors against existing supplier databases.
3. **Importing Additional Suppliers:** SecurityScorecard allows organizations to import and track missing suppliers identified through AVD, ensuring a complete risk assessment ecosystem.

AVD helps organizations meet CPS 230's continuous oversight expectations, reducing the risk of

unmonitored supplier dependencies.

1.1.3 Integrations and REST API

SecurityScorecard's integrations and REST API *(Automation → Integrations)* capabilities enable organizations to seamlessly integrate third-party risk management (TPRM) functions into CPS 230-aligned workflows. Key benefits include:

- **SecurityScorecard MarketPlace:** Pre-built integrations with:
  - GRC (Governance, Risk & Compliance) platforms
  - SIEM (Security Information and Event Management) solutions
  - ITSM (IT Service Management) tools
  - Collaboration platforms (e.g., Microsoft Teams, Slack)
- **Automation and Risk Workflows:** Automate third-party risk scoring, alerts, and remediation tracking, ensuring proactive compliance with CPS 230 risk mandates.
- **Custom REST API Solutions:** Organizations can use the SecurityScorecard REST API to:
  - Extract real-time security ratings for vendor assessment.
  - Integrate risk data with internal compliance dashboards.
  - Build automated workflows for incident management and remediation tracking.

By leveraging integrations and APIs, organizations can realize risk monitoring, automated compliance enforcement, and centralized vendor governance.

1.2 Classify Critical Third-Party Suppliers Based on Their Impact on Business Operations

1.2.1 Aligning Classification with CPS 230

Under CPS 230, organizations must classify critical third-party suppliers based on their operational impact, regulatory risk, and resilience requirements. The classification ensures that risk management controls are applied appropriately based on the potential impact of supplier failure on an organization's ability to provide critical services.

1.2.2 Using SecurityScorecard for Third-Party Classification

SecurityScorecard enables organizations to effectively classify third-party suppliers in alignment with CPS 230 requirements, ensuring continuous risk tracking and compliance enforcement.

Classifying Vendors Based on Key CPS 230 Factors

When determining the business impact classification, organizations should consider:

- **The Type of Data Accessed:** Vendors handling sensitive, regulated, or confidential data (e.g., personal data, financial records, intellectual property) require higher security scrutiny.
- **Criticality of the Supplier's Service:** Vendors delivering essential services, such as banking, financial transactions, cloud computing, and IT infrastructure, require enhanced risk monitoring.
- **Operational Impact in Case of Disruption:** If a supplier's failure would cause a business continuity breach, leading to service outages or regulatory violations, they must be

categorized as high-risk.

- **Cybersecurity and Compliance Posture:** Evaluate a supplier's history of security breaches, regulatory compliance violations, and risk trends, ensuring that risk tiers accurately reflect real-world exposure.

SecurityScorecard supports supplier classification through:

- **Risk-Based Tiering:** Assign suppliers a Business Impact Attribute (Low, Medium, High, Critical) based on operational exposure and cybersecurity posture.*(All companies or portfolio views Business Impact column)*
- **Custom Business Attributes:** Enables mapping of suppliers to business-critical operations, ensuring risk controls are prioritized for high-impact vendors. *(All Companies → Edit icon on the right, or access individual company Scorecard → Edit Details)*

1.2.3 SecurityScorecard Tools for Third-Party Classification

Using Questionnaires for Vendor Risk Tiering

SecurityScorecard enables organizations to classify vendors using automated questionnaires *(Communication → Questionnaires)* that assess:

- **Data access and sensitivity levels.**
- **Cybersecurity policies, frameworks, and certifications.**
- **Vendor risk maturity based on industry benchmarks.**

Security Ratings for Vendor Classification

- **Real-Time Cybersecurity Ratings:** Organizations can classify vendors based on their latest risk scores.
- **Historical Risk Trends:** Monitors vendor security improvements or deteriorations over time.
- **Threat Exposure Analysis:** Uses data-driven insights to map high-risk vendors for enhanced oversight.

Grouping Companies into Portfolios for Risk Management

To enhance vendor classification, SecurityScorecard allows organizations to create risk-based supplier portfolios *(Companies → Portfolios)*, enabling:

- **Tier-Based Compliance Monitoring:** Automatically assigns alerts, monitoring rules, and remediation workflows based on risk tiering.
- **Portfolio-Based Risk Intelligence:** Enables organizations to track risk across critical, high, medium, and low-risk vendors.
- **Business Unit-Based Supplier Oversight:** Segments vendors by business ownership, ensuring clear accountability.

By leveraging SecurityScorecard's classification, continuous monitoring, and portfolio-based risk intelligence, organizations can align their third-party risk management strategies with CPS 230, ensuring full regulatory compliance and enhanced operational resilience.

1.3 Conduct Risk Assessments for Critical Third-Party Suppliers (CPS 230 Compliance)

1.3.1 High-Level Third-Party Risk Assessment Using SecurityScorecard Portfolios

CPS 230 mandates that APRA-regulated entities maintain a structured approach to third-party risk assessment, ensuring continuous oversight and compliance enforcement. Organizations should use SecurityScorecard Portfolios to assess their third-party ecosystem and prioritize high-risk vendors for further evaluation.

Overview of Portfolio Risk Analysis

- **Provides a consolidated risk overview** of all third-party suppliers.
- **Displays portfolio-wide risk ratings**, grade distribution, and top security concerns.
- **Uses real-time monitoring** and alerts to track vendors with declining security postures.
- **Leverages visual risk mapping** tools such as scatter plots to track security posture shifts.

Vendor Detection and Supply Chain Risk Analysis

- SecurityScorecard's Automatic Vendor Detection (AVD) under Portfolio view **aggregates fourth-party supplier dependencies**, ensuring extended supply chain risk visibility.
- **Identifies widely used but potentially vulnerable vendors** across the supply chain.
- **Enables proactive risk mitigation** by providing actionable risk intelligence and insights.

Threat Intelligence for CPS 230 Compliance

SecurityScorecard provides **Supply Chain Risk Intelligence (SCRI)** based on:

1. **Malware and Ransomware Infections**
2. **Exploitable Vulnerabilities (Critical and weaponized CVEs)**
3. **Breach Exposure Data**
4. **High-Risk Products & Zero-Day Threats**
5. **Cloud Provider and Geolocation Risks**

Organizations can filter and prioritize vendors based on recent security breaches, compliance deviations, or identified vulnerabilities, helping to gain alignment with CPS 230's risk mitigation mandates.

1.3.2 Company-Based Risk Assessment for CPS 230 Compliance

Organizations must conduct company-specific risk assessments to validate vendor compliance with CPS 230. SecurityScorecard provides automated and manual validation methods to assess risk.

1.3.2.1 Security Ratings-Based Assessment

- **Real-Time Security Ratings** based on external risk indicators.
- **Historical Risk Trends** showing stability or deterioration over time.
- **Recent Cybersecurity Incidents** and their potential impact.
- **Compliance Certifications** & Security Artifacts stored in the Evidence Locker.

- **Critical Risk Factors** and Breach Exposure Assessment.

Key CPS 230 Validation Criteria:

- **Minimum Score Compliance:** Vendors must meet organizational security thresholds (e.g., B-grade or higher).
- **No Recent Breaches or Critical Vulnerabilities:** Ensures a stable and resilient security posture.
- **Parent-Subsidiary Risk Alignment:** Ensures oversight of hierarchical security risks.

1.3.2.2 Compliance Validation for Third-Party Suppliers

CPS 230 requires organizations to validate vendor compliance with key regulatory frameworks. SecurityScorecard automates compliance validation through:

- **Evidence Locker:** Vendors can proactively upload certifications, penetration test results, and compliance artifacts.
- **Regulatory Mapping:** Automatically maps vendor risk data to major compliance frameworks, including ISO 27001, NIST, PCI-DSS, NIS 2, DORA and other Industry-Specific Regulatory Standards

Using Automated Compliance Validation

- Click Start Initial Assessment in the vendor profile.
- Select Compliance from the SecurityScorecard navigation menu.
- Choose relevant CPS 230-aligned frameworks such as NIS 2 or DORA and view validation status.

Interpreting Compliance Results

- **White:** No data or evidence available. Additional evidence can be requested using the Evidence Locker.
- **Blue:** Compliance met based on available evidence.
- **Red:** Conflicting security findings indicating a potential non-compliance risk.

By leveraging automated compliance mapping, organizations can efficiently track vendor adherence to CPS 230 requirements and reduce regulatory audit workloads.

1.3.2.3 Vendor Questionnaire Assessments

SecurityScorecard enables organizations to conduct supplier-driven security assessments through structured questionnaire workflows.

When to Use Vendor Questionnaires

- Required for all critical third parties.
- Selectively applied to high-risk vendors or those with a declining security posture.

How to Send Questionnaires

- Via Company Compliance Assessments (SecurityScorecard → Compliance → Send Questionnaire).
- From the Vendor Ratings Page (More → Send Questionnaire).
- Via Communications → Questionnaires in the SecurityScorecard dashboard.

Configuring Questionnaires

- Use customized questions to align with specific risk policies.
- Define recipients, deadlines, and response tracking metrics.
- Automate reminder emails to ensure timely responses.

Review and Validation of Supplier Responses

- Compare questionnaire results against real-time risk scores.
- Use SecurityScorecard's automated validation tools to flag discrepancies.
- Generate a finalized assessment report, outlining:
    - Key security gaps and action plans.
    - Vendor commitments for remediation.
    - Compliance adherence status and audit trail.

By integrating automated risk assessments, compliance tracking, and structured questionnaire workflows, organizations can work towards full CPS 230 compliance while strengthening third-party risk governance and resilience.

1.4 Identify Fourth-Party Aggregated Risk (CPS 230 Compliance)

1.4.1 Enhancing Visibility into Fourth-Party Risk

Under CPS 230, organizations must extend risk assessment beyond direct third-party suppliers to fourth-party service providers. This ensures that businesses identify concentration risks, systemic vulnerabilities, and critical service dependencies within their supply chain ecosystem.

1.4.2 SecurityScorecard's Automatic Vendor Detection (AVD) for Fourth-Party Risk

SecurityScorecard provides Automated Vendor Detection (AVD) to map and monitor fourth-party relationships. Organizations can utilize AVD at both the company level and portfolio level to enhance compliance with CPS 230.

Company-Level AVD

- Available directly from an individual Scorecard page, allowing users to:
    - **View detected third-party suppliers** and their security ratings.
    - **Extend risk visibility to fourth-party suppliers**, displaying connections, dependencies, and risk scores.
    - **Track security posture shifts in real-time**, ensuring risk mitigation.

Portfolio-Level AVD

- **Enables a holistic view of aggregated fourth-party risk** across a defined portfolio of

vendors.

- Provides filtering capabilities to:
    - **Identify third-party suppliers relying on the same fourth-party**, highlighting concentration risk.
    - **View a comprehensive list of impacted third-party vendors** if a fourth-party supplier experiences a security breach.
- **Helps organizations implement risk-aware decision-making** by prioritizing remediation for high-impact supply chain dependencies.

1.4.3 Continuous Monitoring of Fourth-Party Suppliers

To fully comply with CPS 230's operational resilience mandates, organizations should create dedicated portfolios for commonly used fourth-party suppliers. This enables:

- **Ongoing security posture monitoring** and risk-based alerting.
- **Automated incident notifications i**n the event of a fourth-party security breach.
- **Strategic risk assessments** to proactively address weak links within the extended supply chain.

By leveraging SecurityScorecard's AVD capabilities, organizations can implement a CPS 230-aligned fourth-party risk management strategy, ensuring continuous visibility, risk mitigation, and regulatory compliance across their supply chain ecosystem.

1.5 Document the Results of Risk Assessments and Develop Risk Mitigation Plans (CPS 230 Compliance)

Under CPS 230, organizations must maintain clear records of third-party risk assessments and define structured risk mitigation strategies to address identified vulnerabilities and compliance gaps.

1.5.1 Assessment Findings Report

Once a supplier assessment has been completed (Ratings, Compliance, Questionnaire), organizations must formally document findings, policy violations, and remediation actions.

Documenting Risk Findings

- **Questionnaire-Based Reports:** Findings reports are linked to an issued questionnaire. If no questionnaire was sent, findings can still be recorded under Vendor Details.
- **Report Contents:**
    - **Identified risks** (cybersecurity, operational, and compliance).
    - **Policy or contract violations** that require remediation.
    - **Risk classification** (Low, Medium, High, Critical) to prioritize follow-up actions.
    - **Final recommendations:** Recommend, Recommend with Conditions, or Do Not Recommend.

Accessing & Generating Reports

1. Navigate to 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 record-keeping and audits.
4. A combined assessment report template (Available in 2025) will be introduced for assessments even if no questionnaire has been issued.

1.5.2 Company-Specific Summary and PDF Reports

Organizations can generate customized vendor reports that align with CPS 230 reporting requirements.

Generating Vendor Reports

- **One-Page Summaries & Detailed Reports:** Generate concise summaries or in-depth security analyses of third-party vendors.
- **How to Generate:**
    1. Go to *Company Scorecard Overview → More → Generate a Report*.
    2. Select a report type (e.g., risk overview, compliance summary, security posture analysis).
    3. Download the report as PDF for board reporting or internal tracking.

1.5.3 Reporting Center

Organizations can use SecurityScorecard's Reporting Center to centralize CPS 230 compliance documentation.

- **Location:** Automation → Reporting Center.
- **Pre-Built & Custom Templates:** Organizations can select templates for board-level risk summaries or technical due diligence reports.
- **Export Options:** Reports can be exported as PDF, CSV, JSON, ensuring easy integration into compliance tracking tools.
- **Storage:** Reports are automatically stored in Reporting Center → Generated Reports for 30 days, facilitating audit readiness.

1.5.4 Document Center (Available in 2025)

CPS 230 requires organizations to maintain structured third-party documentation for risk tracking and regulatory reporting. SecurityScorecard's Document Center (available 2025) will serve as a centralized repository for:

- **Assessment Findings Reports**
- **Third-party security questionnaires**
- **Vendor contracts and compliance certifications**

Until the Document Center is released, organizations should store compliance documentation externally and reference records in Vendor Details Notes.

1.5.5 Action Plans for Risk Mitigation

CPS 230 mandates that organizations implement structured risk remediation plans for third-party

vendors that fail to meet security and compliance thresholds.

Creating an Action Plan

- **Navigate to Communication → Action Plans** or create an Action Plan directly from a vendor's scorecard.
- **Define compliance targets**, e.g., if a supplier's security rating falls below a B grade, trigger a remediation plan.
- **Assign remediation steps**, define deadlines, responsible parties, and escalation procedures.
- **Share the plan with the vendor**, allowing them to access their scorecard, track remediation progress, and submit compliance evidence.

Tracking Vendor Remediation Progress

- The Action Plans dashboard provides a real-time summary of vendor progress on assigned remediation tasks.
- Organizations can set reminder notifications for overdue tasks, ensuring timely security improvements.

2.1 Incorporate CPS 230 TPRM Requirements into Contracts with Critical Third-Party Suppliers

CPS 230 requires organizations to embed operational risk, cybersecurity, and resilience requirements into third-party contracts. This ensures continuous monitoring, compliance enforcement, and regulatory oversight.

Structuring Vendor Contracts for CPS 230 Compliance

- **Security Ratings Compliance:** Vendors must maintain a SecurityScorecard rating of B or higher.
- **Risk Factor Ratings Minimums:**
  - No individual security risk factor should fall below a C rating.
  - No unresolved High Breach Risk Issues.
- **Questionnaire Validation Score:** Vendors must achieve a minimum validation score of 75%.
- **Remediation Timelines:**
  - 90-Day Remediation Requirement for critical findings or compliance violations.
  - Evidence of remediation progress must be provided within the defined period.

How SecurityScorecard Automates Contract Compliance Monitoring

SecurityScorecard enables organizations to embed security clauses directly into vendor contracts and automate compliance tracking.

- **APIs and Integrations:** Automatically enforce compliance clauses via integration with contract management systems.
- **Live Risk Monitoring:** Continuous security posture tracking ensures vendors meet CPS

230-mandated risk controls.

- **Breach Notification and Incident Response Obligations:** Organizations can set up automated alerts for any vendor security breaches, compliance failures, or critical security events.

By ensuring contractual enforcement of CPS 230 TPRM requirements, organizations reduce regulatory exposure, improve vendor accountability, and maintain a resilient third-party risk management framework.

2.2 Monitor Compliance with Contractual Requirements (CPS 230 Alignment)

2.2.1 Custom Compliance Frameworks

Purpose:

CPS 230 mandates that APRA-regulated entities establish contract-based security validation frameworks to ensure ongoing compliance with operational risk and third-party resilience requirements. Organizations must create custom compliance frameworks based on contractual security obligations, business continuity expectations, and APRA-aligned security benchmarks.

Functionality:

- **Track, validate, and enforce** contractual security obligations across all critical suppliers.
- **Automated non-compliance flagging** to identify security posture deviations and enforce corrective actions.
- **Define custom validation criteria** and automate compliance verification.

Implementation Steps:

1. **Define CPS 230-aligned compliance criteria** for vendors (e.g., minimum security ratings, response time for breach resolution, mandatory risk assessments).
2. **Import compliance rules** into SecurityScorecard's Custom Compliance Frameworks.
3. **Automate security compliance validation** for all vendors under contract.

2.2.2 Continuous Monitoring of Third-Party Compliance

Organizations must continuously monitor third-party security postures to detect compliance violations and security weaknesses that may impact operational resilience.

SecurityScorecard enables organizations to:

- **Define risk-based compliance rules** that trigger alerts when vendors violate contractual terms.
- **Monitor all critical suppliers in real-time** to detect emerging risks and compliance deviations.
- **Automate enforcement actions** by linking compliance violations to structured action plans.

Accessing Rule Builder:

1. **Navigate to**: *Automation → Rule Builder.*
2. **Apply in Portfolios:** Within a Portfolio, select “Rules” in the right-side menu.

Rule Attributes:

- **Name:** Clear rule name (e.g., "Vendor Risk Drop Alert").
- **Trigger:** Event-based triggers (e.g., security rating drops below B, new breach detected).
- **Scope:** Apply rules to monitored third-party suppliers or specific vendor tiers.
- **Action:** Define responses (e.g., email alert, escalation to SIEM, automated vendor assessment).

Scope & Limitations:

- **All critical vendors** in portfolios can be fully monitored and alerted.
- **Unmonitored vendors (not in a portfolio)** receive basic monitoring (e.g., overall grade drop alerts, new breach notifications).
- **Advanced rule enforcement** *(Available 2025)* (e.g., policy-based auto-remediation) applies to monitored vendors only.

Examples of Supplier Policy Alerts:

1. **Unmonitored Vendors:** Notify on overall security grade dropping below B or new breach detection.
2. **All Monitored Vendors:** Alert on security grade < B, factor grade < C, or critical breach findings.
3. **Critical Third-Party Suppliers:** Advanced monitoring on specific factor score drops (e.g., IP Reputation, Info Leak, Hacker Chatter).

Notifications & Integrations:

- **Alerting Options:** Email notifications, webhook triggers, and integrations with SIEM, ITSM, Microsoft Teams, Slack.
- **Automated Action Plans:** If a supplier’s security rating falls below a defined threshold (e.g., B to C), initiate an automated action plan requiring remediation and compliance validation.

2.2.3 Portfolio Policies (Available in 2025)

Overview:

- Portfolio Policies will introduce automated supplier tiering based on contractual compliance mandates.
- Ensures continuous vendor security posture monitoring based on risk-tiered policies.
- Automates policy-driven oversight and enforcement for compliance.

Automation Features:

- Integrates directly with rule-based enforcement systems to escalate compliance violations.
- Enables contract-aligned security audits and vendor tiering adjustments.

- Expands compliance tracking to certification validation (e.g., ISO 27001, SOC 2, APRA standards).

By leveraging SecurityScorecard's automated monitoring and compliance enforcement, organizations can work towards third-party risk governance that fully aligns with CPS 230 operational risk mandates, reducing regulatory exposure and improving supply chain resilience.

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 CPS 230 requirements, 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 the earlier section, you can promptly detect changes in the risk landscape. Additionally, creating Action Plans allows you to collaborate with suppliers on remediation and track their progress to meet CPS 230 compliance requirements.

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, operational impact, containment 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 to align with CPS 230's operational risk mandates.

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 risk assessments.

Assessment Questionnaires:

A CPS 230-aligned supplier questionnaire should validate disaster recovery plans, cybersecurity resilience, vulnerability assessment processes, and cybersecurity incident response capabilities, including their review and testing frequency.

Penetration Testing & Simulations:

SecurityScorecard also offers penetration testing and real-world tabletop exercises to assess vendor preparedness for operational disruptions.

3.4 Maintain a Central Repository for All Third-Party-Related Documentation

CPS 230 mandates that organizations maintain a comprehensive Third-Party Risk Register, capturing all contractual agreements with third parties, including:

Required Information:

- **Supplier Identification:** Name, unique identifier (e.g., ABN/ACN), 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., CPS 230, APRA guidelines), 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 CPS 230's cybersecurity resilience requirements and maintain a comprehensive, up-to-date register of third-party information that can be exported when needed and used as part of regulatory reporting obligations.

Supplier Details (Vendor System of Record):

- Add and update most required fields during onboarding or afterward.
- Current version includes a fixed field set. Custom fields will be available in 2025, allowing for a comprehensive CPS 230-specific field set.

Collecting Additional Information:

- Use custom questionnaires to gather details on subcontractors, compliance status, or cybersecurity risk mitigation processes.
- Store questionnaires and assessment results in the 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).
- Link documentation to specific vendors for easy tracking and compliance audits.

Vendor & Portfolio Exports:

- Export supplier information as a CSV via UI or API for easy reporting on supplier status and regulatory compliance tracking.

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

CPS 230 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 sensitive data.

SecurityScorecard helps organizations meet CPS 230 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 executive leadership to technical teams, covering both cybersecurity risks and third-party risk performance.
- **Fully customizable reports:** Reports can be tailored to align with CPS 230 reporting requirements, ensuring they include critical information on cybersecurity resilience, risk mitigation plans, and vendor compliance.
- SecurityScorecard assistance is available to ensure the reports meet CPS 230's regulatory 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 CPS 230's third-party governance mandates.
- **API Exports:** For seamless integration with existing reporting or GRC systems, SecurityScorecard offers a robust API to export data directly into third-party risk tracking systems, ensuring continuous monitoring, tracking, and regulatory compliance.

.