Prevalent™

The Third-Party Risk Management Compliance Handbook

Part II: Industry Standards & Guidelines

An Important Note to Readers

This white paper reviews the key third-party risk management requirements noted in common regulatory and security frameworks, and then maps the capabilities of the Prevalent™ Third-Party Risk Management Platform to those requirements to illustrate the power of a unified solution to achieve compliance while mitigating vendor risks.

This paper should not be considered legal or regulatory advice. Organizations should undertake their own regulatory evaluation and address requirements in partnership with their auditors.

Table of Contents

Executive Summary

As businesses continue to diversify and globalize, organizations looking to focus squarely on core business functions are turning to third parties to fulfill specialized services, such as web hosting, payments processing, and cloud services. Although this provides significant cost benefits, this extended ecosystem is nonetheless rife with escalating threats to data privacy, security, and company reputation.

Data breaches and cybersecurity risks are impacting companies at an alarming rate, with the supply chain at the center of many targeted attacks. According to a recent Ponemon study, 51% of U.S. companies said they experienced a data breach caused by one of their vendors or other third parties. And although cybersecurity risks tend to capture the most attention in the press, more than half of organizations report not tracking risks related to vendor performance management; environment, social and governance (ESG) issues; and anti-bribery and corruption (ABAC) – where failures can lead to regulatory fines and brand damage.

In the face of growing threats, regulators and governing bodies are taking notice. An increase in third-party regulations, along with the accompanying scrutiny from auditors, has obligated organizations to develop effective third-party risk management programs to meet compliance mandates and deepen IT security controls.

This two-part paper reviews the key third-party risk management requirements noted in major government regulations (Part I) and industry guidelines and standards (Part II). It then maps the capabilities of the Prevalent Third-Party Risk Management Platform to those requirements to illustrate the power of a unified solution to achieve compliance while mitigating third-party vendor risks.

Complying with TPRM Regulations, Guidelines and Standards

Regardless of industry, corporate compliance and reporting is an essential part of everyday operations. Ensuring internal adherence to regulations, guidance, and industry standards is complex and challenging at best (especially when manually handled with spreadsheets). Tack on compliance mandates related to third parties, vendors, business associates, and supply chain partners, and the burden of managing data risk takes an entirely new trajectory.

To comply with regulations, guidlelines and standards in this paper, your organization should adopt a third-party risk management (TPRM) program. This includes a multi-step approach where you:

1. Set the rules of third-party engagement based on your organization's risk tolerance and data security and privacy policies
2. Include these rules, as well as auditing requirements, in all third-party contracts
3. Evaluate third parties via risk assessments* in the form of questionnaires or surveys, and for performance against contractual service level agreements
4. Continuously monitor third parties to verify compliance
5. Remediate deficiencies

*Risk assessments are not only a key step, but also mandatory for most legislation. They provide an inside-out approach to determine vendor compliance with IT security controls, data privacy requirements, ESG and labor practices while ensuring that third parties meet the same levels of compliance as your organization. Any third-party risk management program that fails to include an internal, control-based risk assessment is a non-starter for regulatory compliance.

Summary Tables

All regulations, guidelines, and industry standards listed below require the use of internal, control-based third-party risk assessments. While outside-in risk scoring or ranking can deliver risk insights, it will not meet compliance requirements when used as the only mechanism to evaluate vendor risk. Pairing both assessments and monitoring is preferred, but at a minimum, you must assess vendors.

Part I: Government Regulations

Download Part I here.

Authority	Regulation	Assessment Required	Monitoring Required
CA	California Consumer Privacy Act (CCPA)	✅	⛔
	Transparency in Supply Chains Act	✅	✅
EBA	Guidelines on Outsourcing Arrangements	✅	✅
EU	European Corporate Due Diligence Act	✅	✅
	GDPR	✅	⛔
FCA	FG 16/5	✅	✅
HHS	HIPAA Security Rule	✅	⛔
NERC	CIP-013-1 R1 & R2	✅	⛔
NY	23 NYCRR 500	✅	✅
	SHIELD Act	✅	✅
OCC	Bulletin 2013-29	✅	✅
	Bulletin 2017-21	✅	✅
SEC	Foreign Corrupt Practices Act	✅	✅
UK	Anti-Bribery Act	✅	✅
	Modern Slavery Act	✅	✅
US DoD	Cybersecurity Maturity Model Certification (CMMC)	✅	✅

Part II: Industry Guidelines and Standards (this document)

Authority	Guideline or Standard	Assessment Required	Monitoring Required
Guidelines			
CSA	CSA Consensus Assessments Initiative Questionnaire (CAIQ)	✅	⛔
FFIEC	BCP Booklet: Appendix J	✅	✅
	Information Security Booklet	✅	⛔
Industry Standards			
AICPA	Service Organization Control (SOC) 2	✅	⛔
ISO	27001:2013	✅	✅
	27002:2013	✅	✅
	27018:2019(E)	✅	✅
	27036-2:2014(E)	✅	✅
NIST	CSF 1.1	✅	✅
	SP 800-53R4	✅	⛔
	SP 800-161	✅	✅
PCI Security Standards Council	PCI DSS	✅	⛔

How Prevalent Solutions Address Third-Party Compliance Requirements

Prevalent offers a unified third-party risk management platform that enables you to better reveal, interpret and alleviate risk. Delivered in the simplicity of the cloud, the Prevalent platform combines automated vendor assessment with continuous threat monitoring to simplify compliance, reduce security risks, and improve efficiency. Key capabilities include:

- A library of 75+ pre-defined, customizable assessment questionnaires, backed by automated capabilities for gathering and analyzing vendor data
- Bi-directional remediation workflows to facilitate risk management and mitigation, with complete audit trails for all vendor communications and risk decisions
- A central reporting console for visualizing compliance and risk status across the vendor landscape
- Deep data security auditing and business monitoring capabilities that enable you to move beyond tactical network health reporting to reveal critical operational, financial, legal and brand risks

With Prevalent, you gain a 360-degree view of vendor risk – both inside-out and outside-in – for managing regulatory compliance and aligning with industry standards and guidelines.

Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ)

This brief chapter addresses the CSA's questionnaire for assessing security controls in infrastructure-as-a-service, platform-as-a-service and software-as-a service applications. While organizations are not required by law to abide by the results of a CAIQ audit, the CAIQ assessment is widely utilized by organizations looking for a standard approach to evaluating the security controls of a cloud provider.

CAIQ Summary

The Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) provides a set of questions across 16 control domains that the CSA recommends should be asked of a cloud provider, for example those that offer IaaS, PaaS or SaaS applications. The CAIQ was developed to create a commonly accepted industry standard to document security controls, and therefore provides questions that can then be used for cloud provider selection and security evaluation. As of the writing of this white paper, the current CSA CAIQ standard is v4.0.1.

The CAIQ contains a series of 295 yes or no questions that can be customized to fit an individual cloud customer's need. The questionnaire is designed to support organizations when they interact with cloud providers during the cloud providers' assessment process by giving organizations specific questions to ask about the providers operations and processes. As well, cloud providers can use the CAIQ to outline their security capabilities and security posture in a standardized way using the terms and descriptions considered to be best practices by the CSA.

Assessments have been designed to follow two approaches:

1. The full CAIQ survey captures the 16 control domains across 295 questions.
2. A CAIQ-Lite survey has been created to capture the same 16 control domains, but at a reduced scope, with 73 questions used.

The aim with this approach is to enable organizations to select the most appropriate model that best fits their needs for assessing their cloud service providers.

Meeting CAIQ Guidance for Third-Party Risk Management

Prevalent has created two surveys, one representing the full CAIQ, and the other CAIQ-Lite. The full CAIQ survey has been split into individual control groups representing the 16 control domains. This is to allow for customization of the survey to suit the needs to individual customers dependent on their appetite for their assessing cloud providers. The Prevalent approach to hosting both questionnaires in our Third-Party Risk Management Platform has several benefits:

- **Simpler reporting:** Results of CAIQ assessments are aligned to core security standards, including NIST, ISO 27001, CoBiT 5, so that by using the Prevalent Platform you can address multiple cloud security reporting requirements in a single assessment.
- **Tiered assessments:** Questionnaires are customizable to suit the requirements of each cloud customer, with CAIQ-Lite beneficial for cloud service providers deemed "low risk" (for example based on accessibility to sensitive data).
- **Faster turnaround:** The reduced question set in CAIQ-Lite allows for a quicker turnaround time for assessment completion, speeding time to resolution and focusing your team on remediating risks.

The Prevalent Difference

CSA standards require robust management and tracking of third-party risk. Prevalent can help address the requirements in the CAIQ by:

- Automating the end-to-end process of collecting and analyzing CAIQ surveys, speeding and simplifying assessments, compliance, and due diligence review.
- Deliver clear reporting beyond a score, tying risks to business outcomes and helping to make better risk-based decisions, prove compliance, and prioritize resources.
- Meet industry standards and ensure third-party risk management regulatory compliance targets for cyber risk, InfoSec, and data privacy.
- Centralize TPRM functions, delivering a single view that provides single repository for effective reporting to satisfy audit and compliance requirements.
- Utilize a consistent, repeatable, proven methodology, enabling a scalable, more mature vendor risk management program.

As your organization seeks to migrate more workloads to the cloud, assessing third parties will be essential. Prevalent can help by centralizing vendor assessments across a range of requirements.

Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook

This chapter addresses the importance of the FFIEC IT Examination Handbook as a valuable tool for financial firms.

While organizations are not required by law to abide by the guidelines set forth in the 11 FFIEC booklets, the agencies that make up the FFIEC prescribe best practices and a standardized approach for all field examiners conducting audits. Financial institutions should use these as a blueprint when preparing for an examination.

FFIEC IT Examination Handbook Summary

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to establish guidelines and uniform principles and standards for the federal examination of financial institutions by five member agencies. These include:

- Board of Governors of the Federal Reserve System (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Consumer Financial Protection Bureau (CFPB)

FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions.

The FFIEC has created a set of handbooks or booklets to be used by examiners looking at an institution's IT practices, and as such, provide guidelines for those practices. These handbooks cover many subjects including Audit, Business Continuity Planning (BCP), Information Security, Outsourcing Technology Services, and other topics. Each area is covered in detail and provides guidance from the Board of Directors level to practitioners. Of interest for many institutions is the guidance they provide on how to manage the risk associate with third-party providers. The Business Continuity booklet includes an Appendix J, addressing the need to strengthen the resilience of outsourced technology services, and the Information Security booklet includes a specific section on Oversight of Third-Party Service Providers.

These IT Booklets require robust management and tracking of third-party supplier business continuity planning (BCP) and IT security risk. They specify that a policy for managing risk should be in place, relevant due diligence should be applied in choosing third parties, and that policy should be codified in supplier agreements. Additionally, suppliers should be managed and audited according to the agreed requirements.

Meeting FFIEC IT Examination Handbook Guidance for Third-Party Risk Management

Please see the table below for a summary of the guidance set forth in FFIEC IT Examination Handbook as it relates to third-party risk management, and how Prevalent can help your organization address these requirements.

Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook	
A series of booklets on specific topics of interest to field examiners that prescribe uniform principles and standards for financial institutions.	
Business Continuity Planning Booklet Appendix J: Strengthening the Resilience of Outsourced Technology Services	How Prevalent Helps
Third Party Management "Establishing a well-defined relationship with technology service providers (TSPs) is essential to business resilience. **A financial institution's third-party management program should be risk-focused and provide oversight and controls** commensurate with the level of risk presented by the outsourcing arrangement. To ensure business resilience, **the program should include outsourced activities that are critical to the financial institution's ongoing operations.**"	The Prevalent TPRM platform enables internal control-based assessments (based on industry-standard framework questionnaires and/or custom questionnaires). This selection enables an organization to match the assessment's requirements to the level of risk presented by the relationship. In addition, the platform includes built-in workflow capabilities that enable assessors to interact efficiently with third parties during the due diligence collection and review periods.
Third Party Management – Due Diligence "As part of its due diligence**, a financial institution should assess the effectiveness of a TSP's business continuity program,** with particular emphasis on recovery capabilities and capacity. In addition, **an institution should understand the due diligence process the TSP uses for its subcontractors and service providers.** Furthermore, the financial institution should review the TSP's BCP program and its alignment with the financial institution's own program, including an evaluation of the TSP's BCP testing strategy and results to ensure they meet the financial institution's requirements and promote resilience."	Prevalent's standards-based and custom questionnaires focus on Business Continuity Planning, including impact analysis, operational risk assessment, and business recovery management. The Prevalent Assessment service examines the risk posed by both technology service providers and their subcontractors.
Third Party Management – Contracts "Right to audit: Agreements should provide for the right of the financial institution or its representatives to audit the TSP and/or to have access to audit reports. A financial institution should review available audit reports addressing TSPs' resiliency capabilities and interdependencies (e.g., subcontractors), BCP testing, and remediation efforts, and assess the impact, if any, on the financial institution's BCP."	The Prevalent TPRM platform includes effective reporting to satisfy audit and compliance requirements as well as to present findings to the board and senior management. The entire risk profile can be viewed in the centralized live reporting console, and reports can be downloaded and exported to determine compliance status. Deep reporting capabilities include filters and click-through interactive charts. The solution includes a complete repository of all documentation collected and reviewed during the diligence process.

Business Continuity Planning Booklet Appendix J: Strengthening the Resilience of Outsourced Technology Services	How Prevalent Helps
Third Party Management – Ongoing Monitoring **"**Effective ongoing monitoring assists the financial institution in ensuring the resilience of outsourced technology services. **The financial institution should perform periodic in-depth assessments of the TSP's control environment**, including BCP, through the review of service provider business continuity plan testing activities, independent and/or third-party assessments to assess the potential impact on the financial institution's business resilience. **The financial institution should ensure that results of such reviews are documented and reported by the TSP to the appropriate management oversight committee or the board of directors** and used to determine any necessary changes to the financial institution's BCP and, if warranted, the service provider contract."	The Prevalent Third-Party Risk Management platform provides a complete solution for performing assessments including questionnaires; an environment to include and manage documented evidence in response; workflows for managing the review and address findings; and robust reporting to give each level of management the information it needs to properly review the third party's performance.
Cyber Resilience "Cyber threats will continue to challenge business continuity preparedness. **Financial institutions and TSPs should remain aware of emerging cyber threats and scenarios and consider their potential impact to operational resilience.** Because the impact of each type of cyber event will vary, preparedness is the key to preventing or mitigating the effects of such an event."	The Prevalent Cyber & Business Monitoring service provides both snapshot and continuous vendor monitoring for immediate notification of high-risk issues, prioritization, and remediation recommendations. Data security and business risk monitoring enables you to look beyond tactical vendor health for a more strategic view of a vendor's overall information security risk. Prevalent is unique in that it offers business risk monitoring that leverages human analysts to interpret potential operational, brand, regulatory, legal, and financial risks. Examples of business information collected during the analysis include: • M&A activity • Layoffs • Lawsuits • Data breaches • Product recalls • Bankruptcy • Capital transactions: debt, equity

Information Security Booklet	How Prevalent Helps
II.C.20 Oversight of Third-Party Service Providers "Management should **verify that third-party service providers implement and maintain controls sufficient to appropriately mitigate risks.** The institution's contracts should do the following: • Include minimum control and reporting standards • Provide for the right to require changes to standards as external and internal environments change • Specify that the institution or an independent auditor has access to the service provider to perform evaluations of the service provider's performance against the Information Security Standards."	The Prevalent Assessment service simplifies compliance and reduces risk with automated collection and analysis of vendor surveys using industry standard and custom questionnaires. Bi-directional workflows provide back and forth communication with technology service providers to address findings and remediation efforts. Robust reporting and full audit capabilities streamlines proper performance review. Access to completed assessments and audits can be delegated to auditors via standard RBAC capabilities in the platform.

The Prevalent Difference

The goal of the FFIEC IT Examination Handbook is to heighten cybersecurity awareness for the financial industry and stress the importance of accurate cybersecurity assessments, including those for technology service providers. Adhering to these guidelines requires a full set of controls implemented across the supplier organization.

The Prevalent Third-Party Risk Management platform provides a complete framework for managing the risk posed by third-party suppliers. Automated vendor assessments, continuous threat monitoring, assessment workflow, remediation management, and audit and compliance reporting is easily accommodated from a single repository of vendor risks. As stated by the Business Continuity Planning booklet, Appendix J:

> "Many financial institutions depend on third-party service providers to perform or support critical operations. These financial institutions should recognize that using such providers does not relieve the financial institution of its responsibility to ensure that outsourced activities are conducted in a safe and sound manner. The responsibility for properly overseeing outsourced relationships lies with the financial institution's board of directors and senior management. **An effective third-party management program should provide the framework for management to identify, measure, monitor, and mitigate the risks associated with outsourcing.**"

Note: Along with the IT Examination Handbook, the FFIEC created the Cybersecurity Assessment Tool (CAT) to help financial institutions identify risks and determine cybersecurity preparedness. Use of the Assessment by institutions is voluntary, but by using the Assessment, management will be able to enhance its oversight and management of the institution's cybersecurity by doing the following:

- Identifying factors contributing to and determining the institution's overall cyber risk
- Assessing the institution's cybersecurity preparedness
- Evaluating whether the institution's cybersecurity preparedness is aligned with its inherent risks
- Determining risk management practices and controls that are needed or require enhancement and actions to be taken to achieve the desired state
- Informing risk management strategies

International Organization for Standardization (ISO) Information Security Standards

This chapter of the white paper addresses the following ISO standards:

- ISO 27001:2013: Information security management systems (ISMS) - Requirements
- ISO 27002:2013: Code of practice for information security controls
- ISO 27018:2019(E): Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO 27036-2:2014(E): Information security for supplier relationships
- ISO 27701:2019: Extension to ISO 27001 and ISO 27002 for privacy information management

ISO 27001 / 27002 / 27018 / 27036-2 / 27701 Summary

ISO 27001 is the stringent evaluation of cyber and information security practices. It provides requirements for establishing, implementing, maintaining and continually improving an information security management system. Based on an international set of requirements, it outlines a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

ISO 27002 is a supplementary standard that provides advice on how to implement the security controls listed in Annex A of ISO 27001. It helps organizations consider what they need to put in place to meet these requirements.

ISO 27018, when used in conjunction with the information security objectives and controls in ISO 27002, creates “a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor.

ISO 27036-2 is a related framework that specifies information security requirements for "defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships." This standard extends the information security requirements defined in previous ISO standards adding specific guidance to ensure secure acquirer-supplier relationships.

ISO 27701 was the first international standard on privacy information management, which helps organizations to demonstrate the methods and controls used in protecting both their internal and customers’ personal data. It augments security guidance published in ISO 27001 an ISO 27002.

With respect to managing information security in supplier relationships, **Section 15 of 27001 and 27002 summarizes the requirements for securely dealing with various types of third parties.** Using a top down, risk-based approach, the specification provides the following guidance for managing suppliers:

- Create an information security policy for supplier relationships that outlines specific policies and procedures and mandates specific controls be in place to manage risk
- Establish contractual supplier agreements for any third party that may access, process, store, communicate or provide IT infrastructure to an organization’s data
- Include requirements to address the information security risks associated with information and communications technology services and product supply chain
- Monitor, review and audit supplier service delivery
- Manage changes to the supplier services, considering re-assessment of risks

Organizations choose to become certified against these standards in order to benefit from the best practice guidance and to reassure customers and clients that their recommendations have been followed.

Clauses 6 and 7 in ISO 27036-2 define fundamental and high-level information security requirements applicable to the management of several supplier relationships at any point in that supplier relationship lifecycle.

Meeting ISO 27001 / 27002 / 27018 / 27036-2 / 27701 Third-Party Risk Management Standards

Please see the table below for a summary of ISO third-party risk management standards, and how Prevalent can help your organization address these requirements.

ISO 27001:2013: Information Security Management Systems (ISMS) - Requirements ISO 27002:2013: Code of Practice for Information Security Controls ISO 27701:2019: Extension for Privacy Information Management	
These standards set requirements for establishing, implementing, maintaining and continually improving an information security management system.	
ISO 27001 / 27002 Requirements	How Prevalent Helps
15.1 Information security in supplier relationships "Objective: To ensure protection of the organization's assets that are accessible by suppliers."	The Prevalent Assessment service offers security, privacy, and risk management professionals an automated platform to manage the supplier risk assessment process and determine third-party compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live reporting, and an easy-to-use dashboard. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels.
15.1.1 Information security policy for supplier relationships "Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented."	The Prevalent Third-Party Risk Management platform provides a complete solution for performing assessments and an environment to include and manage documented due-diligence evidence.

ISO 27001 / 27002 Requirements	How Prevalent Helps
15.1.2 Addressing security in supplier agreements "The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations . All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information."	The Prevalent Privacy Information Management Survey (PIMS) provides organizations with a comprehensive assessment based around the ISO/IEC 27701:2019 standard for privacy information management, leveraging the structure and framework of the ISO 27001:2013 standard's security controls. This brings together a detailed assessment on how an organization has implemented information security controls and applied additional privacy-based controls to manage and support the products and services being provided. The survey has been designed such that specific sections are used depending on the role an organization plays (that of a PII processor or PII controller). This survey can be used by PII controllers (including those that are joint PII controllers) and PII processors.
15.1.2 (d) "obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;"	The Prevalent solution enables internal control-based assessments (based on industry standard framework questionnaires and/or custom questionnaires). The platform includes built-in workflow capability enabling assessors to interact efficiently with third parties during the due diligence collection and review periods. Robust reporting and audit capabilities give each level of management the information it needs to properly review the third party's performance.
15.1.2 (m) "right to audit the supplier processes and controls related to the agreement;"	The Prevalent Assessment solution provides a simple, trackable, repeatable mechanism to perform controls audits.
15.1.2 (n) "defect resolution and conflict resolution processes;"	Bi-directional workflow in the Prevalent Assessment platform includes built-in discussion tools to enable communication with suppliers on remediating issues.
15.1.2 (p) "supplier's obligations to comply with the organization's security requirements."	The Prevalent Assessment solution ensures suppliers implement the exact, agreed-upon requirements with regular tracking and verification.
15.1.3 Information and communication technology supply chain "Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain."	Prevalent's TPRM platform provides a complete set of internal and external assessment and monitoring services to ensure a full view of a supplier's information, communications and product supply chain security posture.

ISO 27001 / 27002 Requirements	How Prevalent Helps
15.1.3 (d) "implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;"	The Prevalent solution includes a mechanism to perform reviews; monitor compliance with agreed policies; and audit and generate regular reports for all levels of management.
15.2 Supplier service delivery management **15.2.1 Monitoring and review of supplier services** "Organizations should regularly monitor, review and audit supplier service delivery. Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly."	The Prevalent TPRM Platform unifies internal control-based assessments (based on industry standard framework questionnaires and/or custom questionnaires) with continuous vendor threat monitoring to deliver a holistic security risk rating, enabling organizations to zero-in on the most important or impactful risks. The platform includes built-in workflow capability enabling assessors to interact efficiently with third parties during the due diligence collection and review periods.
15.2.1 (c) "conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;"	The Prevalent platform provides a simple, trackable, repeatable mechanism to perform audits along with a workflow and shared communication mechanism to track issues to resolution.
15.2.1 (g) "review information security aspects of the supplier's relationships with its own suppliers;"	The Prevalent solution provides a detailed map to visualize all relationships for each entity and other business entities (e.g., vendors / departments / datasets). This capability enables organizations to monitor the relationships between third, fourth, and Nth parties.

ISO 27018:2019(E): Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	
This standard creates a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor.	
ISO 27018 Requirements	How Prevalent Helps
15 Supplier Relationships "The objectives specified in, and the contents of, ISO/IEC 27002:2013, Clause 15 apply."	Cloud providers must be treated in the same vein as other third-party supplier relationships. The platform delivers a 360-degree view of supplier risk, including cloud providers, with clear and concise reporting tied to specific regulations and control frameworks for improved visibility and decision making.

ISO 27036-2:2014(E): Information security for supplier relationships	
This standard defines information security requirements applicable to the management of several supplier relationships at any point in that supplier relationship lifecycle.	
ISO 27036-2 Requirements	How Prevalent Helps
6 Information security in supplier relationship management 6.1.1.1 Agreement processes / Acquisition process / Objective a) Establish a supplier relationship strategy that: 1) Is based on the information security risk tolerance of the acquirer; 2) Defines the information security foundation to use when planning, preparing, managing and terminating the procurement of a product or service.	Prevalent Vendor Risk Intelligence Networks provide instant access to thousands of completed, industry-standard vendor risk profiles offering real-time security, reputational and financial information. With these insights in hand, procurement teams can contract with vendors that meet their organization's risk tolerance levels and easily compare vendors against common security criteria.
6.2.1 Organizational project-enabling processes / Life cycle model management process a) The acquirer and the supplier shall establish the life cycle model management process when managing information security in supplier relationships.	Prevalent helps to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the entire vendor risk lifecycle – from sourcing and selection to offboarding and everything in between.
6.2.2.1 Organizational project-enabling processes / Infrastructure management process / Objective a) Provide the enabling infrastructure to support the organization in managing information security within supplier relationships.	Prevalent provides a central SaaS platform that enables acquirers and suppliers to collaborate on risk reduction by automating risk assessments against more than 75 industry standards – including ISO. With the platform acquirers gain built-in workflow and remediation, automated analysis and reporting.
6.3.4.1 Project processes / Risk management process / Objective a) Continuously address information security risks in supplier relationships and throughout their life cycle including re-examining them periodically or when significant business, legal, regulatory, architectural, policy and contractual changes occur.	Prevalent Vendor Threat Monitor continuously tracks and analyzes threats to your third parties. The solution monitors the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. The solution is backed by a dedicated and custom contract assessment questionnaire that enables comprehensive reviews by identifying potential breaches of contract and other risks as the relationship progresses.

ISO 27036-2 Requirements	How Prevalent Helps
6.3.7.1 Project processes / Measurement process / Objective a) Collect, analyze, and report information security measures related to the procurement or supply of a product or service to demonstrate the maturity of information security in a supplier relationship and to support effective management of processes.	With Prevalent, acquirers can reveal supplier cyber incidents by monitoring 1,500+ criminal forums; thousands of onion pages; 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. These results can then be correlated against completed risk assessments for a more complete picture of a supplier's risk posture. With these insights, acquirers have a central risk register to manage recommended remediations and report on progress.
7 Information security in a supplier relationship instance 7.2.1 Supplier selection process / Objectives a) Select a supplier that provides adequate information security for the product or service that may be procured.	Prevalent Vendor Risk Intelligence Networks provide instant access to thousands of completed, industry-standard vendor risk profiles offering real-time security, reputational and financial information. With these insights in hand, procurement teams can contract with vendors that meet their organization's risk tolerance levels and easily compare vendors against common security criteria.
7.4.1 Supplier relationship management process / Objectives a) Maintain information security during the execution period of the supplier relationship in accordance with the supplier relationship agreement and by particularly considering the following: 4) Monitor and enforce compliance of the supplier with information security provisions defined in the supplier relationship agreement.	With the Prevalent Platform, acquirers can automatically map information gathered from control-based assessments to regulatory frameworks – including ISO and many others – to quickly visualize and address important compliance requirements at every stage of the supplier lifecycle.
7.5.1 Supplier relationship termination process / Objectives a) Protect the product or service supply during termination to avoid any information security, legal and regulatory impacts after the notice of termination; b) Terminate the product or service supply in accordance to the termination plan.	The Prevalent Third-Party Risk Management Platform automates contract assessments and offboarding procedures to reduce your organization's risk of post-contract exposure. Leverage customizable surveys and workflows report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more.

The Prevalent Difference

The ISO standards presented here require robust management and tracking of third-party supplier security risk. They specify the following:

- A policy for selecting suppliers based on information security practices should be in place;
- A policy for managing risk should be in place;
- A policy should be codified in supplier agreements; and
- Suppliers should be managed and audited to the agreed requirements.

Having strong Information Security Management Systems is part of the supplier lifecycle and requires a complete, internal view of the controls in place as well as continuous monitoring of all third parties. This cannot be addressed with a simple, external automated scan.

Prevalent's Third-Party Risk Management platform offers a complete framework for implementing policy management, auditing and reporting related to the third-party risk and supply chain compliance requirements of ISO 27001, 27002, 27018 and 27036-2.

NIST SP 800-53r4, SP 800-161 and NIST CSF v1.1 Standards and Frameworks

This chapter addresses NIST Special Publication 800-53r4, SP 800-161 and the NIST Framework for Improving Critical Infrastructure (CSF) v1.1.

NIST SP 800-53 is a regulatory document, encompassing the processes and controls needed for a government-affiliated entity to comply with the FIPS 200 certification. This chapter focuses on revision 4, chapter 2.5 External Service Providers.

NIST SP 800-161 is a supplement to SP 800-53 and provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations.

The NIST CSF is a voluntary guideline. This framework builds on, but does not replace, security standards like NIST 800-53.

NIST SP 800-53r4, SP 800-161 and NIST CSF v1.1 Summary

The National Institute of Standards and Technology (NIST) is a federal agency within the United States Department of Commerce. One of NIST's responsibilities includes establishing computer and information technology-related standards and guidelines for federal agencies. Because NIST evolved into a key resource for managing cybersecurity risks, many private sector organizations consider compliance with these standards and guidelines to be a top priority.

NIST's Special Publication (SP) 800 series presents information of interest to the computer security community. The NIST Cybersecurity Framework v1.1 realizes that specific controls and processes have already been covered and duplicated in existing standards, and thus provides streamlined, high-level guidance for improving cybersecurity defenses.

The risk framework in SP 800-53r4 consists of the following:

- Step 1: Categorize
- Step 2: Select the applicable security control baseline
- Step 3: Implement the security controls
- **Step 4: Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system**
- Step 5: Authorize information system operation
- **Step 6: Monitor the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness**

An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations. The resulting set of security controls establishes a level of security due diligence for the organization.

NIST devotes an entire section of the document – Section 2.5 External Service Providers – to discussing third-party risk. Risk is addressed by incorporating the Risk Management Framework (RMF) as part of the terms and conditions of the contracts with external providers. Organizations can require external providers to implement all steps in the RMF. In other words, assessments need to be conducted for each

external service provider, risks mitigated, and ongoing monitoring performed throughout the contract period.

The NIST Cybersecurity Framework v1.1 document is divided into the framework core, the implementation tiers, and the framework profile. The framework core describes five functions of an information security program: **identify**, **protect**, **detect**, **respond**, and **recover**. For organizations looking to establish or improve a cybersecurity program, this framework follows similar steps to that of NIST SP 800-53r4. Section 3.3, Communicating Cybersecurity Requirements with Stakeholders, explains how to use the framework to manage supply chain risk. Activities include:

- Determining cybersecurity requirements for suppliers
- Enacting cybersecurity requirements through formal agreement (e.g., contracts)
- Communicating to suppliers how those cybersecurity requirements will be verified and validated
- **Verifying that cybersecurity requirements are met through a variety of assessment methodologies**
- Governing and managing the above activities

NIST SP 800-161 presents an additional layer of supply-chain-specific guidance on top of SP 800-53, introducing a framework of framing, assessing, responding to and monitoring risks inherent in supply chain relationships across 18 control families.

For organizations worried about cyber threats, supply chain risk management is an important piece in NIST standards and frameworks.

Meeting NIST SP 800-53r4, SP 800-161 and NIST CSF v1.1 Standards and Frameworks

Please see the table below for a summary of the NIST guidance, and how Prevalent can help your organization address these requirements.

NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations	
The NIST standard establishes computer and information technology-related standards and guidelines for both federal agencies and private organizations.	
NIST SP 800-53r4 Guidelines	How Prevalent Helps
Chapter 2.5 External Service Providers "FISMA and OMB policies require that federal agencies using external service providers assure that such use meets the same security requirements that federal agencies are required to meet. Organizations can require external providers to implement all steps in the Risk Management Framework."	Prevalent offers security, privacy, and risk management professionals an automated platform to manage the vendor risk assessment process and determine vendor compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live reporting, and an easy-to-use dashboard for efficiency. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels.

NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations	
The NIST standard establishes computer and information technology-related standards and guidelines for both federal agency supply chains.	
NIST SP 800-53r4 Guidelines	How Prevalent Helps
CA-2 SECURITY ASSESSMENTS (2) SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS Supplemental ICT SCRM Guidance: Organizations may want to use a variety of assessment techniques and methodologies such as continuous monitoring, insider threat assessment, and malicious user's assessment. These assessment mechanisms are context-specific and require the organization to understand its ICT supply chain infrastructure and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.	Prevalent Vendor Threat Monitor (or VTM) continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data by monitoring the Internet and dark web for cyber threats and vulnerabilities — and correlating assessment findings with research on operational, financial, legal and brand risks. Part of the cloud-based Prevalent Third-Party Risk Management Platform, VTM is integrated with questionnaire-based assessments to deliver a comprehensive, 360-degree view of vendor security and compliance.
(3) SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS Supplemental ICT SCRM Guidance: For ICT SCRM, organizations should consider using external security assessments for system integrators, suppliers, and external service providers. External assessments include certifications and third-party assessments, such as those driven by organizations such as the International Organization for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and The Open Group Trusted Technology Forum (OTTF), if such certifications meet agency needs.	The Prevalent Platform includes more than 75 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls.
CA-7 CONTINUOUS MONITORING (3) CONTINUOUS MONITORING | TREND ANALYSES Supplemental ICT SCRM Guidance: Information gathered during continuous monitoring/trend analysis serves as input into ICT SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially can identify an ICT supply chain compromise, including insider threat.	Cyber Threat Intelligence: Reveal third-party cyber incidents for 550,000 companies by monitoring 1,500+ criminal forums; thousands of onion pages, 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases.

CP-2 CONTIGENCY PLAN (7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS Supplemental ICT SCRM Guidance: Organizations should ensure that information systems and ICT supply chain infrastructure components provided by an external service provider have appropriate failover to reduce service interruption. Organizations should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms addressing critical components and functionality support in case of denial of service to ensure continuity of operation. Organizations should coordinate with external service providers to identify service providers' existing contingency plan practices and build on them as required by the organization's mission and business needs. Such coordination will aid in cost reduction and efficient implementation.	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES (10) INCIDENT HANDLING | SUPPLY CHAIN COORDINATION Supplemental ICT SCRM Guidance: A number of organizations may be involved in managing incidents and responses for supply chain security. After an initial processing of the incident is completed and a decision is made to take action (in some cases, the action may be "no action"), the organization may need to coordinate with their system integrators, suppliers, and external service providers to facilitate communications, incident response, root cause, and corrective actions activities. Organizations should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting system integrators, suppliers, and external service providers with mature capabilities for supporting ICT supply chain incident handling is important for reducing ICT supply chain risk. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A review (and	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.

potential revision) of the agreement is recommended, based on the lessons learned from previous incidents.	
RA-1 RISK ASSESSMENT POLICY AND PROCEDURES Supplemental ICT SCRM Guidance: Risk assessments should be performed at the organization, mission/program, and system levels of the organization. The system-level risk assessment should include both the ICT supply chain infrastructure (e.g., development and testing environments, and delivery systems) and the information system/components traversing the ICT supply chain. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact to the mission, if compromised. The policy should include ICT supply chain-relevant roles applicable to performing and coordinating risk assessments across the organization (see Chapter 2 for the listing and description of roles). Applicable roles within acquirer, system integrator, external service providers, and supplier organizations should be defined.	The Prevalent Platform includes more than 75 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls. Automatically generate a risk register upon survey completion, ensuring that the entire risk profile can be viewed in the centralized, real-time reporting dashboard – and reports can be downloaded and exported to determine compliance status. This filters out unnecessary noise and zeroes-in on areas of possible concern, providing visibility and trending to measure program effectiveness. Take actionable steps to reduce vendor risk with built-in remediation recommendations and guidance.
RA-3 RISK ASSESSMENT Supplemental ICT SCRM Guidance: Risk assessments should include consideration of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Chapter 2, Integration of ICT SCRM into Risk Management. Data to be reviewed and collected includes ICT SCRM-specific roles, processes, and results of system/component implementation and acceptance. Risk assessments should be performed at Tiers 1, 2, and 3. Risk assessments at Tier 1 should be primarily a synthesis of various risk assessments performed at Tiers 2 and 3 and used for understanding the overall organizational impact.	The Prevalent Platform includes more than 75 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that maps responses to any compliance regulation or framework. All assessments are based on industry standards and address all information security topics as they pertain to supply chain partner security controls.
SA-12 SUPPLY CHAIN PROTECTION (2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS Supplemental ICT SCRM Guidance: The organization should define and implement a supplier review program to analyze system integrator, supplier, and external services provider activities where relevant.	Dedicated and custom contract assessment questionnaires enable comprehensive reviews by identifying potential breaches of contract and other risks. Gain visibility into vendor contract status, contact information, risk and compliance status, performance metrics, and more via centralized dashboards, and leverage PowerBI integration for custom reporting.

Usually, an agreement is reached between the organization and system integrators, suppliers, and/or external services providers that guides the level of traceability and visibility achievable. Organizations should be cautious in scoping the review program, as there are costs associated with data collection and keeping, managing, and analyzing the data for relevance once obtained.	Track resolution of issues throughout the remediation process to show risk reduction progress over time and report against KPIs.
8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE Supplemental ICT SCRM Guidance: Ensure that all-source threat and vulnerability information includes any available foreign ownership and control (FOCI) data. Review this data periodically as mergers and acquisitions, if affecting a supplier, may impact both threat and vulnerability information and therefore SCRM.	Cyber Threat Intelligence: Reveal third-party cyber incidents for 550,000 companies by monitoring 1,500+ criminal forums; thousands of onion pages, 80+ dark web special access forums; 65+ threat feeds; and 50+ paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases. Business Updates: Access qualitative insights from over 550,000 public and private sources of reputational information, including M&A activity, business news, negative news, regulatory and legal information, operational updates, and more. Financial Insights: Tap into financial information from a global network of 365 million businesses. Access 5 years of organizational changes and financial performance, including turnover, profit and loss, shareholder funds, etc. Screen new vendors, monitor existing vendors, and evaluate their health for informed sourcing decisions. Adverse Media Screening: Avoid working with corrupt businesses and individuals by screening them against an extensive database of profiles linked to illicit activities. By consolidating intelligence from 30,000 global news sources, Prevalent enables fast and comprehensive screening to protect your company and its reputation. Global Sanctions Lists: Simultaneously screen against important sanctions lists (e.g., OFAC, EU, UN, BOE, FBI, BIS, etc.), plus over 1,000 global enforcement lists and court filings (e.g., FDA, US HHS, UK FSA, SEC, etc.) to proactively identify prohibited relationships. State-Owned Enterprise Screening: Check companies against a proprietary list of government-owned and government-linked enterprises to avoid conflicts of interest. Politically Exposed Persons (PEP) Screening: Demonstrate your commitment to fighting corruption and bribery by screening against a global PEP database. With access to over 1.8 million politically exposed person profiles, including their families and

	associates, Prevalent enables you to instantly identify potential vulnerabilities. Breach Event Notification Monitoring: Access a database containing 10+ years of data breach history for thousands of companies around the world. Includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications.

NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1	
The NIST guidance provides high-level guidance for improving cybersecurity defenses.	
NIST CSF v1.1 Guidelines	How Prevalent Helps
Supply Chain Risk Management (ID.SC) **ID.SC-2:** Suppliers and third-party partners of information systems, components, and services are **identified, prioritized, and assessed using a cyber supply chain risk assessment process.**	Prevalent offers security, privacy, and risk management professionals an automated platform to manage the vendor risk assessment process and determine vendor compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live reporting, and an easy-to-use dashboard for efficiency. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels. In addition to facilitating automated, periodic internal control-based assessments, the platform also provides cyber security and business monitoring – continually assessing the third-party networks to identify potential weaknesses that can be exploited by cyber criminals. Prevalent also offers penetration testing as-a-service to help customers investigate vendor network operations at a much more granular level. With the integration of internal assessments, external cyber monitoring and penetration testing, organizations gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.
Supply Chain Risk Management (ID.SC) **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	The Prevalent Assessment solution can implement customized questionnaires that verify the vendor is meeting the detailed requirements of the contract.

NIST CSF v1.1 Guidelines	How Prevalent Helps
Supply Chain Risk Management (ID.SC) ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	The Prevalent Third-Party Risk Management platform includes effective reporting to satisfy audit and compliance requirements as well as to present findings to the board and senior management. The entire risk profile can be viewed in the centralized live reporting console, and reports can be downloaded and exported to determine compliance status. Deep reporting capabilities include filters and click-through interactive charts. The solution includes a complete repository of all documentation collected and reviewed during the diligence process.
Supply Chain Risk Management (ID.SC) ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	In addition to facilitating automated, periodic internal control-based assessments, the platform also provides cyber security and business monitoring – continually assessing the third-party networks to identify potential weaknesses that can be exploited by cyber criminals. Prevalent also offers penetration testing as-a-service to help customers investigate vendor network operations at a much more granular level. With the integration of internal assessments, external cyber monitoring and penetration testing, organizations gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.

The Prevalent Difference

NIST requires robust management and tracking of third-party supply chain security risk. SP 800-53r4, SP 800-161 and CSF v1.1 specify that a policy for managing risk should be in place; security controls should be selected; a policy should be codified in supplier agreements where appropriate; and suppliers should be managed and audited to the requirements and controls. In the simplest terms, an organization needs to establish and implement the processes to identify, asses and manage supply chain risk.

Delivered in the simplicity of the cloud, the Prevalent platform provides deep, internal control-based assessments to help determine supplier compliance with IT security controls and data privacy requirements. Findings and remediation management between an organization and its suppliers ensure that required controls remain aligned with a company's own risk appetite and tolerance levels.

This inside-out view of suppliers complies with the frameworks and standards set forth by NIST. Ratings companies that provide an outside-in approach to risk go no further than draw assumptions about the likelihood of issues based on outside information. The rating does nothing to actually determine what controls are in place, or what IT security and data privacy policies and procedures a supplier follows.

Payment Card Industry Data Security Standard (PCI DSS)

This chapter addresses the Payment Card Industry Data Security Standard (PCI DSS), specifically version 3.2.1 released in January 2019.

PCI DSS Summary

PCI DSS was developed to enhance cardholder data security and to facilitate the broad adoption of consistent data security measures globally. The standard applies to all entities that store, process or transmit cardholder data. With 12 requirements across six areas, the standard aims to ensure that organizations have the proper controls and procedures in place to secure cardholder data.

Specific to third-party risk management, PCI DSS requirements are applicable to organizations that have outsourced 1) their payment operations, or 2) the management of systems (such as routers, firewalls, databases, physical security, and/or servers) that are involved in transmitting, housing or protecting cardholder data. Those third parties are therefore responsible for ensuring that the data is protected per the applicable PCI DSS requirements.

It's crucial for third parties to show compliance with PCI DSS requirements, and that's where an internal controls assessment is essential – offering a survey with specific PCI requirement questions and the ability to include applicable agreements and contracts as evidence along with the answers. If a third party performs a PCI DSS assessment, they should:

> "…provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place."[1]

All service providers with access to cardholder data – including shared hosting providers – must adhere to PCI DSS; shared hosting providers must protect each entity's hosted environment and data. This chapter of the paper focuses specifically on those hosting provider requirements.

Meeting PCI DSS Requirements

Please see the table below for a summary of the third party-related PCI DSS guidance, and how Prevalent can help your organization address these requirements. For the purposes of this white paper (and considering the breadth of the PCI standard) only requirements 12.8 and 12.9 are reviewed. With regard to and Appendix A1 (Additional PCI DSS Requirements for Shared Hosting Providers), the requirement and associated testing procedures can be accomplished through assessments available in the Prevalent platform.

Please be sure to review the entire PCI DSS standard to determine how each requirement applies to your business.

[1] Payment Card Industry (PCI) Data Security Standard, v3.2.1 © 2006-2019 PCI Security Standards Council, LLC

Payment Card Industry (PCI) Data Security Standard	
To enhance cardholder data security and to facilitate the broad adoption of consistent data security measures globally.	
PCI DSS Guidelines	How Prevalent Helps
Requirement 12: Maintain a policy that addresses information security for all personnel. 12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: 12.8.1 Maintain a list of service providers including a description of the service provided.	Prevalent offers an internal automated qualification assessment that enables you to gather required details about all entities your organization is working with from all departments. Prevalent utilizes standardized rule-based profiling and tiering logic to help risk and security teams understand the scope of their vendors. Through a combination of information collection and specific tiering questions, Prevalent leverages data interaction, financial, regulatory and reputational considerations to inform tiering. This process ensures that third parties are assessed properly according their importance to the organization and provides a central repository for vendor management.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Prevalent enables organizations to centralize agreements, contracts and supporting evidence with built-in task and acceptance management, plus mandatory upload features. A dedicated contract assessment in the platform raises risks related to the achievement of contract clauses. Visualizing breaches of certain contract requirements or clauses ensures that organizations have the insights they need when renewing contracts.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Prevalent delivers a customized PCI assessment that incorporates all 12 requirements, with built-in workflow to ensure the entire process – from survey collection and analysis to risk identification and reporting – is automated and efficient.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually	Prevalent offers a customizable survey to gather and analyze performance data, delivering a single repository of all third-party vendor evidence.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Prevalent enables organizations to centralize agreements, contracts and supporting evidence.

PCI DSS Guidelines	How Prevalent Helps
Requirement 12: Maintain a policy that addresses information security for all personnel. 12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Prevalent enables organizations to centralize agreements, contracts and supporting evidence with built-in task and acceptance management, plus mandatory upload features. A dedicated contract assessment in the platform raises risks related to the achievement of contract clauses. Visualizing breaches of certain contract requirements or clauses ensures that organizations have the insights they need when renewing contracts.

The Prevalent Difference

Prevalent can help address the third-party requirements published in the PCI standard by:

- Assessing third-parties using a comprehensive PCI assessment built-in to the Prevalent platform.
- Automatically generating a risk register once a survey has been completed, filtering out any unnecessary noise and zeroing-in on areas of possible concern.
- Matching documentation or evidence against risks and vendors, creating an audit trail for review.
- Reporting against PCI compliance.
- Identifying relationships between your organization and third parties to discover dependencies and visualize information paths.

With advisory, consulting and managed services, organizations that need to assess their third parties for PCI compliance can be assured of best practices with Prevalent.

Service Organization Control (SOC) 2

SOC 2 Summary

Service Organization Control (SOC) 2 is a standard that is designed to provide assurance that an organizations' systems are set up to cover the security, availability, processing integrity, confidentiality, and privacy of customer data.

These five core subject areas are commonly known as Trust Service Principles. The purpose of a SOC 2 (also referred to as a Type 2 report) is for an organization to detail the operational effectiveness of their systems, based on the five principles outlined above. To achieve compliance against a SOC 2 assessment, organizations must develop a clear documentation framework, built around security policies, security procedures and supporting documentation.

The five principles are further defined to account for criteria common to all five of the trust service categories (common criteria) and additional specific criteria for the availability, processing integrity, confidentiality and privacy categories. Clear objectives of each principle are set out within the Trust Services Criteria and provide an organization with clear expectations to look for when validating or verifying security controls.

Meeting SOC 2 Requirements

Please see the table below for a summary of the SOC 2 requirements, and how Prevalent can help your organization address these requirements as they pertain to third-party risk management.

Service Organization Control (SOC) 2	
SOC 2 reports provide assurance over an organizations' systems are securely managing its customer data.	
SOC 2 Trust Service Criteria	How Prevalent Helps
Requirement CC1.1: (Illustrative Control): "Roles and responsibilities for privacy and data governance are defined and communicated to personnel as well as to third parties."	Prevalent offers the ability to profile your customer base, to determine roles and responsibilities in manging privacy and data governance, and how it relates to the scope of product or service provisioning. Prevalent can deliver this through the utilization of standardized rule-based profiling and tiering logic to help risk and security teams understand the scope of their vendors. This process ensures that third parties are assessed properly according their importance to the organization and provides a central repository for vendor management.
Requirement CC3.1: (Illustrative Control): The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Prevalent enables organizations with an automated platform to manage the vendor risk assessment process, including the setting of risk impact scoring, based on risk acceptance criteria and tolerance levels.

SOC 2 Trust Service Criteria	How Prevalent Helps
Requirement C1.2 (Illustrative Control): Personal information involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	Prevalent enables organizations to centralize agreements, contracts and supporting evidence that can include records and documents pertinent to could be used to validate how third-party providers consider privacy requirements when accessing personal information pertinent to the organization

The Prevalent Difference

Prevalent can help address the third-party requirements published through SOC 2 reporting by:

- Assessing third parties using a comprehensive SOC2-based assessment built-in to the Prevalent platform.
- Automatically generating a risk register once a survey has been completed, filtering out any unnecessary noise and zeroing-in on areas of possible concern.
- Matching documentation or evidence against risks and vendors, creating an audit trail for review.
- Reporting against SOC2 compliance.
- Providing mapping across industry leading standards for a holistic approach to verifying information and cyber security compliance

With advisory, consulting and managed services, organizations that need to assess their third parties for SOC2 compliance can be assured of best practices with Prevalent.

Conclusion

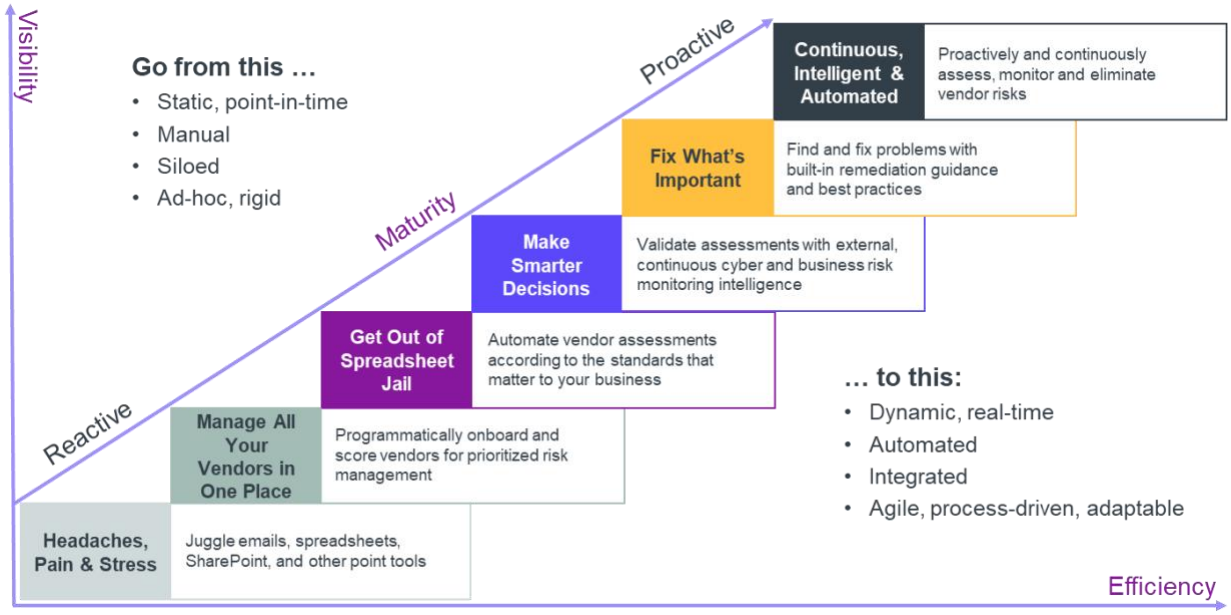
Regulatory compliance is an important driver of third-party risk management program design and implementation. While regulatory guidance varies slightly across governing authorities and standards bodies, all agree that conducting a risk assessment, with proper due diligence before and during the lifecycle of each business relationship, is a critical step to reducing third-party risks. These risk assessments are not only mandated under most regulations but can also be a key tool for organizations as they develop stronger data and privacy security measures.

Monitoring-only solutions that deliver scores and security ratings are a helpful companion to internal control-based risk assessments, but alone, do not meet the compliance obligations of the most commonly referenced regulations and standards.

Companies that do not follow mandatory regulatory compliance practices face numerous possible repercussions, including hefty fines and penalties.

A Path to Maturing and Optimizing Your Third-Party Risk Management Program

By partnering with Prevalent, organizations are able to effectively adapt to the ever-changing regulatory landscape for third-party risk management. Our recommend approach follows best practices guidance for a closed-loop third-party risk management program.



Prevalent's proven, five-step process ensures greater TPRM visibility, efficiency and scale.

With Prevalent, you can mature your third-party risk management program from reactive, low-visibility, and low-efficiency, to a proactive, intelligent and agile. Key steps include:

1) **Manage all your vendors in one place:** The first step is to take control of your third-party ecosystem by onboarding vendors and getting a picture of their inherent risk. You can do that yourself, or you can have Prevalent do it for you.

2) **Get out of spreadsheet jail:** Next, get out of spreadsheet jail with an automated assessment solution that enables everyone to collaborate on industry-standard questionnaires. Again, you're welcome to do that yourself, or Prevalent can do it for you.

3) **Make smarter decisions:** Then, validate assessment responses against external cyber security scores and business risk intelligence from continuous monitoring across thousands of public and private sources.

4) **Fix what's important:** Next, prioritize and fix what's important to your organization by consulting a centralized risk register that unifies assessment data and monitoring intelligence for each vendor.

5) **Continuous, intelligent and automated:** Finally, this gets you to a place where the third-party risk management process is much more predictable and proactive, with continuous risk insights informing your assessment cadence.

Following this process enables you to not only able to reveal potential compliance issues, but also adhere to the TPRM lifecycle recommended by most regulatory bodies. By combining automated vendor assessments with continuous risk monitoring, you gain a 360-degree, "inside-out / outside-in," view of third-party risk. This results more secure, more compliant operations between your organization and its vendors, suppliers and business partners.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time..

To learn more, please visit www.prevalent.net.