Prevalent™

The Third-Party Risk Management Compliance Handbook

The Complete Reference Guide

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, guidelines 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

Authority	Regulation	Assessment Required	Monitoring Required
Bank of England PRA	Supervisory Statement SS2/21 Outsourcing and Third-Party Risk Management	✅	✅
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

Authority	Guideline or Standard	Assessment Required	Monitoring Required
Guidelines			
CSA	CSA Consensus Assessments Initiative Questionnaire (CAIQ)	✅	⛔
FFIEC	BCP Booklet: Appendix J	✅	✅
	Information Security Booklet	✅	⛔
OSFI	Guideline B-10	✅	✅
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 800-53r5	✅	⛔
	SP 800-66r2	✅	✅
	SP 800-161r1	✅	✅
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 100+ 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.

Part I: Regulatory Requirements

Bank of England Prudential Regulatory Authority (PRA) Supervisory Statement SS2/21 Outsourcing and Third-Party Risk Management

This chapter of the white paper addresses how the PRA SS2/21 requires business resilience oversight by financial institutions doing business with third parties.

PRA SS2/21 Summary

In March 2022, the Bank of England's Prudential Regulatory Authority (PRA) activated a new Supervisory Statement (SS2/21), which set expectations for how PRA-regulated firms should comply with regulatory requirements relating to outsourcing and third-party risk management.

Applicable to all UK banks, investment and insurance firms, and UK branches of overseas banks and insurance firms, the objectives of the Supervisory Statement (SS) are to:

> *"… facilitate greater resilience and adoption of the cloud and other new technologies … complement the requirements and expectations on operational resilience in the PRA Rulebook; SS1/21 … and implement the European Banking Authority (EBA) 'Guidelines on outsourcing arrangements' (EBA Outsourcing GL)."*

The Supervisory Statement clarifies the difference between material outsourcing and non-outsourcing third-party arrangements, sets expectations for assessments and third-party due diligence, and identifies areas that require detailed examination, including:

- Data security
- Access, audit and information rights
- Sub-outsourcing
- Business continuity and exit strategies

Supervisory Statement SS2/21 requires that PRA-regulated firms conduct a Materiality Assessment for each vendor during onboarding and periodically thereafter. PRA expects to be informed of each firm's material third parties, so now is the time to ensure your third parties follow the business and operational resilience practices necessary to be compliant and minimize risk to your organization.

Meeting PRA SS2/21 Requirements

The summary table below maps capabilities in the Prevalent Third-Party Risk Management Platform to select outsourcing and non-outsourcing third-party requirements.

NOTE: This table is a summary of the most relevant requirements only, and it should not be considered comprehensive, definitive guidance. For a complete list of requirements, please review the complete Supervisory Statement in detail and consult your auditor.

Prudential Regulatory Authority Supervisory Statement 2/21 Outsourcing and Third-Party Risk Management	
Facilitate greater business and operational resilience.	
PRA SS2/21 Requirement	How Prevalent Helps
2 Definitions and scope	
2.8 "In line with the expectations in Chapter 4 of this SS, firms may implement a holistic, single third party risk management policy covering outsourcing and non-outsourcing third party arrangements. Alternatively, they may have separate policies on each of those respective areas provided that they are aligned, consistent, effective, and suitably risk-based."	The Prevalent Third-Party Risk Management Platform simplifies the management of third parties, enabling organizations to unify and automate the critical tasks required to identify, assess, manage, continuously monitor, and remediate third-party security, privacy, compliance and operational risks across every stage of the vendor lifecycle. The solution delivers: • Profiling, tiering, and inherent and residual risk scoring based on comprehensive criteria to identify material and non-material outsourcing third parties • More than 100 standardized templates and custom risk assessments tuned to material and non-material third parties with built-in workflow, task and evidence management • Remediation management with built-in guidance to act on identified risks from material outsourcing third parties • Compliance and risk reporting by framework or regulation to simplify the auditing process
2.9 "The following standards apply to all third party ICT arrangements: […] relevant legal requirements and standards on ICT security (e.g., Cyber Essentials Plus) and data protection, including but not necessarily limited to General Data Protection Regulation (GDPR) and the Data Protection Act 2018."	The Prevalent Platform includes a library of more than 100 questionnaire templates that address a multitude of ICT security-based frameworks, including Cyber Essentials, ISO 27001, NIST 800-53, GDPR, and many others.
3 Proportionality	
3.6 "Depending on its level of control and influence in respect of intragroup outsourcing arrangements, a firm may, for example:	The Prevalent TPRM Platform enables security and risk management teams to automatically tier suppliers according to their inherent risk scores. Results can be used to

PRA SS2/21 Requirement	How Prevalent Helps
• adjust its vendor due diligence, although firms should still carefully assess whether a potential service provider that is part of its group has the ability, capacity, resources, and appropriate organisational structure to support the performance of the outsourced function or third party service; • …"	set appropriate levels of further due diligence and determine the scope of ongoing assessments.
3.7 "Where relevant, firms may be able to leverage compliance with existing requirements in other areas of regulation to help meet their regulatory obligations in respect of their intragroup outsourcing arrangements."	The Prevalent Platform automatically maps information gathered from control-based assessments to regulatory frameworks including ISO 27001, GDPR and dozens more. This enables you to quickly visualize and address important compliance requirements and simplify auditing processes. Customers can also choose to use the Prevalent Compliance Framework (PCF), a single, comprehensive assessment that enables security and risk management teams to map answers to several regulatory requirements.
5 Pre-outsourcing phase	
5.8 "Firms are responsible for assessing the materiality of their outsourcing and third party arrangements. Materiality may vary throughout the duration of an arrangement and should therefore be (re)assessed: • prior to signing the written agreement; • at appropriate intervals thereafter, eg during scheduled review periods; • where a firm plans to scale up its use of the service or dependency on the service provider; and/or • if a significant organisational change at the service provider or a material sub-outsourced service provider takes place that could materially change the nature, scale, and complexity of the risks inherent in the outsourcing arrangement, including a significant change to the service provider's ownership or financial position."	The Prevalent Platform enables organizations to assess, monitor and remediate risks at all stages of the third-party lifecycle. Key capabilities include: • RFx management, enabling organizations to automate and add risk intelligence to vendor selection decisions • Contract lifecycle management, delivering automation to improve the vendor contracting experience and conduct continuous SLA monitoring • The largest library of standardized and custom risk assessments with built-in workflow, tasks, and evidence management for regular risk assessments • Native cyber, breach, business, reputational and financial risk monitoring to continuously assess vendor risks between annual assessments and correlate findings against assessment

PRA SS2/21 Requirement	How Prevalent Helps
	results to determine if further investigation is needed
5.10 "Firms should develop their own processes for assessing materiality as part of their outsourcing or third party risk management policy (see Chapter 4)."	The Prevalent Platform automates the identification, assessment, analysis, ongoing monitoring and remediation of third-party risks at every stage of the vendor lifecycle – from selection to offboarding. The Platform includes an extensive library of assessment templates, including those to determine the materiality of a third-party arrangement and the risks involved.
5.11 "Consistent with the definition of 'material outsourcing' in the PRA Rulebook and, where applicable, the criteria in the EBA Outsourcing GL, a firm should generally consider an outsourcing or third party arrangement as material where a defect or failure in its performance could materially impair the: • financial stability of the UK; • firms': o ability to meet the Threshold Conditions; o compliance with the Fundamental Rules; o requirements under 'relevant legislation' and the PRA Rulebook;36 o safety and soundness, including its: ▪ financial resilience, ie assets, capital, funding, and liquidity; or ▪ operational resilience, ie its ability to continue providing important business services; o for insurers only, the: ▪ ability to provide an appropriate degree of protection for those who are or may become policyholders in line with the PRA's statutory objectives; and	The Prevalent TPRM Platform automates the assessment, continuous monitoring, analysis, and remediation of outsourcing and non-outsourcing third-party business resilience and continuity – while automatically mapping results to NIST, ISO, and other control frameworks to demonstrate compliance. To complement business resilience assessments and validate results, Prevalent: • Automates continuous cyber monitoring to predict possible third-party business impacts • Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability • Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns

PRA SS2/21 Requirement	How Prevalent Helps
▪ requirement not to undermine the 'continuous and satisfactory service to policyholders' in line with Conditions Governing Business 7.2. o OCIR and if applicable, resolvability."	
5.12 "The PRA also expects firms to classify an outsourcing arrangement as material if the service being outsourced involves an: • entire 'regulated activity', eg portfolio management; or • 'internal control' or 'key function', unless the firm is satisfied that a defect or failure in performance would not adversely affect the relevant function."	Prevalent enables organizations to classify third parties based on multiple criteria, including: • Type of content required to validate controls • Criticality to business performance • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and implications • Reputation An effective tiering and categorization process enables organizations to assess third parties according to their criticality to business operations, while informing further due diligence efforts.
5.13 "The PRA expects firms to have regard to all applicable criteria in Table 5 below, both individually and in conjunction, when assessing the materiality of an outsourcing or third party arrangement not otherwise covered by paragraphs 5.8 and 5.9. Although in practice many material outsourcing and third party arrangements involve ICT products or services (eg cloud), the presence of a given ICT product or service does not, in itself, automatically render an outsourcing arrangement material. *Recreated from Table 5:* Direct connection to the performance of a regulated activity.	The Prevalent Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices. This enables organizations to: • Categorize suppliers according to their risk profile and criticality to the business • Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) • Centralize system inventory, risk assessments, RACI charts, and third-party company profiles • Ensure consistent communications with suppliers during business disruptions

PRA SS2/21 Requirement	How Prevalent Helps

Size and complexity of relevant business area(s) or function(s).
 	
The potential impact of a disruption, failure, or inadequate performance on the firm's:
• business continuity, operational resilience, and operational risk, including:
  ○ conduct risk;
  ○ ICT risk;
  ○ legal risk; and
  ○ reputational risk.
• ability to:
  ○ comply with legal and regulatory requirements;
  ○ conduct appropriate audits of the relevant function, service, or service provider; and
  ○ identify, monitor, and manage all risks
• obligations under
  ○ the PRA Rulebook;
  ○ the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity of the institution or payment institution and its clients, including but not limited to GDPR and the Data Protection Act 2018
• counterparties, customers, or policyholders.
• early intervention, recovery and resolution planning, OCIR, and resolvability.
 	
The firm's ability to scale up the outsourced service.
 	
Ability to substitute the service provider or bring the outsourced service back in-house, including	

PRA SS2/21 Requirement	How Prevalent Helps
estimated costs, operational impact, risks, and timeframe of an exit in stressed and non-stressed scenarios."	
5.18 "The PRA expects firms to conduct appropriate due diligence on the potential service provider before entering into an outsourcing arrangement, and to identify a suitable alternative or back-up providers where available. If no alternative or back-up providers for a material outsourcing arrangement are available, firms should consider alternative business continuity, contingency planning, and disaster recovery arrangements to ensure they can continue providing relevant important business within their impact tolerances in the event of material disruption at their chosen service provider (see Chapter 10)."	Prevalent RFx Essentials centralizes and automates the distribution, comparison, and management of requests for proposals (RFPs) and requests for information (RFIs). RFx Essentials makes it easy for procurement teams to not only select solutions and vendors that meet the organization's functionality and risk requirements, but also take a critical first step in managing risk throughout the third-party lifecycle. Prior to selecting the vendor, Prevalent enables teams to compare and monitor vendor demographics, fourth-party technologies, ESG scores, recent business and reputational insights, data breach history, and financial performance. Organizations can also take advantage of the Prevalent Vendor Intelligence Networks, which are on-demand libraries of thousands of vendor risk reports based on security, privacy, business resilience and operational risks. Prevalent Vendor Networks are continuously updated and populated with supporting evidence.
5.19 "In the case of material outsourcing, the PRA expects firms' due diligence to consider the potential providers': • business model, complexity, financial situation, nature, ownership structure, and scale; • capability, expertise, and reputation; • financial, human, and technology resources; • ICT controls and security; and • sub-outsourced service providers, if any, that will be involved in the delivery of important business services or parts thereof."	The Prevalent Platform includes 100+ pre-defined assessment templates including standardized information security vendor risk assessment questionnaires, as well as business resilience, GDPR, FCA, ISO 27001, Modern Slavery, Anti-Bribery, Health & Safety, Financial Performance, Management & Ethics and more. Prevalent Vendor Threat Monitor continuously tracks and analyzes external threats to 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. Prevalent manages centralized vendor profiles that unify demographics, Modern Slavery statements, ESG scores, and mapped fourth parties.
5.20 "The due diligence should also consider whether potential service providers:	

PRA SS2/21 Requirement	How Prevalent Helps
• have the authorisations or registrations required to perform the service; • comply with GDPR, the Data Protection Act, and other applicable legal and regulatory requirements on data protection; • can demonstrate certified adherence to recognised, relevant industry standards; • can provide, where applicable and upon request, relevant certificates and documentation (eg data dictionaries); and • have the ability and capacity to provide the service that the firm needs in a manner compliant with UK regulatory requirements (including in the event of a sudden spike in demand for the relevant service, for instance as a result of a shift to remote working during a pandemic). A 'general' track-record of previous performance may not be sufficient evidence by itself."	Prevalent integrates and correlates continuous monitoring and profile insights against assessment results to provide a central location to view and act on risks.
5.21 "In line with Risk Control 3.4(2) and Risk Management 3.1, firms should, in a proportionate manner, assess the potential risks of all third party arrangements, including outsourcing arrangements, regardless of materiality. As part of the risk assessment, the PRA expects firms to consider: • operational risks based on an analysis of severe but plausible scenarios, for instance a breach or outage affecting the confidentiality and integrity of sensitive data and/or availability of service provision (see Chapter 10); and • financial risks, including the potential need for the firm to provide financial support to a material outsourced or sub-outsourced service provider in distress or take over its business, including as a result of an economic downturn ('step-in' risk)."	The Prevalent Third-Party Incident Response Service enables teams to rapidly identify and mitigate the impact of third-party vendor breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance. Customers can also access a database containing 10+ years of data breach history for thousands of companies around the world. The database includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications. Combined with continuous cyber monitoring, it provides organizations with a comprehensive view of external information security risks that can impact operations. Prevalent taps into financial information from a global network of 2 million businesses. This includes 5 years of organizational changes and financial performance, such as turnover, profit and loss, shareholder funds, and other data useful for evaluating company health and viability.

PRA SS2/21 Requirement	How Prevalent Helps
5.22 "The PRA expects firms to carry out risk assessments in the circumstances referred to in paragraph 5.6 and also if they consider that there may have been a significant change to an outsourcing arrangement's risks due to, for instance, a serious breach/continued breaches of the agreement or a crystallised risk."	Prevalent continuously tracks and analyzes external threats to 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 Platform offers access to a database containing 10+ years of data breach history for thousands of companies around the world. The database includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications. These capabilities help to fill gaps in between regular third-party risk assessments, with results triggering automated actions such as additional assessments and remediations.
5.23 "A firm's risk assessment should balance any risks that the outsourcing arrangement may create or increase against any risks it may reduce or enable the firm to manage more effectively (for instance, a firm's resilience to disruption). The assessment should also take into account existing or planned risk mitigation, eg staff procedures and training."	The Prevalent Platform includes built-in remediation recommendations to accelerate risk mitigations with third parties. Organizations can use the platform to communicate with vendors and coordinate remediation efforts, as well as capture and audit conversations; record estimated completion dates; accept or reject individual assessment responses; assign tasks based on risks, documents or entities; and match documentation and evidence to risks.

5.24 "The PRA expects firms and groups to periodically (re)assess and take reasonable steps to manage:
• their overall reliance on third parties; and
• concentration risks or vendor lock-in at the firm or group, due to:
  ○ multiple arrangements with the same or closely connected service providers;
  ○ fourth party/supply chain dependencies, for instance, where multiple otherwise unconnected service providers depend on the same sub-contractor for the delivery of their services;
  ○ arrangements with service providers that are difficult or impossible to substitute; and/or
	Prevalent mitigates concentration risks by identifying fourth-party relationships through a native identification assessment or by passively scanning the third party's public infrastructure. The resulting relationship map depicts information paths and dependencies that could open pathways into an environment.
	
	Suppliers discovered through this process are monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening.

PRA SS2/21 Requirement	How Prevalent Helps
○ concentration of outsourcing and other third party dependencies in a close geographical location, such as one jurisdiction. This type of concentration may arise even if a firm uses multiple, unconnected third party service providers, for instance, a business process outsourcing or offshoring hub."	
6 Outsourcing agreements	
6.3 "Firms should ensure that written agreements for non-material outsourcing arrangements include appropriate contractual safeguards to manage and monitor relevant risks. Moreover, regardless of materiality, firms should ensure that outsourcing agreements do not impede or limit the PRA's ability to effectively supervise the firm or outsourced activity, function, or service."	Prevalent Contract Essentials centralizes the distribution, discussion, retention, and review of vendor contracts. It also includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With Contract Essentials, organizations can centrally track all contracts and contract attributes that can impact service levels, effectively enforcing contractual safeguards.
7 Data security	
Prevalent delivers a single, collaborative platform for conducting privacy assessments and mitigating both third-party and internal privacy risks. Key data security and privacy assessment capabilities include: • Scheduled assessments and relationship mapping to reveal where personal data exists, where it is shared, and who has access to it – all summarized in a risk register that highlights critical exposures. • Privacy Impact Assessments to uncover at-risk business data and personally identifiable information (PII) – enabling you to analyze the origin, nature and severity of risk and get remediation guidance. • Vendor assessments against GDPR and other privacy regulations via the Prevalent Compliance Framework (PCF) – enabling you to reveal potential hot spots by mapping identified risks to specific controls. • GDPR risk and response mapping to controls – equipping you with percent-compliance ratings and stakeholder-specific reports. • 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. • Centralized onboarding, distribution, discussion, retention, and review of vendor contracts. This ensures data protection provisions are enforced from the beginning of the relationship.	

PRA SS2/21 Requirement	How Prevalent Helps
8 Access, audit, and information rights	
8.7 "Firms may use a range of audit and other information gathering methods, including: • offsite audits, such as certificates and other independent reports supplied by service providers; and • onsite audits, either individually or in conjunction with other firms (pooled audits)."	The Prevalent Controls Validation Service reviews third-party assessment responses and documentation against established testing protocols to validate that indicated controls are in place. Prevalent experts first review assessment responses, whether from custom or standardized questionnaires. We then map the responses to SIG, SCA, ISO, SOC II, AITECH, and/or other control frameworks. Finally, we work with you to develop remediation plans and track them to completion. With remote and onsite options available, Prevalent delivers the expertise to help you reduce risk with your existing resources.
8.9 "Certificates and reports supplied by service providers may help firms obtain assurance on the effectiveness of the service provider's controls. However, in material outsourcing arrangements, the PRA expects firms to: • assess the adequacy of the information in these certificates and reports, and not assume that their mere existence or provision is sufficient evidence that the service is being provided in accordance with their legal, regulatory, and risk management obligations; and • ensure that certificates and audit reports meet the expectations in Table 8."	Prevalent centralizes certifications, agreements, contracts and supporting evidence with built-in task and acceptance management, plus mandatory upload features.
9 Sub-outsourcing	
Prevalent identifies fourth-party and Nth-party relationships through a native identification assessment or by passively scanning the third party's public infrastructure. The resulting relationship map depicts information paths and dependencies that could open pathways into an environment. Suppliers discovered through this process are monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening.	
10 Business continuity and exit plans	

PRA SS2/21 Requirement	How Prevalent Helps

10.1 "For each material outsourcing arrangement, the PRA expects firms to develop, maintain, and test a:
• business continuity plan; and
• documented exit strategy, which should cover and differentiate between situations where a firm exits an outsourcing agreement:
  ○ in stressed circumstances, (eg following the failure or insolvency of the service provider (stressed exit)); and
  ○ through a planned and managed exit due to commercial, performance, or strategic reasons (non-stressed exit)."
	The Prevalent Third-Party Risk Management Platform automates the assessment, continuous monitoring, analysis, and remediation of third-party business resilience and continuity – while automatically mapping results to NIST, ISO, and other control frameworks.
	
	To complement business resilience assessments and validate results, Prevalent:
	• Automates continuous cyber monitoring to predict possible third-party business impacts
	• Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability
	• Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns.
	
	This proactive approach enables organizations to minimize the impact of third-party disruptions and stay on top of compliance requirements.

10.3 "Firms should implement and require service providers in material outsourcing arrangements to implement appropriate business continuity plans to anticipate, withstand, respond to, and recover from severe but plausible operational disruption." **10.9** "In line with Fundamental Rule 7, in the event of a disruption or emergency (including at an outsourced or third party service provider), firms should ensure that they have effective crisis communication measures in place. This is so all relevant internal and external stakeholders, including the Bank, PRA, FCA, other international regulators, and, if relevant, the service providers themselves, are informed in a timely and appropriate manner."	The Prevalent Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: • Categorize suppliers according to their risk profile and criticality to the business • Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) • Centralize system inventory, risk assessments, RACI charts, and third parties • Ensure consistent communications with suppliers during business disruptions Prevalent delivers free resources for organizations to use as they build or mature their third-party business continuity programs.

The Prevalent Difference

Prevalent can help organizations automate Materiality Assessments and continuously monitor their outsourcing and non-outsourcing third parties for business resilience risks. Prevalent assessment and monitoring capabilities enable organizations to determine and validate whether a defect or failure in the performance of a vendor materially impairs:

- The organization's ability to meet *Threshold Conditions*
- Compliance with the Fundamental Rules or the Financial Conduct Authority's (FCA's) Principles of Business
- The financial stability of the UK
- The organization's requirements under the *Information Gathering* section of the PRA Rulebook
- The organization's financial or operational resilience

For organizations that have outsourced an internal control or key function, Prevalent can help determine whether a defect or failure in performance would adversely affect the relevant function. It can also help determine the potential impact of a disruption, failure or inadequate performance on:

- operational risk, conduct risk, information and communication technology (ICT) risk, legal risk and reputational risk
- the organization's ability to comply with and report against legal and regulatory requirements
- the organization's access to essential data or risk of breach to Confidential or Highly Confidential Data

California Consumer Privacy Act (CCPA)

This chapter of the white paper addresses how the California Consumer Privacy Act defines third-party vendors.

CCPA Summary

The California Consumer Privacy Act of 2018 (CCPA) was designed to regulate business' collection and sale of consumer data, thereby protecting California residents' sensitive personal information and providing consumers with control over how that information is used. Under the CCPA, sensitive personal information is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." In January 2023, the CCPA will be updated through the California Privacy Rights Act (CPRA) and apply to personal information collected by a covered business on or after January 1, 2022.

The CCPA requires companies to inform California residents about data being collected prior to collecting the data. It allows consumers to access all personal data held by a company and receive information about individuals or organizations with whom that data has been shared. It also allows consumers to opt out and prevent their personal data from being sold or shared with a third party.

Since California represents an enormous market – the 5th largest economy in the world if it were a country – companies must assume that California consumers are among their customers and should be prepared to comply with the CCPA. In fact, many businesses opt to treat every consumer as if they were a California resident, and therefore prepare for CCPA compliance across their businesses.

Meeting CCPA Requirements

Section 1798.100 of the CCPA states that a business that collects a consumer's personal information and sells or shares it with a third party must enter into an agreement with that third party that "obligates the third party, service provider, or contractor to comply" with the CCPA's privacy regulations. While the regulation is not prescriptive in the steps organizations should take, section 1798.81.5 requires organizations to, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

Organizations should ensure that their third-party partners and service providers are well prepared to protect consumer information. The first step in any security program is to identify and prioritize existing risks via a thorough security assessment. CCPA Section 1798.185 (15) speaks to, "requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to conduct annual cybersecurity audits and submit to the California Privacy Protection Agency a risk assessment.

Although limited guidance on achieving compliance with CCPA requirements is available, standard best practices, similar to those employed in addressing GDPR, can be applied here as well.

California Consumer Privacy Act (CCPA)	
Regulates business' collection and sale of consumer data, thereby protecting California residents' sensitive personal information and providing consumers with control over how that information is used.	
CCPA Standards	How Prevalent Helps
1798.100 General Duties of Businesses that Collect Personal Information (e) **A business that collects a consumer's personal information shall implement reasonable security procedures and practices…**in accordance with Section 1798.81.5. 1798.81.5 (b) A business that owns, licenses, or maintains personal information about a California resident **shall implement and maintain reasonable security procedures and practices** appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.	For any regulatory standard, organizations must ensure that they measure the correct risks and apply the correct controls. In the case of CCPA, that could mean leveraging the Center for Internet Security (CIS) Critical Security Controls as a framework. The Prevalent Third-Party Risk Management Platform includes questionnaires that map to dozens of standards, including the CIS Critical Security Controls. This helps organizations align with California's standard for "reasonable security." The Prevalent Platform enables organizations to assess not only their third parties' data privacy controls, but also their own through internal data privacy impact assessments. The results of this comprehensive assessment approach ensures that organizations have a holistic internal and external picture of risks to data.
1798.140 Definitions (C) Permits, subject to agreement with the contractor [or service provider], the business to monitor the contractor's [or service provider's] compliance with the contract through measures, including, but not limited to, **ongoing manual reviews and automated scans and regular assessments, audits**, or other technical and operational testing at least once every 12 months.	To avoid reputational and operational risk and business disruptions, organizations should ensure that their partners and third parties adhere to reasonable security measures. However, attempting to conduct third-party assessments using manual questionnaires and spreadsheets is inconsistent and unscalable. The Prevalent Third-Party Risk Management Platform automates third-party risk assessments. It provides questionnaires designed specifically for the CCPA and other privacy and security standards, scores risks automatically based on third-party responses, and provides remediation guidance to reduce risk and reporting to satisfy auditor needs. Prevalent Vendor Threat Monitor (VTM) complements the Platform with continuous scanning of third-party cyber, business, reputational and financial risks, including providing access to a database of data breach history. These insights provide a real-time view of potential risks to your consumers' data.

CCPA Standards	How Prevalent Helps
1798.185 Regulations (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: (15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (C) **Perform a cybersecurity audit on an annual basis**, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities. **Submit to the California Privacy Protection Agency on a regular basis a risk assessment** with respect to their processing of personal information…	Most risk assessment surveys focus on general controls and policies. Complying with the CCPA requires a technical understanding of data processing – specifically with the CIS Critical Security Controls, which are suggested as a framework to ensure proper security over data. Prevalent provides technical expertise in the design of its surveys and controls, ensuring that required implementation details are not missed. The Platform can map to the CIS Critical Security Controls to ensure complete coverage for the CCPA and help distinguish properly designed systems from "bolt-on" security and privacy features to ensure full compliance. When third parties use 4th or Nth parties to help process data, Prevalent provides visibility with detailed relationship mapping and audit trails of flows of information throughout a supplier ecosystem. The Prevalent Platform includes effective reporting to satisfy CCPA audit and compliance requirements, as well as to present findings to the board and senior management. The entire risk profile can be viewed in a centralized 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.

The Prevalent Difference

Organizations that must comply with CCPA and other state-level privacy regulations should ensure that third parties with whom they share personal information have controls in place to protect that information. As new state-level legislation is passed, organizations must also prepare for the possibility of data controller liability when data processors and third parties do not provide reasonable security controls.

Prevalent offers organizations with a scalable third-party risk management platform that addresses data protection risks. The Prevalent solution:

- Discovers and maps data between third, 4th and Nth party relationships
- Enables self-assessments to understand the maturity of internal processes, as well as data owners
- Assesses third parties for data privacy controls
- Automates risk response when third-party answers don't line up with expectations
- Reports on CCPA compliance with built-in reporting
- Delivers automated data breach notifications to understand possible risks to your customers' data

The outcomes include greater visibility into where data is, accelerated identification and remediation of potential risks, and reduced reporting complexity.

California Transparency in Supply Chains Act

This chapter of the white paper addresses how the California Transparency in Supply Chains Act impacts how organizations assess their third party vendor and suppliers.

California Transparency in Supply Chains Act Summary

The California Transparency in Supply Chains Act is a law enacted in 2012 that requires companies to disclose their efforts, if any, to ensure that the goods they sell are not produced by workers who are forced into servitude or labor. The law applies to any company that does business in the U.S. state of California, with at least $100 million in global revenue, and that makes or sells goods in California.

A company's public disclosure must be conspicuous and include information on how it:

- Verifies labor practices in their supply chains
- Audits suppliers
- Certifies that materials are not produced by forced labor
- Maintains internal accountability
- Trains employees and management

Meeting California Transparenc in Supply Chains Act Requirements

As part of the law, compares are required to:

- Publish an annual statement detailing the steps taken (or not) to ensure that human trafficking and slavery is not taking place in their business or supply chain
- Improve due diligence on suppliers to ensure they are adhering to the law

Although limited guidance on achieving compliance is available, standard best practices, similar to those employed in addressing other labor standards, can be applied here as well.

The below table summarizes how Prevalent can simplify this process.

California Transparency in Supply Chains Act	
Ensuring companies producing good are not using slavery or other forms of servitude to produce them.	
CTSCA Best Practices	How Prevalent Helps
Pre-Screen Suppliers	Rapidly pre-screen vendors using a library of continuously updated risk scores based on inherent/residual risk, assessment results and real-time reputational monitoring.
Build a Comprehensive Supplier Profile	Tap into 550,000+ sources of vendor intelligence to build a comprehensive supplier profile that includes industry and business insights, including potentially risky 4th-party relationships.
Score Inherent Risks	Use a simple assessment with clear scoring to track and quantify inherent risks for all onboarded suppliers

CTSCA Best Practices	How Prevalent Helps
Perform Detailed Assessments	Leverage Prevalent's built-in Modern Slavery assessment to determine adherence to policies. Review and approve assessment responses to automatically register risks or reject responses and request additional input.
Monitor Supplier Reputation	Validate assessment results and gain continuous supplier insights from over 550,000 public and private sources of reputational information, including negative news, regulatory and legal actions, sanctions, adverse media, OFAC violations, and more.
Centrally Manage Risks	Normalize, correlate and analyze assessment results and continuous monitoring intelligence for unified risk reporting and remediation.
Remediate	Take actionable steps to reduce modern slavery exposure with built-in remediation recommendations and guidance.
Store Documents and Evidence	Store and distribute Modern Slavery policy documents for dialog and attestation.
Map Relationships	Identify relationships between your organization and third, fourth and Nth parties to discover dependencies and assess your exposure.
Report on Compliance	Visualize and address compliance requirements by automatically mapping assessment results to Modern Slavery requirements.

The Prevalent Difference

Prevalent helps organizations apply a rigorous level of due diligence to their suppliers by determining if a public statement exists, and validating policies and processes through modern slavery risk assessments and continuous external monitoring of their real-world practices. Armed with these insights, organizations improve their visibility into their supply chain partners' labor practices, reducing the risk of reputational damage.

European Banking Authority (EBA) Guidelines on Outsourcing Arrangements

This chapter of the white paper addresses the EBA's framework for financial institutions that are subject to the Capital Requirements Directive (CRD).

These guidelines are consistent with the requirements on outsourcing under the Payments Services Directive (PSD2), the Markets in Financial Instruments Directive (MiFID II) and the Commission's Delegated Regulation (EU) 2017/565.

EBA Guidelines on Outsourcing Arrangement Summary

The European Banking Authority (EBA) is an independent EU Authority that works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.

In early 2019, the EBA published revised Guidelines on Outsourcing Arrangements, including specific provisions for financial institutions' governance frameworks within the scope of the EBA's mandate with regard to their outsourcing arrangements and related supervisory expectations and processes. The recommendation on outsourcing to cloud service providers, published in December 2017, is integrated into the guidelines.

The EBA, recognizing the vast ecosystem in financial services and the various types of integrated services used, dedicated 70 pages to the management of outsourcing in the financial services industry, plus another 55 pages for responses to comments on these guidelines.

Highlights from these requirements include:

- A member of a financial institution's senior management team is responsible for all activities, including setting the overall business strategy and the establishment of an effective risk management program to oversee all risks and manage all outsourcing arrangements
- A sound outsourcing framework that:
    - **Distinguishes outsourcings that are "critical or important"** from those that are not
    - **Performs due diligence** in the outsourcing selection process
    - **Enables proper risk assessment, whereby all potential operational risks are identified, managed, monitored and reported**
    - Requires contracts that set out **rights of access and audit** for the banks and their regulators to ensure effective oversight
    - **Performs ongoing assessment and continuous monitoring, with clear reporting to senior management**
    - **Makes available to authorities all documentation for transparency**
    - Defines a clear exit strategy in the event of a failure by the service provider

The guidelines became effective on September 30, 2019.

Meeting EBA Outsourcing Guidelines

Please see the table below for a summary of EBA supplier risk management guidelines, and how Prevalent can help your organization address these requirements.

EBA Guidelines on Outsourcing Arrangements	
The EBA Guidelines set out the internal governance arrangements that credit institutions, payment institutions and electronic money institutions should implement when outsourcing internal services, activities or functions.	
EBA Guidelines	How Prevalent Helps
Title II – Assessment of Outsourcing Arrangements **4 – Critical or important functions** **Paragraph 30** "Particular attention should be given to the assessment of the criticality or importance of functions if the outsourcing concerns functions related to core business lines."	The Prevalent Assessment solution enables financial institutions to classify third parties based on their importance to the organization. A selection of customizable questionnaires enables you to match the assessment requirements to the level of risk presented by the relationship.
Title III - Governance Framework **5 - Sound governance arrangement and third-party risk** **Paragraph 32** "Institutions and payment institutions should have a holistic institution-wide risk management framework to identify and manage all their risks, including risks caused by arrangements with third parties."	Prevalent delivers the industry's only purpose-built, unified platform for third-party risk management. Our solution automates the inside-out process of vendor risk assessments while including proactive continuous monitoring using an outside-in approach to reduce risk and meet the demands of regulatory compliance.
Title III - Governance Framework **5 - Sound governance arrangement and third-party risk** **Paragraph 33** "Institutions and payment institutions should identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed."	The Prevalent Assessment service 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.

EBA Guidelines	How Prevalent Helps
Title III - Governance Framework **6 - Sound governance arrangements and outsourcing** **Paragraph 40(c)** "When outsourcing, institutions and payment institutions should at least ensure that: the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech)."	The Prevalent Third-Party Risk Management platform provides a complete solution to perform 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.
Title III - Governance Framework **10 - Internal audit function** **Paragraph 50** "The internal audit function's activities should cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and programme should include, in particular, the outsourcing arrangements of critical or important functions."	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.
Title III - Governance Framework **12.3 – Due Diligence** **Paragraphs 70 & 71** "With regard to critical and important functions, institutions and payment institutions should ensure that the service provider has the business reputation to meet its obligations. Additional factors to be considered include its business model, nature, scale, complexity, financial situation, ownership and group structure."	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 include: • Insider threats • Financial problems • M&A activity • Layoffs • Data breach cases • Reputational metrics

EBA Guidelines	How Prevalent Helps
Title III - Governance Framework **13.2 Security of data and systems** **Paragraph 82** "Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis."	The Prevalent Third-Party Risk Management platform provides a complete solution to perform 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.
Title III - Governance Framework **13.3 Access, information and audit rights** **Paragraph 87 (b)** “Institutions and payment institutions should ensure that the service provider grants them: • unrestricted rights of inspection and auditing related to the outsourcing arrangement (‘audit rights’), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements”	The Prevalent Assessment solution ensures service providers implement the exact, agreed upon requirements with regular tracking and verification. 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.
Title III - Governance Framework **13.3 Access, information and audit rights** **Paragraph 91** "Institutions and payment institutions may use: • pooled audits organized jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organizational burden on both the clients and the service provider"	Prevalent’s Vendor Evidence Sharing Networks are repositories of completed, validated vendor questionnaires and supporting evidence that eliminate the tedious time- and resource-consuming process of collecting data from scratch. Prevalent offers both horizontal and vertical networks to speed assessment and collaboration within the community.

EBA Guidelines	How Prevalent Helps
Title III - Governance Framework **14 Oversight of outsourced functions** **Paragraph 100** "Institutions and payment institutions should monitor, on an ongoing basis, the performance of the service providers. Where the risk, nature or scale of an outsourced function has materially changed, institutions and payment institutions should reassess the criticality or importance of that function."	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, covered entities gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.
Title III - Governance Framework **14 Oversight of outsourced functions** **Paragraph 104** "Institutions and payment institutions should ensure that outsourcing arrangements meet appropriate performance and quality standards in line with their policies by: a. ensuring that they receive appropriate reports from service providers; b. evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and c. reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing."	The Prevalent Assessment service captures and audits conversations and matches documentation or evidence against risks. Visually appealing and coherent dashboards provide a clear overview of tasks, schedules, risk activities, survey completion status, agreements, and associated documents.
Title III - Governance Framework **14 Oversight of outsourced functions** **Paragraph 105** "If shortcomings are identified, institutions and payment institutions should take appropriate corrective or remedial actions."	The Prevalent solution includes bi-directional workflow and shared communication mechanisms to track findings and remediate issues.

The Prevalent Difference

The EBA guidelines require robust management and tracking of service provider risks. They specify that a policy for managing risk should be in place, including internal controls-based assessments and continuous monitoring of third-party outsourcing arrangements. The policy should be codified in a contract between the financial institution and the outsourcing relationship, with proper documentation and reporting for both remediation efforts and audit capabilities.

Prevalent can help address EBA requirements by efficiently collecting, analyzing, and identifying risks in a third-party ecosystem. Specifically, Prevalent can help:

- Identify and tier third parties by criticality to the business
- Measure the internal controls of third parties against several different industry standard control frameworks through the automation of assessments
- Monitor the cyber and business health of third parties continuously to inform risk management professionals of immediate risks to the business
- Raise risks from the combination of third-party internal controls assessments and ongoing monitoring, aiding in prioritization of the most significant risks
- Provide remediation guidance to transform inherent risk into acceptable levels of residual risk tolerance
- Centralize all third-party risk management functions into a single platform with stakeholder-specific reporting and views

European Corporate Due Diligence Act

This chapter of the white paper addresses the European Corporate Due Diligence Act, which is set to become law in 2021.

European Corporate Due Diligence Act Summary

In March 2021, the European Parliament published a draft directive that introduced mandatory corporate due diligence requirements in areas such as human rights and environmental practices in an organization's supply chain.

As part of the directive, any organization in the European Union (EU) - whether private, state-owned or publicly-listed - would be required to, "identify and assess potential or actual impacts on human rights, the environment or good governance caused by, contributing to or linked to their operations or business relationships, using a risk-based monitoring methodology that takes into account the impact, nature and context of the undertaking's operations." and, "review business relationships for the same risks."

Organizations should perform due diligence initiatives on a regular basis to ensure their third parties are actively engaged in human rights and environmental practices and develop remediations to mitigate any potential financial, legal or reputational risks before they arise.

Meeting European Corporate Due Diligence Act Requirements

Although the directive is not yet law, it is important that any organization that does business in the EU:

- Conduct due diligence according to the likelihood and severity of adverse environmental or human rights impacts
- Publish a statement, including the risk assessment, data and methodology, concluding that the company does not cause, contribute to and is not directly linked to adverse human rights or environmental impacts
- Establish and implement a due diligence strategy, reviewed annually
- Verify that subcontractors and suppliers comply with obligations

The table on the following page summarizes how Prevalent can simplify this due diligence process.

European Corporate Due Diligence Act	
This draft directive introduces mandatory corporate due diligence requirements in areas such as human rights and environmental practices in an organization's supply chain.	
European Corporate Due Diligence Act Requirements	How Prevalent Helps
Conduct due diligence according to the likelihood and severity of adverse environmental or human rights impacts	Prevalent's built-in Modern Slavery and environmental assessments help to to determine adherence to policies. Review and approve assessment responses to automatically register risks or reject responses and request additional input or supporting documentation.
Publish a statement, including the risk assessment, data and methodology, concluding that the company does not cause, contribute to and is not directly linked to adverse human rights or environmental impacts	Store and manage policy documents, evidence and more for dialog and attestation.
Establish and implement a due diligence strategy, reviewed annually	Visualize and address compliance requirements by automatically mapping assessment results to any regulation or framework on an annual or periodic basis.
Verify that subcontractors and suppliers comply with obligations	Perform controls-based assessments against Modern Slavery and environmental requirements and validate the results against qualitative insights from over 550,000 public and private sources of reputational information, including negative news, regulatory and legal actions, adverse media, conflicts of interest and more.

The Prevalent Difference

The Prevalent Third-Party Risk Management Platform delivers a complete vendor due diligence solution that unifies assessment results with financial and reputational monitoring for a continuous, closed-loop view of vendor risks. With Prevalent, organizations can:

- Implement comprehensive supply chain partner pre-screening including centralizing previous assessment results, reputational information, legal actions and previous sanctions so sourcing and procurement teams can make informed supplier sourcing decisions.
- Assess supply chain partners regularly by leveraging an automated solution that hosts assessment questionnaires, raises risks based on variance to acceptable results, and offers specific remediation recommendations.
- Fill gaps between assessments with continuous reputational monitoring of supplier reputation, global sacntions, and adverse media.
- Know their Nth parties, or their extended partner ecosystems which can be a source of unseen risks.
- Simplify compliance reporting by automatically mapping assessment results to any regulation or framework.

General Data Protection Regulation (GDPR)

This chapter of the white paper addresses the General Data Protection Regulation (GDPR) set forth by the European Union (EU) in May 2018.

GDPR Summary

The General Data Protection Regulation (GDPR) is a privacy law that governs the use, movement, and protection of data collected on European Union (EU) citizens. The GDPR covers any organization that collects, stores, processes, or transfers personal data on individuals in Europe, regardless of the organization's location. This includes organizations offering goods and services and monitoring behavior – including those with websites that track cookies or IP addresses of people who visit their website from EU countries.

The regulation was put into effect on May 25, 2018, and imposes penalties of up to €20 million or 4% of global revenue (whichever is higher), plus compensatory damages to individuals.

Because third parties are often responsible for managing personal data on behalf of their customers, organizations must take special care in ensuring those vendors and partners have data protection controls and governance in place. This involves conducting data privacy controls assessments; analyzing the results for potential risks; and requiring third parties remediate those risks to avoid regulatory, financial, and reputational exposures.

Meeting GDPR Requirements

To protect themselves from risk, organizations are required by the GDPR to conduct risk assessments to identify risks both inside the organization and with any third party that will have access to personal data. Recital 76 – Risk Assessment – states that, "Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."

Organizations subject to GDPR regulations must ensure that they and their third parties protect the privacy of any personal information collected and/or processed. This means conducting a thorough evaluation of the risks present in each third party and ensuring that appropriate controls are in place to mitigate risk.

Please see the table below for a summary of GDPR as it relates to data processors, and how Prevalent can help your organization address these requirements.

General Data Protection Regulation (GDPR)	
GDPR is a set of laws designed to give EU citizen more control over their personal data and increase the obligations of organizations to deal with that data in transparent and secure ways.	
GDPR Requirements	How Prevalent Helps
Article 24: Responsibility of the controller 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons**, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.** Those measures shall be reviewed and updated where necessary. *Article 24 references two Recitals for guidance:* **Recital 76: Risk assessment** The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. **Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.** **Recital 77: Risk assessment guidelines** Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards **the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk.**	When using third parties as "processors," it is the information controller (owner) that is liable for ensuring each third party has appropriate controls in place to ensure the privacy and security of personal data. Attempting to conduct third-party assessments using manual questionnaires and spreadsheets is inconsistent and unscalable. In the event of an audit, the ability to "demonstrate that processing is performed in accordance" with the GDPR can be challenging. Manual assessments can result in missed requirements and responses that are poorly answered or incomplete. To satisfy the GDPR requirements, assessments must be objective and scoring consistent. Prevalent's Third-Party Risk Management Platform automates third-party risk assessments. It provides questionnaires designed specifically for the GDPR and scores risks according to "likelihood and severity," while facilitating remediation in alignment with GDPR guidelines. Prevalent provides a library of over 75 standardized assessment templates – including the GDPR and other privacy-related regulatory standards – along with customization capabilities and built-in workflows. In addition, Prevalent's Controls Validation Service reviews third-party assessment responses and documentation against established testing protocols to validate that indicated controls are in place. To accelerate assessments, Prevalent's Vendor Intelligence Networks provide access to thousands of completed and verified assessments, which are continuously updated and provide supporting evidence.

GDPR Requirements	How Prevalent Helps
Article 25: Data protection by design and by default 1. "… **the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement data-protection principles,** such as data minimisation, in an effective manner and to **integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation** and protect the rights of data subjects." **Recital 78: Appropriate technical and organisational measures** In order to be able to demonstrate compliance with this Regulation, **the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.**	Complying with the GDPR requires deep technical understanding of data processing, data governance, and controls. While most risk assessment surveys focus on general controls and policies, the GDPR requires special treatment of personal information, including pseudonymization, data minimization, and (per Recital 78) data protection "by design and by default." Prevalent provides technical expertise in the design of its GDPR surveys and controls, ensuring that required implementation details are not missed. It helps organizations distinguish properly designed systems from "bolt-on" security and privacy features to ensure full compliance. When third parties use 4th or Nth parties to help process data, Prevalent provides visibility with detailed relationship mapping and audit trails of flows of information throughout a supplier ecosystem.
Article 28: Processor Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation** and ensure the protection of the rights of the data subject.	Organizations often work with dozens of third parties with access to personal information covered by the GDPR. Examples include advertising partners, data processors (including cloud applications), and cloud hosting providers. Compliance with the GDPR requires more than simple vendor agreements. It requires understanding how data is used, how it moves, and evidence of specific controls to protect personal data. Prevalent offers security, privacy, and risk management professionals an automated platform to manage the third-party risk assessment process and determine compliance with IT security, regulatory, and data privacy requirements, including GDPR. It 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.

GDPR Requirements	How Prevalent Helps
Article 28: Processor Paragraph 3: "That contract or other legal act shall stipulate, in particular, that the processor: (f) **assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 considering the nature of processing and the information available to the processor**	Articles 32 to 36 provide the requirements for a data protection impact assessment along with continuous monitoring of critical data processors (third parties). Each processor relationship "shall be governed by a contract or other legal act" that obligates the processor to protect personal information. The required risk assessment is to identify risks to personal information and ensure the processor has adequate controls in place. Prevalent delivers the industry's only purpose-built, unified platform for third-party risk management. The platform combines automated third-party assessments and continuous threat monitoring to simplify compliance, reduce security risks, and improve efficiency. The platform provides security and compliance professionals with a 360-degree view of data processor risks, via clear and concise reporting tied to specific regulations and control frameworks, including GDPR, for improved visibility and decision making. The Prevalent Platform enables contract reviews, helping to reveal potential contract violations and inform renewal negotiations via dedicated contract assessments.
Article 28: Processor Paragraph 3: "That contract or other legal act shall stipulate, in particular, that the processor: (h) **makes available to the controller all information necessary to demonstrate compliance** with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."	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 a centralized live reporting console, and reports can be downloaded and exported to determine compliance status with GDPR provisions. 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. Prevalent Vendor Threat Monitor (VTM) alerts organizations to adverse changes in third parties' businesses and triggers targeted assessments to address interim immediate risks. Early alerts enable more time to respond to incidents, and built-in remediation guidance helps organizations protect personal data and avoid regulatory actions and reputational damage.

GDPR Requirements	How Prevalent Helps
Article 32: Security of Processing Paragraph 1: "The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including: (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures** for ensuring the security of the processing. **Recital 76: Risk Assessment** The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. **Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.**	While assessments are often viewed as an onboarding exercise, GDPR and other regulatory standards require continuous compliance. Managing a single compliance review can be challenging using manual processes. Knowing when circumstances would warrant a periodic update across dozens or hundreds of third parties across the globe is even harder. Prevalent offers security, privacy, and risk management professionals an automated platform to manage the third-party risk assessment process and determine ongoing compliance with IT security, regulatory, and data privacy requirements, including the GDPR. 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.
Article 35: Data protection impact assessment 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. 7. The assessment shall contain at least: 1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; 2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	Technology evolves daily and new service offerings can provide enhanced business value. The GDPR makes clear that *prior to adopting new ways of processing personal data,* organizations must assess the impact of those operations on the data. With Prevalent, you can conduct Privacy Impact Assessments to uncover at-risk business data and personally identifiable information (PII). Analyze the origin, nature and severity of risk and get remediation guidance. For organizations needing more resources, Prevalent's Vendor Risk Assessment Services experts can handle everything from risk collection and analysis, to reporting and remediation management.

GDPR Requirements	How Prevalent Helps
Article 35: Data protection impact assessment (continued) 3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and 4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	
Article 45: Transfers On The Basis Of An Adequacy Decision 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. 2. Such a transfer shall not require any specific authorisation. **When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements**: **the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data.**	Increasingly, boards of directors, investors, and customers want to ensure organizations and their partners and suppliers share common values and commitments. The GDPR captures this in Article 45, requiring that human rights and rule of law be considered when transferring personal information. Prevalent supports Environment, Social, and Governance (ESG) compliance with capabilities to assess third parties against a number of ESG topics and correlate the findings with continuous external monitoring into vendor practices. This includes stewardship of the environment, diversity and inclusion, human rights (e.g., anti-slavery), labor standards, finance and tax strategies, and overall operational transparency. In addition, Prevalent includes Breach Event Notification Monitoring, providing access to a database containing 10+ years of data breach history for thousands of companies around the world. This Includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications to help determine the posture of companies you are considering transferring data to.

The Prevalent Difference

The Prevalent Third-Party Risk Management Platform includes built-in capabilities to assess internal and external risks to consumer data, automate the remediation of findings, and report to regulators on progress. To address GDPR requirements, Prevalent:

- Offers a specific GDPR questionnaire in the Prevalent Platform, querying the vendor on their technical and organizational measures to protect of the rights of the data subject per Article 28, paragraph 1.
- Provides data controllers with a 360-degree view of data processor risks via clear and concise reporting on control failures along with recommended remediations per Article 28, paragraph 3.
- Centralizes a data processor's risk profile, enabling a thorough audit of processes mandated by the data controller per Article 28, paragraph 3.
- Provides ongoing periodic or secondary assessments to continually monitor the technical and organizational measures in place by the data processor to ensure a level of security appropriate to the risk, e.g. regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing per Article 32, paragraph 1.

Financial Conduct Authority (FCA) FG 16/5 Guidance

This chapter addresses the Financial Conduct Authority's FG 16/5 Guidance for firms outsourcing to the cloud and other third-party IT services.

FCA FG 16/5 Summary

The Financial Conduct Authority (FCA) is a financial regulatory body in the United Kingdom but operates independently from the UK Government. The FCA regulates financial firms providing services to consumers and maintains the integrity of the financial markets in the United Kingdom. Their work includes implementing, supervising, and enforcing EU and international standards and regulations in the UK.

In July 2018, the FCA released its finalized guidance, FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services, to help financial firms effectively oversee all aspects of the lifecycle of outsourcing arrangements. This includes:

- Making decisions to outsource and selecting a service provider
- Performing proper risk assessments for all outsourcing arrangements
- Monitoring outsourced activities on an ongoing basis, and identifying and managing risks

The FCA Guidance 16/5 adds cloud-specific controls in alignment with the general FCA outsourcing requirements found in the systems and controls (SYSC) sections of the FCA handbook for appropriately regulated firms, and also requires consistency with GDPR. This guidance is not binding and is intended to illustrate ways in which firms can comply with the relevant rules. Firms should consider this guidance in the context of their overarching obligations under the regulatory system. Complying with this guidance will generally indicate compliance with the FCA outsourcing regulatory requirements.

Meeting FCA FG 16/5 Guidance

Please see the table below for a summary of the FG 16/5 Guidance, and how Prevalent can help your organization address these requirements.

FCA FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services

The FCA FG 16/5 Guidance helps firms effectively oversee all aspects of the lifecycle of outsourcing arrangements.

FCA FG 16/5 Guidelines	How Prevalent Helps
Section 3.4 "A firm appropriately identifies and manages the operational risks associated with its use of third parties, including undertaking due diligence before deciding on outsourcing. Our approach is risk-based and proportionate, considering the nature, scale and complexity of a firm's operations."	Prevalent's Cyber & Business Monitoring solution offers firms the ability to gain insight into a service provider's potential cyber vulnerabilities or relevant business risks prior to entering into a contract or during a defined business arrangement. Prevalent combines native vulnerability scanning with multiple external sources for cyber threat intelligence to deliver deep insights into the cyber risks of service providers. 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 include: • Insider threats • Financial problems • M&A activity • Layoffs • Data breach cases • Reputational metrics
Risk Management "Accordingly, firms should: • carry out a risk assessment to identify relevant risks and identify steps to mitigate them • document this assessment	The Prevalent Assessment service offers security, privacy, and risk management professionals an automated platform to manage the service provider risk assessment process and determine 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.
Oversight of Service Provider "Ensure staff have sufficient skills and resources to oversee and test the outsourced activities; identify, monitor and itigate against the risks arising."	Third-party risk management is costly and time-consuming when using inefficient and error-prone manual data-gathering and sharing processes. Prevalent's Assessment solution automates this by collecting, organizing, and presenting service provider data to immediately facilitate decision making and manage vendor risk.

FCA FG 16/5 Guidelines	How Prevalent Helps
Data Security "Firms should carry out a security risk assessment that includes the service provider and the technology assets administered by the firm."	The Prevalent solution enables automated, standards-based or custom questionnaires to identify and manage third-party risk. Standards-based questionnaires evaluate third parties on various controls, including cybersecurity, IT, privacy, data security, cloud hosting, and business resiliency. The platform also includes bi-directional remediation workflows, live reporting, and an easy-to-use dashboard for efficiency.
Effective Access to Data **"**A firm should: • ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive • ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data"	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.

The Prevalent Difference

The FCA views the proper use of outsourcing to the cloud and other third-party IT services as a way for firms to increase flexibility and enable innovation. On the other hand, the FCA acknowledges that cloud outsourcing can also introduce risks that need to be properly identified, monitored and mitigated. This is accomplished through a proper risk assessment.

The cloud-based Prevalent Assessment Service helps risk management and information security professionals determine vendor compliance with IT security, regulatory, and data privacy requirements. Utilizing a library of over 50 pre-defined assessments, standardized content, or leveraging the flexibility of the platform to build custom surveys, the Prevalent Assessment Service automates the vendor risk management lifecycle, including the collection, analysis, and remediation of third-party data.

Key benefits include:

- Automates the manual work of vendor survey management
- Zeroes-in on risks and control failures, providing actionable guidance for remediation
- Clearly communicates actual business risk to multiple stakeholders
- Simplifies communications and status reporting with vendors
- Provides visibility and trending to measure the effectiveness of the program

Prevalent's Third-Party Risk Management platform provides a complete framework for implementing policy management, auditing and reporting related to the FCA's FG 16/5 Guidance.

Health Insurance Portability and Accountability Act (HIPAA)

This chapter provides an overview of HIPAA legislation, and focuses on the requirements of the HIPAA Security Rule.

HIPAA Summary

The US Health Insurance Portability and Accountability Act (HIPAA) was established to ensure that sensitive protected health information (PHI) would not be disclosed without the patient's consent. HIPAA includes a Security Rule that establishes safeguards for organizations holding electronically stored protected health information PHI (ePHI), as well as a Privacy Rule that sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

The HIPAA Privacy Rule defines Protected Health Information (PHI) as "any information held by a covered entity which concerns health status, the provision of healthcare, or payment for healthcare that can be linked to an individual."

The HIPAA Security Rule deals specifically with safeguarding electronically stored PHI (ePHI).

Although HIPAA regulations are most closely aligned with "covered entities" such as health plans, health care clearinghouses, and some health care providers, it also applies to "business associates" — third-party vendors that have access to PHI. This dramatically expands the number of organizations that must comply with HIPAA requirements – and the number of third parties that providers must assess.

Meeting HIPAA Security Rule Requirements

Organizations must be aware of risks to critical information both within their own entity and with third parties that have access to ePHI. HIPAA makes this a requirement, and extends the term "organization" to covered entities and business associates. Section 164.308(a)(1)(ii)(A) states:

> RISK ANALYSIS (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

Healthcare and related organizations must ensure that business associates and other third parties have the security and privacy controls in place to prevent unwanted access that impacts the confidentiality, integrity or available of ePHI. To achieve this, companies should conduct thorough vendor risks assessments.

Please see the table below for a summary of the HIPAA Security Rule requirements as it relates to managing vendor risk, and how Prevalent can help your organization address these requirements.

Health Insurance Portability and Accountability Act (HIPAA) Security Rule	
The HIPAA Security Rule is a set of laws designed to safeguard electronically stored PHI (ePHI).	
HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	How Prevalent Helps
Security Management Process Administrative Safeguards (§ 164.308(a)(1)) (A) Risk analysis (REQUIRED) "A covered entity or business associate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."	The first step in complying with HIPAA regulations is a comprehensive risk assessment – both internally and of third parties that may have access to PHI. While some organizations attempt this with spreadsheet-based questionnaires, that approach does not scale. Prevalent offers security, privacy, and risk management professionals a platform to automate the third-party risk assessment, scoring, and remediation process and determine compliance with IT security, regulatory, and data privacy requirements. Prevalent provides a library of over 75 standardized assessment templates – including for HIPAA and the Health Information Sharing and Analysis Center (H-ISAC) – customization capabilities, and built-in workflow and remediation guidance. In addition, the Prevalent Healthcare Vendor Network simplifies and accelerates the due diligence process, providing an on-demand library of thousands of completed healthcare vendor risk reports based on the H-ISAC questionnaire, which are continuously updated and backed by supporting evidence.
Security Management Process Administrative Safeguards (§ 164.308(a)(1)) (B) Risk management (REQUIRED) "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [HIPAA Security Standards]."	Once risks are identified, organizations must implement controls to minimize risk. Once assessments are collected and analyzed, the Prevalent TPRM Platform offers built-in remediation recommendations and guidance. With clear reporting and remediation guidance, the platform ensures that risks are identified, analyzed, and escalated to the proper channels so that your organization achieves a risk level appropriate to its risk appetite.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	How Prevalent Helps
Security Management Process Administrative Safeguards 164.308(a)(1)) (D) Information system activity review (REQUIRED) "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."	Since a lot can change between annual assessments, organizations should perform continuous monitoring of risks, contract performance and service level agreements (SLAs). Prevalent delivers a continuous view of risks through Internet and Dark Web threat monitoring feeds, as well as business and financial risk analysis, to reveal developments that could impact risks. The Prevalent Platform also enables comprehensive reviews with a dedicated and custom contract assessment questionnaire, plus continuously tracked performance metrics via centralized vendor dashboards. Prevalent maintains a complete repository of all documentation collected and reviewed during the diligence process, with specific regulatory compliance and security framework reporting.
Business associate contracts and other arrangements. **§ 164.308(b)(1)** "A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor."	Business associate contracts are required, but smart compliance and security teams will require evidence of compliance and controls. Prevalent's assessment capabilities simplify compliance and reduce risk with automated collection, analysis, and remediation of vendor responses using industry-standard or custom surveys – including those measuring information safeguards. Although not required, Prevalent provides visibility into 4th and Nth parties (e.g., subcontractors) with detailed relationship mapping, providing audit trails of flows of information throughout a supplier ecosystem.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	How Prevalent Helps
Security Management Process, Administrative Safeguards **§ 164.308(a)(6)** Implementation specification: Response and reporting (REQUIRED) "Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes."	Some vendors may not know when they have been breached, or may not promptly report incidents which can delay Mean Time to Discovery (MTTD) and Mean Time to Resolution (MTTR), opening an organization up to potential exploits. Prevalent Vendor Threat Monitor (VTM) monitors the Internet and Dark Web for cyber threats and vulnerabilities – as well as public and private sources of reputational, sanctions, and financial information – providing real-time visibility into risks and enabling risk management and security teams to act immediately. The Prevalent Third-Party Incident Response Service enables organizations to rapidly identify and mitigate the impact of third-party breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
Security Management Process, Administrative Safeguards **§ 164.308(a)(8)** "Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart."	All organizations experience personnel changes and periodically implement new policies and procedures. Covered entities must continuously monitor cyber, business, and financial intelligence for visibility into material changes to a vendor's risk profile between annual internal control assessments. Prevalent Vendor Threat Monitor alerts organizations to adverse changes in third parties' businesses and triggers targeted assessments to address interim immediate risks. Early alerts enable more time to respond to incidents and built-in remediation guidance helps organizations protect PHI and avoid OCR actions and reputational damage. Some changes, like the COVID-19 pandemic, forced fundamental changes in how businesses operate. Prevalent's assessment questionnaires include questions designed to reveal internal business continuity gaps and external supply chain weaknesses that could negatively impact an organization's ability to maintain control over sensitive PHI or prompt one to consider alternate vendors.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	How Prevalent Helps
Policies and procedures and documentation requirements **§ 164.316(b)(1)** "Standard: Documentation • (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and • (ii) If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."	In the event of an incident or audit, or in the course of a business relationship, organizations are required to produce evidence supporting policies, identified risks, and controls. The Prevalent TPRM Platform includes contract, document, evidence and certifications management with built-in version controls, task assignment, and auto-review cadences in centralized vendor profiles. In addition, Prevalent captures and audits conversations and matches documentation or evidence against risks. Intuitive and straightforward dashboards provide a clear overview of tasks, schedules, risk activities, survey completion status, agreements, and associated documents.

The Prevalent Difference

HIPAA requirements make it clear that risk assessments should be completed for covered entities and business associates to identify potential risks and vulnerabilities to the confidentiality, availability, and integrity of all PHI that an organization creates, receives, maintains or transmits.

Complying with HIPAA requires a complete internal and external view of the controls in place for all business associates. Managing this process efficiently across hundreds of third parties with manual spreadsheets is impossible. Prevalent can help:

- Automate business associate vendor onboarding and offboarding to ensure consistent processes
- Profile, tier and score inherent risk to guide full risk assessment decisions
- Assess business associates against standardized content that simplifies regulatory and standards mapping
- Centralize all business associate documentation, including contract, reporting and evidence
- Perform continuous monitoring of cybersecurity, business/reputational and financial information to correlate risks against assessment results
- Report regularly against SLAs, performance and compliance using standardized, pre-built templates
- Leverage best practices guidance to guide remediation decisions according to organizational risk appetite

Complying with HIPAA legislation requires a complete internal view of the controls in place of all business associates; something that cannot be addressed with a simple external automated scan.

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP-013-1) Supply Chain Risk Management

This chapter provides an overview of NERC CIP-013-1 for Supply Chain Risk Management and focuses on how organizations can implement security controls for supply chain risk management of bulk electronic systems (BES).

NERC CIP-013-1 Summary

The North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) standard establishes new cybersecurity requirements for electric power and utility companies to ensure, preserve, and prolong the reliability of the bulk electric system (BES). Enforceable starting on July 1, 2020, responsible entities have 18 months to comply in order to avoid penalties. NERC is authorized to penalize registered entities up to $1 million per day per outstanding violation.

Third-party risk management plays a pivotal role in ensuring supply chain security through the regular assessment of supply chain partners' internal security controls and the ongoing monitoring of vendor risks in real time. Taken together, this inside-out, outside-in view provides more complete visibility in supply chain risks.

Meeting NERC CIP-013-1 Requirements

Please see the table below for a summary of the NERC CIP-013-1 requirements as it relates to managing supply chain risk, and how Prevalent can help your organization address these requirements.

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP-013-1) Supply Chain Risk Management	
To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. .	
CIP-013 Cyber Security Criteria At a minimum, entities assess whether their vendor(s) can meet basic security criteria	How Prevalent Helps
1.2.1 Notification/Recognition of Cyber Security Incidents Vendors need to be able to identify when an incident occurred to ensure that the vendor can notify the entity in the case of such an incident.	Prevalent enables responsible entities to regularly assess their vendors' incident response plans, requiring upload of plans to the platform for validation. With this level of review, entities have visibility into how a supply chain partner would respond to a breach or cyber incident. Monitoring and scoring tools along cannot provide this level of internal controls or process visibility, however these tools can complement assessments to trigger on public disclosure of an incident.

CIP-013 Cyber Security Criteria At a minimum, entities assess whether their vendor(s) can meet basic security criteria	How Prevalent Helps
1.2.2 Coordination of Responses to Cyber Security Incidents Vendors should coordinate with the entity their responses to incidents related to the products or services provided to the entity that pose cyber security risk to the entity.	Prevalent provides a central platform for the review of evidence supporting incident response and communications plans, with the flexibility to built custom workflow, tasks and escalation paths to enable rapid response.
1.2.3 Notification when Remote or Onsite Access is No Longer Needed or Should No Longer be Available to Vendor Representatives Vendors should respond accordingly to personnel changes. A vendor should be able to tell the entity when a personnel change occurs that could impact whether or not remote access should still be available to vendor representatives.	The Prevalent platform includes a custom survey creation wizard that enables organizations to create and issue a customizable survey for offboarding asking specific questions of the vendor and internal team regarding system access, data destruction, and final payments, with built-in workflows to ensure that the separation process is seamless.
1.2.4 Vulnerability Identification Vendors are to notify an entity when a vulnerability related to a product or service is identified. In order to meet this obligation, a vendor needs to know when a vulnerability exists in their environment.	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. Built-in continuous monitoring capabilities complement assessments by performing external vulnerability scanning for web facing service interfaces, with results integrated into a single risk register.
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System	The Prevalent platform includes more than 50 built-in industry standard questionnaires (such as those for CIP, NIST, ISO and others), many of which ask specific questions around patching cadence and software integrity checks for internal systems. Answers to these questions are escalated into risks if proper patching thresholds are not met, informing responsible entities of potential risks.
1.2.6 Coordination of Controls for Vendor-Initiated Interactive Remote Access and System-to-System Remote Access with a Vendor Vendors must coordinate with entities to control vendor-initiated interactive remote access and ensure system-to-system remote access with a vendor is appropriately managed.	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.

Asset, Change, and Configuration Management As an entity performs a risk assessment and considers risk exposure of products or services to be procured in its environment, additional cyber security controls may be necessary to protect the entity's operating environment. An entity may consider obtaining and evaluating additional information regarding the vendor's capabilities with respect to the following security areas.	How Prevalent Helps
Asset, Change, & Configuration Management Inventory of Authorized & Unauthorized Devices • Physical devices and systems within the organization are inventoried • Software platforms and applications within the organization are inventoried • Organizational communication and data flows are mapped • External information systems are catalogued	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.
Change Control and Configuration Management Considerations • Uses a recognized framework for its information technology processes (e.g., ITIL) • Includes security in its system development life cycle • Has a mature change-control process • Maintains separate development and production environments • Maintains separate environments for different customers • Has mechanism for software integrity (e.g., PKI with encryption, digital signature) • Product allows for hardening to minimize attack surface • Processes to identify, discover, inventory, classify, and manage information assets (hardware and software • Processes to detect unauthorized changes to software and configuration parameters • Able to identify whether hardware, software, or components are U.S. and/or internationally sourced	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.

Governance As an entity performs a risk assessment and considers risk exposure of products or services to be procured in its environment, additional cyber security controls may be necessary to protect the entity's operating environment. An entity may consider obtaining and evaluating additional information regarding the vendor's capabilities with respect to the following security areas.	How Prevalent Helps
Establish and Implement Security Awareness Program • Documented and implemented security policy and procedures • All users are informed and trained on cybersecurity policies and procedures • Third-party stakeholders understand roles and responsibilities and are accountable to same requirements • Senior executives understand roles and responsibilities • Physical and information security personnel understand roles and responsibilities • Ability to provide ongoing support for software and hardware • Personnel background checks • Ability to retain data for events such as litigation holds, cyber security incidents • Presence of trained, knowledgeable, and sufficient cyber security resources • Supplier has certifications for manufacturing process (e.g., ISO)	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.
Logging and Monitoring Considerations • Maintains a program to perform continuous logging, monitoring, and analysis of its systems to identify events of significance • Has sufficient segregation of duties to ensure logging and monitoring are effective to detect anomalies	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.
Information Protection Considerations • Uses appropriate controls to manage data at rest (vendor or entity data) • Ability to provide additional hardware for failures • Encrypts credentials in transit, internal and externally • Encrypts credentials at rest • Uses strongest standard encryption algorithms (e.g., AES or SHA-2) • Supplier physical access controls to hardware, software, and manufacturing centers • Physical devices and systems within the organization are inventoried • Supplier location of data centers (U.S./Canada-based vs international)	The Prevalent platform offers evidence and process validation that such policies exist, requiring the supply chain partner to provide such evidence. The platform also quantifies vendor risks, offers prescriptive remediation guidance, tracks tasks and automates workflows to drive adherence to policy and best practices.

The Prevalent Difference

The Prevalent Third-Party Risk Management (TPRM) Platform enables electric utilities to centralize the assessment of their supply chain partners' internal controls, providing a repository of supporting evidence and documentation that can be used to audit and validate the presence of the proper supply chain security measure. With built-in continuous cyber security and business monitoring that can inform the issuing of secondary assessments based on triggered criteria, the Prevalent platform provides a more complete solution for supply chain risk management than what is offered by scoring-only tools.

As well, the Prevalent assessment platform supports questionnaires, risk registers and reporting against multiple industry standard frameworks, including the NIST CSF, PCI DSS 3.2, HIPAA, COBIT 5, and SOC 2, using the Prevalent Compliance Framework. Organizations need only ask a single set of questions and then map the results back to any number of these regulations, which simplifies and accelerates compliance reporting.

New York State Department of Financial Services (DFS) NY CRR 500

This chapter addresses the Cybersecurity Requirements Regulation for Financial Services Companies Part 500 (NY CRR 500) of Title 23.

23 NY CRR 500 Summary

In early 2017, the New York State Department of Financial Services (DFS) instituted this regulation to establish new cybersecurity requirements for financial services companies. Designed to protect the confidentiality, integrity, and availability of customer information as well as information technology systems, this regulation demands the following:

- A covered entity must establish risk controls against a baseline assessment
- A covered entity must create a cybersecurity program that addresses its risks in a robust fashion, including an audit trail
- A covered entity must appoint a CISO, and senior management must be responsible for and review the organization's cybersecurity program
- A covered entity must create a third-party risk management program
- A covered entity must file an annual certification confirming compliance with these regulations

According to the regulation, "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law" is considered a "covered entity" and must comply.

This legislation was enacted after the realization that data breaches and cyber threats were rising at an alarming rate, as cybercriminals develop sophisticated tools to gain access to exceptionally valuable data. The potential risk estimates to financial institutions remain staggering.

A key component of complying with 23 NY CRR 500 is managing your vendors' IT security controls and data privacy policies. As organizations look to focus on core competencies, reduce costs, and keep up with today's business pace, the proliferation of third-party vendors is at an all-time high. This extended enterprise enables businesses to thrive, but along with the benefits come added risks.

Two sections of the regulation specifically address third-party providers. Section 500.04 relates to the appointment of a CISO which can be employed by an affiliate or third-party. If not a direct employee, the Covered Entity must still retain responsibility for compliance, designate a senior person responsible for direction and oversight of the third-party service provider, and require the third-party to maintain a cybersecurity program that is compliant with the regulation. A report by the CISO must be provided annually regardless of whether they are a direct employee or a third party.

Section 500.11 directly addresses third-party service provider security policy. It requires covered entities to have a written policy that addresses third-party information systems security based on a risk assessment, and it requires the policy to cover:

- Identification and risk assessment of the third party
- Minimum cybersecurity practices
- Due diligence used to evaluate the adequacy of their cybersecurity practices, and
- Periodic assessment of the provider based on risk and continued adequacy of their cybersecurity practices.

It goes on to state that the policy includes specific requirements for access control and multi-factor authentication, encryption, notice of any cybersecurity event, and representations and warranties related to cybersecurity policies and procedures, but those requirements will not be discussed here.

Meeting 23 NY CRR 500 Third-Party Risk Management Compliance Requirements

Please see the table below for a summary of NY CRR 500 third-party risk management requirements, and how Prevalent can help your organization address these requirements.

New York State Department of Financial Services (DFS): Cybersecurity Requirements for Financial Services Companies Part 500 (NY CRR 500) of Title 23 (23 NY CRR 500)	
This bulletin requires NY insurance companies, banks, and other regulated financial services organizations to assess their cybersecurity profile.	
NY CRR 500 Requirements	How Prevalent Helps
23 NYCRR 500.04 - Chief Information Security Officer "(a) The CISO may be employed by the Covered Entity, one of its Affiliates or a Third-Party Service Provider. To the extent this requirement is met using a Third-Party Service Provider or an Affiliate, the Covered Entity shall: 1) **Retain responsibility for compliance** with this Part; 2) Designate a senior member of the Covered Entity's personnel **responsible for direction and oversight of the Third-Party Service Provider**; and 3) Require the **Third-Party Service Provider to maintain a cybersecurity program** that protects the Covered Entity in accordance with the requirements of this Part."	Prevalent delivers the industry's only purpose-built, unified platform for third-party risk management. The Prevalent Third-Party Risk Management platform combines automated vendor assessments and continuous threat monitoring to simplify compliance, reduce security risks, and improve efficiency. The platform provides CISOs with a 360-degree view of their vendor risks, via clear and concise reporting tied to specific regulations and control frameworks for improved visibility and decision making.
23 NYCRR 500.04 - Chief Information Security Officer "(b) The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable: 1) The confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems; 2) The Covered Entity's cybersecurity policies and procedures;	The Prevalent Third-Party Risk Management platform provides a complete solution to perform 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.

NY CRR 500 Requirements	How Prevalent Helps
3) Material cybersecurity risks to the Covered Entity; 4) Overall effectiveness of the Covered Entity's cybersecurity program; and 5) Material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.	
23 NYCRR 500.11 -Third Party Service Provider Security Policy "(a) Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable: **1) The identification and risk assessment of Third-Party Service Providers;** 2) Minimum cybersecurity practices required to be met by such Third-Party Service Providers in order for them to do business with the Covered Entity; 3) **Due diligence processes** used to evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers; and 4) **Periodic assessment of such Third-Party Service Providers** based on the risk they present and the continued adequacy of their cybersecurity practices." Details follow in this section including requirements for access controls with multi-factor authentication, encryption, **notice of cybersecurity events**, and representations and warrantees addressing cybersecurity policy.	The Prevalent TPRM Platform unifies internal control-based assessments (based on industry standard framework questionnaires or on 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. The platform includes continuous cyber and business risk review and analysis that can be performed at any time – during or between control-based assessments – providing an updated view of important cyber security risks and business developments that could impact risks.

The Prevalent Difference

23 NYCRR 500 specifically requires that covered entities develop written policies and procedures to ensure the security of information systems and the integrity of data accessed or held by third parties. Implementing a third-party service provider security policy should include the following elements:

- An accurate and comprehensive list of third-party service providers, including the identification of the specific services provided by each
- Cybersecurity practices to be followed by third parties, based on the policies and security controls of the covered entity's baseline risk assessment
    - Use of multi-factor authentication
    - Use of encryption
    - Notification of cybersecurity events
- Periodic assessment of vendors based on those requirements, including due diligence processes to be utilized
- Applicable contract requirements and guidelines

Prevalent's Third-Party Risk Management Platform enables financial institutions to fulfil these requirements across their entire vendor ecosystem. It 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 and risk. It also includes cyber and business intelligence monitoring to capture ongoing potential threats to a covered entity.

The responsibility for properly overseeing the IT security of outsourced relationships lies with the covered entity's CISO, who must present an annual report. With advanced reporting capabilities by compliance requirement and industry framework, the Prevalent TPRM platform can simplify compliance reporting and clarify risks.

Stop Hacks and Improve Electronic Data Security (SHIELD) Act

This chapter of the white paper addresses New York S.5575B/A.5635 – or SHIELD Act – which imposes stronger obligations on businesses handling private customer data to provide proper notification of security breaches.

SHIELD Act Summary

Signed into law by the Governor of the US State New York on July 25, 2019, the Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a data protection law that has broadened the definition of personal information to include username and password for an online account and biometrics; requires specific data security controls for organizations to protect the personal information of New York residents; and sets specific data breach notification requirements and penalties on organizations where the data of New York residents has been compromised.

Largely an update to previous New York state laws, the SHIELD Act will go into effect on March 21, 2020 and is meant to improve cybersecurity protections and data breach notification, with penalties ranging from $5,000 per violation to $20 per failed notification (capped at $250,000). Much like what the California Consumer Privacy Act (CCPA) does for that state, if your organization collects any kind of personal information from a resident of New York State – or you exchange information with a business partner that does – the law applies to you regardless of where your organization is located.

Meeting SHIELD Act Third-Party Risk Management Compliance Requirements

What's notably different about the SHIELD Act versus other related data protection laws is that it provides *some* criteria for compliance. The Act defines three (3) types of safeguards to measure compliance against – Administrative, Physical, and Technical – with requirements including:

- Designating and training employees to coordinate cybersecurity compliance
- Using third-party service providers capable of maintaining appropriate cybersecurity practices, with safeguards required by contract
- Assessing the risk of the company's cybersecurity program, including both the network and software design and the information processing, transmission and storage
- Applying processes and physical safeguards to detect, prevent and respond to attacks or system failures
- Monitoring and testing of the effectiveness of the cybersecurity program
- Applying processes to safely, securely and permanently dispose of data within a reasonable amount of time after it is no longer needed for business purposes
- Updating the program periodically to address changes in the business or circumstances that would require the program to be changed

According to definitions in the Act, compliance can be achieved (called a "safe harbor") if an organization meets the requirements of the GLBA Safeguards Rule, HIPAA, or 23 NYCRR Part 500 – although the Act is not clear on how an organization can prove that it is compliant with any of these regulatory regimes.

In examining the SHIELD Act requirements, there are several areas where third-party business relationships will have to be considered in ensuring compliance. Please review the Act's text for a complete view of requirements. The table below should not be construed as compliance recommendations – merely questions to assess what your organization might need to address.

New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act	
This imposes stronger obligations on businesses handling private customer data to provide proper notification of security breaches.	
SHIELD Act Requirements	How Prevalent Helps
Using third-party service providers capable of maintaining appropriate cybersecurity practices, with safeguards required by contract	• Is the organization conducting internal controls-based assessments of third-parties based on the requirements in applicable laws such as GLBA, HIPAA, or NYCRR Part 500? • Is the organization monitoring external third-party networks and utilizing business risk intelligence such as news events, financials, layoffs, leadership changes, lawsuits, etc. that can serve as predictors of future vulnerabilities? • Is there a defined process in place to identify, categorize, prioritize, and manage risks to an acceptable level? • Does the organization have a defined workflow process in place to escalate identified risks for remediation?
Assessing the risk of the company's cybersecurity program, including both the network and software design and the information processing, transmission and storage	• Is the organization utilizing external network vulnerability scanning along with multiple external sources for cyber threat intelligence? • Aside from external monitoring, is the organization conducting penetration testing to highlight vulnerabilities? • Is the organization monitoring relationships between different third-parties to gain visibility on how personal information could be shared?
Monitoring and testing of the effectiveness of the cybersecurity program	• Is there a central audit trail in place that keeps track of all interactions between suppliers and the organization? • Is there a central risk register in place to centralize all identified risks from internal control failures or external cyber scanning results so that a clear risk score is communicated? • Is there a live reporting capability to show existing risks and effects of planned remediations? • Is there compliance-specific reporting showing percent attainment or progress to compliance?

SHIELD Act Requirements	How Prevalent Helps
Updating the program periodically to address changes in the business or circumstances that would require the program to be changed	Does the organization have options to maintain program flexibility including: • Multiple industry standard questionnaire options with the ability to customize one appropriate to the business? • Defining assessment schedules to determine what third-parties to assess with automated chasing reminders? • The ability to outsource the collection and analysis of vendor surveys to focus internal risk management teams on risk management? • Leveraging pre-completed surveys and supporting vendor evidence to accelerate the risk management process?

The Prevalent Difference

NY SHIELD provides guidance to covered entities that they must assess the risk of the company's cybersecurity program, use third parties that maintain appropriate cybersecurity practices, and continually monitor and test the effectiveness of the cybersecurity program. Prevalent delivers the industry's only purpose-built, unified platform for third-party risk management. Delivered in the simplicity of the cloud, the Prevalent platform combines automated vendor assessments, continuous threat monitoring, assessment workflow, and remediation management across the entire vendor life cycle, with expert advisory and consulting services, network, and outsourced options to optimize your risk management program. With 50+ built-in questionnaire options – including for NYCRR 500 and other others helpful for the SHIELD Act – Prevalent can help organizations gain a 360-degree view of vendors to simplify compliance, reduce risks, and improve efficiency for a scalable third-party risk management program.

Office of the Comptroller of the Currency (OCC) Bulletins

This chapter of the white paper addresses the following OCC Bulletins:

- OCC Bulletin 2013-29: Third-Party Relationships: Risk Management Guidance
- OCC Bulletin 2017-07: Third-Party Relationships: Supplemental Examination Procedures
- OCC Bulletin 2017-21: Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

OCC 2013-29 / 2017-07 / 2017-21 Summary

The Office of the Comptroller of the Currency (OCC) is part of the US Department of the Treasury. The OCC charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks. Its mission is to ensure that national banks and federal savings associations operate in a safe and sound manner; provide fair access to financial services; treat customers fairly; and comply with applicable laws and regulations. The OCC has the power to enforce the regulations it issues with examinations – and it can deny applications for new charters or take other supervisory actions against banks and thrifts that do not comply with laws and regulations or otherwise engage in unsafe practices.[1]

OCC Bulletin 2013-29, clarified with a FAQ in OCC Bulletin 2017-21, provides risk management guidance for all national banks, federal savings associations and technology service providers for "**assessing and managing risk associated with third-party relationships**." OCC 2017-07 provides guidance to Examiners on what to look for when examining a bank's third-party risk management program. In so doing, it sets forth the practices that banks are expected to have in place.

These bulletins highlight the need for an effective risk management process throughout the lifecycle of the relationship, including **the need to assess, continuously monitor, and provide adequate documentation and reporting** to facilitate oversight and accountability.

Meeting OCC Third-Party Risk Management Compliance Requirements

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

[1] https://www.occ.treas.gov/about/what-we-do/mission/index-about.html

OCC Bulletin 2013-29
Third-Party Relationships: Risk Management Guidance

This bulletin provides guidance to national banks and federal savings associations for assessing and managing risks associated with third-party relationships.

Bulletin 2013-29 Requirements	How Prevalent Helps
Due Diligence and Third-Party Selection: "A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.	The Prevalent Assessment service 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.
Risk Management: "Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls."	The Prevalent Assessment service simplifies compliance and reduces risk with automated collection, analysis, and remediation of vendor surveys using industry standard and custom surveys.
Information Security: "Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests.	In addition to facilitating automated, periodic internal control-based assessments, the platform provides cyber security and business monitoring – continually assessing 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, covered entities gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.
Management of Information Systems: "Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining accurate inventories of its technology and its subcontractors. Assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place. Understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations"	

Bulletin 2013-29 Requirements	How Prevalent Helps
Ongoing Monitoring: "Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Some key areas of consideration for ongoing monitoring may include assessing changes to the third party's • business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) • compliance with legal and regulatory requirements • financial condition"	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 (e.g., debt, equity)
Documentation and Reporting: "A bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation typically includes: • A current inventory of all third-party relationships • Due diligence results, findings, and recommendations • Regular reports to the board and senior management"	The Prevalent Third-Party Risk Management platform includes 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.

OCC Bulletin 2017-21 – Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29	
Bulletin 2017-21 Questions	How Prevalent Helps
2. OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships? "The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The level of due diligence and ongoing monitoring, however, may differ for, and should be specific to, each third-party relationship."	A selection of customizable questionnaires enables you to match assessment requirements to the level of risk presented by the relationship.
4. When multiple banks use the same third-party service providers, can they collaborate to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29? "If they are using the same service providers to secure or obtain like products or services, banks may collaborate to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013-29."	Prevalent's Vendor Evidence Sharing Networks are repositories of completed, validated vendor questionnaires and supporting evidence that eliminate the tedious time- and resource-consuming process of collecting data from scratch. Prevalent offers both horizontal and vertical networks to speed assessment and facilitate collaboration within the community.
8. Can a bank engage with a start-up fintech company with limited financial information? "Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring stage of the life cycle."	The Prevalent Cyber & Business Monitoring service offers a continuous view of potential vendor risks. It goes beyond the technical monitoring of cyber threats and network health to deliver a strategic view behind the business drivers of information security risk. Prevalent is the only solution to deliver insight into your vendor ecosystem from data, brand, financial, operational, and regulatory angles, while correlating its findings with internal, control-based assessments for a complete view of third-party risk.
10. What should a bank consider when entering a marketplace lending arrangement with nonbank entities? "Banks should have the appropriate personnel, processes, and systems so that they can effectively monitor and control the risks inherent within the marketplace lending relationship. Risks include reputation, credit, concentrations, compliance, market, liquidity, and operational risks."	

The Prevalent Difference

According to the OCC Bulletin 2013-29, an effective third-party risk management process includes:

- Plans that outline the bank's strategy; identify the inherent risks of the activity; and **detail how the bank selects, assesses, and oversees the third party**
- Proper due diligence in selecting a third party
- Written contracts that outline the rights and responsibilities of all parties
- Ongoing monitoring of the third party's activities and performance
- Contingency plans for terminating the relationship in an effective manner
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management
- Independent reviews that enable bank management to determine that the bank's process aligns with its strategy and effectively manages risks

Prevalent's Third-Party Risk Management Platform enables national banks, federal savings associations, and technology service providers to fulfil these requirements across the entire vendor ecosystem. Delivered in the simplicity of the cloud, the Prevalent platform combines automated vendor assessments, continuous threat monitoring, assessment workflow, and remediation management across the entire vendor life cycle.

Vendor tiering enables third parties to be managed according to the risk they present with different assessments, frequencies, and scoring as warranted. Customizable surveys with documented evidence enable the assessment and monitoring to be carried out relative to the risk and function of each third party. Reporting provides the information necessary in multiple forms as required for different levels of the organization.

Having strong Information Security and Systems Management policies, as well as measuring and monitoring risk associated with being out of compliance, is part of the Third-Party Risk Management Lifecycle. This requires a complete internal view of the controls in place, as well as continuous monitoring of all third parties; something that cannot be addressed with a simple external automated scan. Trust Prevalent's Third-Party Risk Management platform to help address the compliance requirements of OCC Bulletins 2013-29, 2017-07, and 2017-21.

Office of the Superintendent of Financial Institutions of Canada

This chapter of the white paper addresses OSFI Guideline B-10 for third-party risk management.

OSFI and Third-Party Risk Management

In April 2022, the Canadian Government Office of the Superintendent of Financial Institutions (OSFI) issued a draft of Third-Party Risk Management Guideline B-10, which addresses the operational and financial risks associated with vendor and supplier relationships.

Guideline B-10 sets expectations for federally regulated financial institutions (FRFIs) to manage risks associated with third-party arrangements. It is applicable to all FRFIs, except for foreign bank branches and foreign insurance company branches. The Guideline states:

> *"The Office of the Superintendent of Financial Institutions (OSFI) expects that FRFIs practice effective risk management and retain ultimate accountability for all their business activities, functions, and services, whether they are performed in-house or through a third-party arrangement.*
>
> *"To that end, FRFIs are required to provide to OSFI, upon request, information related to their business and strategic arrangements with third parties, risk management, and control environments, to support supervisory monitoring and review work. OSFI expects to be promptly notified of substantive issues affecting the soundness of the FRFI due to a third-party arrangement."*

As well, the guideline expands the definition of a third party to include more entities like independent professionals, brokers, and utilities, and recommends including all third-party types in as part of an assessment.

Driving these new requirements is the shift from materiality to criticality – where a third party performs a function that is integral to the FRFI's provision of a significant operation, function or service, requiring a dual-pronged approach where risk and criticality inform the nature and extent of due diligence activities.

Mapping Prevalent Capabilities to OSFI Guideline B-10 Principles

Guideline B-10 presents five expected outcomes for FRFIs to achieve through managing third-party risk. These outcomes are meant to contribute to the FRFI's operational and financial resilience and help safeguard its reputation. Integrating contract lifecycle management systems with existing risk and procurement solutions will support contracting requirements such as rights and responsibilities of each party throughout its lifecycle, as expected by OSFI.

Supporting the five expected outcomes are 11 principles that OSFI describes as best practices for third-party risk management. The summary table below maps Prevalent Third-Party Risk Management Platform capabilities to these 11 principles.

NOTE: This table should not be considered comprehensive, definitive guidance. Consult your auditor for a complete list of requirements,.

Office of the Superintendent of Financial Institutions Guideline B-10: Third-Party Risk Management	
Managing risks associated with third-party arrangements.	
OSFI Guideline B-10 Principles	How Prevalent Helps
Outcome 1: Governance and accountability structures are clear with comprehensive risk strategies and frameworks in place to contribute to ongoing operational and financial resilience.	
Principle 1: "The FRFI is ultimately accountable for all business activities, functions, and services outsourced to third parties and for managing the risks related to third-party arrangements."	Prevalent partners with you to build a comprehensive third-party risk management (TPRM) program based on proven best practices and extensive real-world experience. Our experts collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence, to termination and offboarding. As part of this process, Prevalent can help you define: • Clear roles and responsibilities (e.g., RACI) • Third-party inventories • Risk scoring and thresholds based on your organization's risk tolerance • Assessment and monitoring methodologies based on third-party criticality • Fourth-party mapping • Sources of continuous monitoring data (cyber, business, reputational, financial) • Key performance indicators (KPIs) and key risk indicators (KRIs) • Governing policies, standards, systems and processes to protect data • Compliance and contractual reporting requirements against service levels • Incident response requirements • Risk and internal stakeholder reporting • Risk mitigation and remediation strategies
Principle 2: "The FRFI should establish a third-party risk management framework (TPRMF) that sets out clear accountabilities, responsibilities, policies, and processes for identifying, managing, mitigating, monitoring, and reporting on risks relating to the use of third parties."	

OSFI Guideline B-10 Principles	How Prevalent Helps
Outcome 2: Risks posed by third parties are identified and assessed.	
Principle 3: "Before entering a third-party arrangement—and, periodically thereafter, proportionate to the level of risk and criticality of the arrangement—the FRFI should identify and assess the risks of the arrangement. Specifically, the FRFI should conduct risk assessments to decide on third-party selection; (re)assess the risk and criticality of the arrangement; and plan for adequate risk mitigation and oversight."	Prevalent centralizes and automates the distribution, comparison, and management of requests for proposals (RFPs) and requests for information (RFIs). Our solutions also deliver business, reputational, financial, and data breach risk insights to inform and add context to vendor selection decisions. Prevalent moves each selected vendor into contracting and/or onboarding due diligence phases, automatically progressing the vendor through the third-party lifecycle. Prevalent features a library of more than 100 pre-built templates for ongoing third-party risk assessments. These are integrated with native cyber, business, reputational, and financial risk monitoring capabilities, which continuously validate assessment findings and fill gaps between assessments. Built-in remediation recommendations ensure that third parties address risks in a timely and satisfactory manner.
Principle 4: "The FRFI should undertake due diligence prior to entering contracts or other forms of arrangement with a third party, and on an ongoing basis proportionate to the level of risk and criticality of the arrangement."	Prevalent offers a pre-contract due diligence assessment with clear scoring based on eight criteria to capture, track and quantify inherent risks for all third parties. Criteria includes: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation From this inherent risk assessment, your team can automatically tier suppliers; set appropriate levels of further diligence; and determine the scope of ongoing assessments.

OSFI Guideline B-10 Principles	How Prevalent Helps
	Rule-based tiering logic enables vendor categorization using a range of data interaction, financial, regulatory and reputational considerations. Prevalent features a library of more than 100 pre-built templates for third-party risk assessments. Assessments can be conducted at the time of contract renewal or at any required frequency (e.g., quarterly or annually). Assessment questionnaires can be globally focused or regional to address unique legal or operational requirements. Prevalent delivers built-in remediation recommendations based on risk assessment results. These are backed by workflow and task management capabilities to ensure that third parties address risks in a timely and satisfactory manner. Integrated, native cyber, business, reputational, and financial risk monitoring capabilities flag material changes between periodic assessments and can trigger notifications, follow-up assessments, or other actions.
Principle 5: "The FRFI should assess, manage, and monitor the risks of subcontracting arrangements entered by third parties, including the impact of these arrangements on concentration risk."	Prevalent can identify fourth-party and Nth-party subcontracting relationships by conducting a questionnaire-based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk. Suppliers discovered through this process are continuously monitored to identify financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening. This approach provides insights to address potential technology or geographic concentration risk.
Outcome 3: Risks posed by third parties are managed and mitigated within the FRFI's Risk Appetite Framework.	
Principle 6: "The FRFI should enter into written arrangements that set out the rights and responsibilities of each party."	Prevalent centralizes the distribution, discussion, retention, and review of vendor contracts. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. Key capabilities include:

OSFI Guideline B-10 Principles	How Prevalent Helps
	• Centralized tracking of all contracts and contract attributes such as type, key dates, value, reminders, and status – with customized, role-based views • Workflow capabilities (based on user or contract type) to automate the contract management lifecycle • Automated reminders and overdue notices to streamline contract reviews • Centralized contract discussion and comment tracking • Contract and document storage with role-based permissions and audit trails of all access • Version control tracking that supports offline contract and document edits • Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access
Principle 7: "Throughout the duration of the third-party arrangement, the FRFI and third party should establish and maintain appropriate measures to protect the confidentiality, integrity and availability of records and data."	Prevalent delivers a centralized, collaborative platform for conducting privacy assessments and mitigating both third-party and internal privacy risks. Key data security and privacy assessment capabilities include: • Scheduled assessments and relationship mapping to reveal where personal data exists, where it is shared, and who has access – all summarized in a risk register that highlights critical exposures • Privacy Impact Assessments to uncover at-risk business data and personally identifiable information (PII) • Vendor assessments against GDPR and other privacy regulations via the Prevalent Compliance Framework (PCF) – reveals potential hot spots by mapping identified risks to specific controls • GDPR risk and response mapping to controls. Includes percent-compliance ratings and stakeholder-specific reports. • A database containing 10+ years of data breach history for thousands of companies – includes types and quantities

OSFI Guideline B-10 Principles	How Prevalent Helps
	of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications • Centralized onboarding, distribution, discussion, retention, and review of vendor contracts – ensures that data protection provisions are enforced from the beginning of the relationship
Principle 8: "The FRFI's third-party arrangements should allow the FRFI timely access to accurate and comprehensive information to assist it in overseeing third-party performance and risks. The FRFI should also have the right to conduct or commission an independent audit of a third party."	With Prevalent, auditors can establish a program to efficiently achieve and demonstrate compliance. The solution automates third-party risk management compliance auditing by collecting vendor risk information, quantifying risks, recommending remediations, and generating reports for dozens of government regulations and industry frameworks. Prevalent automatically maps information gathered from control-based assessments to ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, SOX, NYDFS, and other regulatory frameworks, enabling you to quickly visualize and address important compliance requirements.
Principle 9: "The FRFI's agreement with the third party should encompass the ability to deliver operations through a disruption, including the maintenance, testing, and activation of business continuity and disaster recovery plans. The FRFI should have contingency plans for its critical third-party arrangements."	Prevalent automates the assessment, continuous monitoring, analysis, and remediation of third-party business resilience and continuity – while automatically mapping results to NIST, ISO, and other control frameworks. To complement business resilience assessments and validate results, Prevalent: • Automates continuous cyber monitoring that may predict possible third-party business impacts • Accesses qualitative insights from over 550,000 public and private sources of reputational information that could signal vendor instability • Taps into financial information from a global network of 2 million businesses to identify vendor financial health or operational concerns This proactive approach enables your organization to minimize the impact of third-

OSFI Guideline B-10 Principles	How Prevalent Helps
	party disruptions and stay on top of compliance requirements. The Prevalent Platform includes a comprehensive business resilience assessment based on ISO 22301 standard practices that enables organizations to: • Categorize suppliers according to their risk profile and criticality to the business • Outline recovery point objectives (RPOs) and recovery time objectives (RTOs) • Centralize system inventory, risk assessments, RACI charts, and third parties • Ensure consistent communications with suppliers during business disruptions When a termination or exit is required for critical services, Prevalent leverages customizable surveys and workflows to report on system access, data destruction, access management, compliance with relevant laws, final payments, and more. The solution also suggests actions based on answers to offboarding assessments and routes tasks to reviewers as necessary.
Outcome 4: Third-party performance is continually monitored and assessed, and risks and incidents are proactively addressed.	
Principle 10: "The FRFI should monitor its third-party arrangements to verify the third party's ability to continue to meet its obligations and effectively manage risks."	Prevalent continuously tracks and analyzes external threats to 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. All monitoring data is correlated to assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting and response initiatives. Monitoring sources include: • 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 covering 550,000 companies

OSFI Guideline B-10 Principles	How Prevalent Helps
	• A database containing 10+ years of data breach history for thousands of companies around the world • 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 • A global network of 2 million businesses with 5 years of organizational changes and financial performance, including turnover, profit and loss, shareholder funds, etc. • 30,000 global news sources • A database containing over 1.8 million politically exposed person profiles • Global sanctions lists and over 1,000 global enforcement lists and court filings
Principle 11: "Both the FRFI and its third-party should have documented processes in place to effectively identify, investigate, escalate, track, and remediate incidents to ensure ongoing operational and financial resilience and maintain risk levels within the FRFI's risk appetite."	Prevalent enables your team to rapidly identify and mitigate the impact of third-party vendor incidents by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
Outcome 5: The FRFI's risk management program is dynamic and actively captures and appropriately manages a range of third-party arrangements and interactions.	
Results from the Prevalent inherent risk assessment enables you to tier suppliers, set appropriate levels of further diligence, and determine the frequency and scope of subsequent assessments. Rule-based tiering logic enables vendor categorization based on a range of data interaction, financial, regulatory and reputational considerations. Rules apply to all third parties, regardless of contract status. You can also continuously monitor non-contract vendors against cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information to catch potential problems before they escalate.	

The Prevalent Difference

Prevalent can help organizations automate the assessment and continuous monitoring of third-party business and financial resilience to support compliance and conformity with OSFI Guideline B-10. The Prevalent Third-Party Risk Management Platform:

- Automates and adds business resilience risk intelligence to vendor selection decisions
- Delivers comprehensive pre-contract due diligence assessments to calculate inherent risk
- Simplifies contracting processes to ensure all business resilience key performance indicators (KPIs) are in place and tracked
- Profiles and tiers all third parties, right-sizing ongoing due diligence according to criticality
- Maps fourth parties to understand risk among subcontractors
- Adds workflow to automate the assessment, risk scoring and remediation process
- Continuously monitors third parties for cyber, business, reputational and financial risk monitoring to correlate risks against assessment results and validate findings
- Automates incident response process, speeding time to resolution
- Includes compliance and risk reporting by framework or regulation
- Delivers a foundation for an agile third-party risk management program

Foreign Corrupt Practices Act (FCPA)

This chapter of the white paper addresses how organizations should assess suppliers to ensure their business practices do not include illegal bribes.

FCPA Summary

Originally passed into law in 1977 and amended in 1988 and 1998, the US Foreign Corrupt Practices Act (FCPA) makes it unlawful for US citizens and companies to make payments to foreign government officials to assist in obtaining or retaining business. The law also contains provisions prohibiting foreign representatives from doing the same within the territory of the United States. As well, the FCPA requires companies whose securities are listed in the US to keep records and maintain internal accounting controls to detect such transactions.

Meeting FCPA Requirements

With fines for violations of up to $5 million and 20 years in prison, and $25 million for companies, it is important to ensure that not only your organization's practices, but also your third-party vendor's and supplier's practices, are compliant with FCPA to avoid a business-impacting disruption or reputational damage.

Provisions in the FCPA include:

- Public companies filing annual documentation with the Securities & Exchange Commission (SEC) attesting to adherence to FCPA provisions
- Keeping financial records for all transaction in scope, which are auditable at any time
- Maintaining internal accounting controls and monitoring to track and prevent potential violations

The problem many organizations face when assessing their third parties' anti-bribery and corruption (ABAC) policies is that the effort is highly manual and lacks real time insights into legal filings.

The below table summarizes how Prevalent can simplify this process.

Foreign Corrupt Practices Act	
Maintaining ethics and transparency in conducting business transactions.	
FCPA Best Practices	How Prevalent Helps
Implement comprehensive supply chain partner pre-screening	Ensure that procurement and sourcing teams have access to intelligence pertaining to all new supply chain partner ABAC practices. This can include centralizing previous assessment results, reputational information, legal actions, country-level corruption perception index (CPI) scores and previous sanctions so they can make informed supplier sourcing decisions.
Assess supply chain partners regularly	Leverage an automated solution that hosts assessment questionnaires, raises risks if results don't line up with expected risk tolerance levels, and offers specific remediation recommendations. Include supporting evidence and ABAC policy documentation with assessment results to simply inevitable audit reporting.

FCPA Best Practices	How Prevalent Helps
Fill gaps between assessments with continuous reputational monitoring	Adding real-time monitoring of the following sources will help to catch potential adverse events before they impact your business and will also validate the results of assessments. • Supplier Reputation: Public and private sources of reputational information, including regulatory and legal actions, M&A activity, adverse media and conflicts of interest. • Financials and Investments: Financial performance, turnover, profit and loss, and shareholder funds transparency. • Global Sanctions: Screen against the world's most important sanctions lists (including OFAC, EU, UN, BOE, FBI, BIS, etc.), global enforcement lists, and court filings (such as the FDA, US HHS, UK FSA, SEC and more). • Politically Exposed Persons (PEP): Politically exposed person profiles, including families and associates, to identify potential leadership risks. • State-Owned Enterprises: A list of government-owned and government-linked enterprises.
Know Your Nth Parties	Your third parties rely on their own suppliers and third parties to deliver goods and services to you and other customers. And when this extended partner ecosystem has an adverse event you need to respond quickly to it. That's why it's important to identify and visualize relationships between your organization and third, fourth and Nth parties to discover dependencies and risks and avoid the reputational hit.
Simplify compliance reporting	The fastest, least-complex approach to meeting audit requirements would be to automatically map the assessment results to reporting that aligns with FCPA requirements.

The Prevalent Difference

The US federal government has not hesitated to file charges against individuals and companies that have violated the anti-bribery provisions in the FCPA. Prevalent can help you centralize the management of third parties, define the appropriate assessment methodology, monitor adherence to requirements, and simplify regulatory reporting.

UK Bribery Act of 2010

This chapter of the white paper addresses how organizations should consider assessing their suppliers to ensure their business practices comply with anti-bribery legislation..

UK Bribery Act of 2010 Summary

The Bribery Act of 2010 is a United Kingdom (UK) law that defines and enforces the crime of bribery to ensure companies can compete on a level playing field. Section 7 of the law introduced a new offense - the failure of an organization to prevent bribery on its behalf.

The UK government provides guidance to help organizations meet the requirements in the Act. Companies that use third parties should be aware of these provisions and assess their vendors, supply chain partners and other third parties accordingly.

Meeting UK Bribery Act of 2010 Requirements

As part of the law, companies are required to:

- Conduct third-party risk assessments to determine how a supplier's country, sector, transactional and partnership risks impact the organization
- Perform due diligence as part of a wider governance approach to third-party risks
- Validate supplier anti-bribery practices with external verification and monitoring

The below table summarizes how Prevalent can simplify this process.

UK Bribery Act of 2010	
Preventing bribery on an organization's behalf.	
UK Bribery Act Best Practices	How Prevalent Helps
Pre-Screen Suppliers	Rapidly pre-screen vendors using a library of continuously updated risk scores based on inherent/residual risk, assessment results and real-time reputational monitoring.
Build a Comprehensive Supplier Profile	Tap into 550,000+ sources of vendor intelligence to build a comprehensive supplier profile that includes industry and business insights, including potentially risky 4th-party relationships.
Score Inherent Risks	Use a simple assessment with clear scoring to track and quantify inherent risks for all onboarded suppliers
Perform Detailed Assessments	Leverage Prevalent's built-in Anti-Bribery and Ethics assessments to determine adherence to policies and identify potential areas of concern. Review and approve assessment responses to automatically register risks or reject responses and request additional input.
Monitor Supplier Reputation	Validate assessment results and gain continuous supplier insights from over 550,000 public and private sources of reputational information, including negative news, regulatory and legal actions, adverse media, and more.

UK Bribery Act Best Practices	How Prevalent Helps
Financial & Investment Monitoring	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 transparency, and more.
Monitor Against a Central Global Sanctions Database	Simultaneously screen against the world's most important sanctions lists (including OFAC, EU, UN, BOE, FBI, BIS, etc.), over 1,000 global enforcement lists, and court filings (such as the FDA, US HHS, UK FSA, SEC and more) to proactively identify prohibited business relationships.
Screen for Politically-Exposed Persons (PEPs)	Screen against a global PEP database with access to over 1.8 million politically exposed person profiles, including families and associates, to identify potential leadership risks.
Screen for State-Owned Enterprises	Avoid conflicts of interest by checking companies against a proprietary list of government-owned and government-linked enterprises.
Score the Corruption Perception Index	Corruption Perception Index (CPI) scores of company head office countries add more business context to vendor risk analysis by delivering insights into a vendor's viability and ethics.
Centrally Manage Risks	Normalize, correlate and analyze assessment results and continuous monitoring intelligence for unified risk reporting and remediation.
Remediate	Take actionable steps to reduce modern slavery exposure with built-in remediation recommendations and guidance.
Store Documents and Evidence	Store and distribute Modern Slavery policy documents for dialog and attestation.
Map Relationships	Identify relationships between your organization and third, fourth and Nth parties to discover dependencies and assess your exposure.
Report on Compliance	Visualize and address compliance requirements by automatically mapping assessment results to Modern Slavery requirements.

The Prevalent Difference

Prevalent helps organizations assess their third parties against multiple anti-bribery, corruption and ethics requirements and provides continuous reputational, compliance and corruption insights to ensure their third parties are complying with the law.

UK Modern Slavery Act of 2015

This chapter of the white paper addresses how organizations should consider assessing their suppliers to ensure their business practices comply with ant-slavery labor legislation.

UK Modern Slavery Act of 2015 Summary

The Modern Slavery Act of 2015 is a United Kingdom (UK) law that requires organizations to publicly communicate the steps they are taking (or not taking) to ensure that forced labor, human trafficking, and other forms of involuntary servitude are not taking place in their businesses or supply chains. The "Transparency in Supply Chains" section of the Act (Part 6, Section 54), defines what form this should take for third party relationships.

Meeting Modern Slavery Act Requirements

As part of the law, companies are required to:

- Publish an annual statement detailing the steps taken (or not) to ensure that modern slavery is not taking place in their business or supply chain
- Improve due diligence on suppliers to ensure they are adhering to the law

The below table summarizes how Prevalent can simplify this process.

UK Modern Slavery Act of 2015	
Ensuring that forced labor, human trafficking, and other forms of involuntary servitude are not taking place in a business or supply chain.	
UK Modern Slavery Act Best Practices	How Prevalent Helps
Pre-Screen Suppliers	Rapidly pre-screen vendors using a library of continuously updated risk scores based on inherent/residual risk, assessment results and real-time reputational monitoring.
Build a Comprehensive Supplier Profile	Tap into 550,000+ sources of vendor intelligence to build a comprehensive supplier profile that includes industry and business insights, including potentially risky 4th-party relationships.
Score Inherent Risks	Use a simple assessment with clear scoring to track and quantify inherent risks for all onboarded suppliers
Perform Detailed Assessments	Leverage Prevalent's built-in Modern Slavery assessment to determine adherence to policies. Review and approve assessment responses to automatically register risks or reject responses and request additional input.
Identify Modern Slavery Statements	Automatically identify if a Modern Slavery Statement exists on the website of over 18,000 companies to support compliance validation activities.
Monitor Supplier Reputation	Validate assessment results and gain continuous supplier insights from over 550,000 public and private sources of reputational information, including negative news, regulatory and legal actions, adverse media, and more.

UK Modern Slavery Act Best Practices	How Prevalent Helps
Centrally Manage Risks	Normalize, correlate and analyze assessment results and continuous monitoring intelligence for unified risk reporting and remediation.
Remediate	Take actionable steps to reduce modern slavery exposure with built-in remediation recommendations and guidance.
Store Documents and Evidence	Store and distribute Modern Slavery policy documents for dialog and attestation.
Map Relationships	Identify relationships between your organization and third, fourth and Nth parties to discover dependencies and assess your exposure.
Report on Compliance	Visualize and address compliance requirements by automatically mapping assessment results to Modern Slavery requirements.

The Prevalent Difference

Prevalent helps organizations apply a rigorous level of due diligence to their suppliers by determining if a public statement exists, and validating policies and processes through Modern Slavery risk assessments and continuous external monitoring of their real-world practices. Armed with these insights, organizations improve their visibility into their supply chain partners' labor practices, reducing the risk of reputational damage.

US Department of Defense Cybersecurity Maturity Model Certification (CMMC)

This chapter provides an overview of US Department of Defense (DoD) cybersecurity requirements for Defense Industrial Base Suppliers (DIBS) as updated in November 2021.

CMMC Summary

In November 2021, the Office of the Under Secretary of Defense for Acquisition and Sustainment in the United States Department of Defense (DoD) released v2.0 of the Cybersecurity Maturity Model Certification (CMMC), a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. Version 2.0 greatly simplifies the model by streamlining certification levels from five (5) to three (3), eliminating priorietary maturity layers, and adjusting assessment responsibilities.

CMMC requires companies to achieve certification against cybersecurity and controlled unclassified information (CUI) handling best practices, with that certification eventually determining whether a company can be awarded a contract by the DoD. Meant to help small businesses demonstrate cybersecurity protections more easily and cost-effectively, CMMC aims to ensure that our entire national defense supply chain is secure and resilient.

All DoD suppliers will eventually be required to be certified at one of three levels, from Level 1 (Foundational) to Level 3 (Expert). This represents a change from version 1.0 that featured five certification levels. Version 2.0 certification levels are derived from the basic safeguarding requirements for Federal Contract Information (FCI) specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for controlled unclassified information (CUI) specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 and additional controls from NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171.

- **Level 1** – Self-assessment performed by the supplier against 17 controls. This level of certification is considered foundational and for suppliers managing FCI that is not critical to national security. This certification level is unchanged from version 1.0, originally announced in January 2020.
- **Level 2** – A more advanced level of certification performed by third-party auditors (known as C3PAOs, or certified third-party audit organizations) against an additional 110 controls in the NIST SP 800-171 standard. This level is considered for companies that have controlled unclassified information (CUI). In some cases organizations can perform a self-assessment at this level.
- **Level 3** – Considered an expert level for the highest-priority DoD suppliers, this level builds on Level 2 by adding a subset of NIST SP 800-172 controls on top. The federal government will conduct the audits for companies at this level.

Meeting CMMC Requirements

Please see the table below for a summary of the CMMC requirements by level, organized by NIST SP 800-171 Relevant Security Controls. The Prevalent Third-Party Risk Management Platform has built-in questionnaires for each level, enabling auditors to assess their clients, and suppliers to assess themselves and their suppliers for compliance against each level.

US Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)

To ensure that our entire national defense supply chain is secure and resilient.

NIST 800-171r2 Relevant Security Controls by Level of Certification

Domain	Level 1 (17 Controls)	Level 2 (+110 Controls)	Level 3
Access Control	**3.1.1** Authorized Access Control **3.1.2** Transaction & Function Control **3.1.20** External Connections **3.1.22** Control Public Information	**3.1.3** Control CUI Flow **3.1.4** Separation of Duties **3.1.5** Least Privilege **3.1.6** Non-Privileged Account Use **3.1.7** Privileged Functions **3.1.8** Unsuccessful Logon Attempts **3.1.9** Privacy & Security Notices **3.1.10** Session Lock **3.1.11** Session Termination **3.1.12** Control Remote Access **3.1.13** Remote Access Configurability **3.1.14** Remote Access Routing **3.1.15** Privileged Remote Access **3.1.16** Wireless Access Authorization **3.1.17** Wireless Access Protection **3.1.18** Mobile Device Connection **3.1.19** Encrypt CUI on Mobile **3.1.21** Portable Storage Use	*Information on Level 3 will be released at a later date and will contain a subset of the security requirements specified in NIST SP 800-172.*
Awareness and Training		**3.2.1** Role-Based Risk Awareness **3.2.2** Roles-Based Training **3.2.3** Insider Threat Awareness	
Audit and Accountability		**3.3.1** System Auditing **3.3.2** User Accountability **3.3.3** Event Review **3.3.4** Audit Failure Alerting **3.3.5** Audit Correlation **3.3.6** Reduction & Reporting **3.3.7** Authoritative Time Source **3.3.8** Audit Protection **3.3.9** Audit Management	
Configuration Management		**3.4.1** System Baselining	

		3.4.2 Security Configuration Enforcement **3.4.3** System Change Management **3.4.4** Security Impact Analysis **3.4.5** Access Restrictions for Change **3.4.6** Least Functionality **3.4.7** Nonessential Functionality **3.4.8** Application Execution Policy **3.4.9** User-Installed Software	
Identification and Authentication	**3.5.1** Identification **3.5.2** Authentication	**3.5.3** Multi-factor Authentication **3.5.4** Replay-Resistant Authentication **3.5.5** Identifier Reuse **3.5.6** Identifier Handling **3.5.7** Password Complexity **3.5.8** Password Re-use **3.5.9** Temporary Passwords **3.5.10** Cryptographically-Protected Passwords **3.5.11** Obscure Feedback	
Incident Response		**3.6.1** Incident Handling **3.6.2** Incident Reporting **3.6.3** Incident Response Testing	
Maintenance		**3.7.1** Perform Maintenance **3.7.2** System Maintenance Control **3.7.3** Equipment Sanitization **3.7.4** Media Inspection **3.7.5** Nonlocal Maintenance **3.7.6** Maintenance Personnel	
Media Protection	**3.8.3** Media Disposal	**3.8.1** Media Protection **3.8.2** Media Access **3.8.4** Media Markings **3.8.5** Media Accountability **3.8.6** Portable Storage Encryption **3.8.7** Removable Media **3.8.8** Shared Media **3.8.9** Protect Backups	
Personnel Security		**3.9.1** Screen Individuals **3.9.2** Personnel Actions	
Physical Protection	**3.10.1** Limit Physical Access **3.10.3** Escort Visitors **3.10.4** Physical Access Logs **3.10.5** Manage Physical Access	**3.10.2** Monitor Facility **3.10.6** Alternative Work Sites	
Risk		**3.11.1** Risk Assessments	

Assessment		**3.11.2** Vulnerability Scan **3.11.3** Vulnerability Remediation	
Security Assessment		**3.12.1** Security Control Assessment **3.12.2** Plan of Action **3.12.3** Security Control Monitoring **3.12.4** System Security Plan	
System and Communications Protection	**3.13.1** Boundary Protection **3.13.5** Public-Access System Separation	**3.13.2** Security Engineering **3.13.3** Role Separation **3.13.4** Shared Resource Control **3.13.6** Network Communication by Exception **3.13.7** Split Tunneling **3.13.8** Data in Transit **3.13.9** Connections Termination **3.13.10** Key Management **3.13.11** CUI Encryption **3.13.12** Collaborative Device Control **3.13.13** Mobile Code **3.13.14** Voice over Internet Protocol **3.13.15** Communications Authenticity **3.13.16** Data at Rest	
System and Information Integrity	**3.14.1** Flaw Remediation **3.14.2** Malicious Code Protection **3.14.4** Update Malicious Code Protection **3.14.5** System & File Scanning	**3.14.3** Security Alerts & Advisories **3.14.6** Monitor Communications for Attacks **3.14.7** Identify Unauthorized Use	

The Prevalent Difference

The Prevalent Third-Party Risk Management Platform has built-in questionnaires for Level 1 and Level 2, enabling suppliers to assess themselves and auditors to assess their clients against each level. When Level 3 certification requirements have been published, Prevalent will add the appropriate questionnaire to the Platform.

C3PAOs can:

- Invite clients into the Prevalent Platform to complete their standardized Level 2 control assessment in an easy-to-use, secure tenant
- Automate chasing reminders to suppliers or clients to reduce the time required to complete assessments
- Centralize supporting documents submitted as evidence of the presence of controls
- View a single register of risks raised depending on how the client or supplier responds to the questions
- Issue remediation recommendations for failed controls
- Deliver customized reporting on the current level of compliance, demonstrating the risk-reducing impact of the application of future controls

Any DoD supplier can conduct a Level 1 or Level 2 self-assessment to:

- Assess themselves against the 17 controls required to measure Level 1 compliance
- Assess themselves against the 110 controls required to measure Level 2 compliance
- Upload documentation and evidence to support answers to questions
- Gain visibility into current compliance status
- Leverage built-in remediation guidance to address shortcomings
- Produce reporting to measure compliance for auditors

Part II: Industry Standards & 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 provides a framework for establishing, implementing, maintaining, and continually improving an information security management system. It also outlines a systematic approach to managing sensitive company information so that it remains secure.

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 identify what they need to meet these requirements.

Together, ISO 27001 and 27002 are the foundation of most ISO standards related to cybersecurity. With respect to managing information security in supplier relationships, **Section 15 of ISO 27001 and ISO 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.

ISO 27018 establishes control objectives, controls, and guidelines for implementing measures to protect Personally Identifiable Information (PII). It specifies guidelines based on ISO 27002, and is applicable to both PII processors and controllers. Any organization that uses third parties to store or manage their customer data should assess those vendors against this standard.

ISO 27701 details requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as a complementary extension to ISO 27001 and 27002. As with ISO 27018, organizations with third parties that manage data on their behalf should assess those vendors against this ISO standard.

ISO 27036-2 specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships. This

standard is particularly relevant for third-party risk management, as the requirements cover procurement and supply of products and services.

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

This table summarizes specific supplier relationship controls discussed in ISO 27001 and ISO 27002, overlaid by complementary ISO 27701 privacy controls. ISO 27018 guidance is not referenced below, because ISO 27018 simply indicates that ISO 27002 controls are applicable in each use case.

ISO 27001:2013: Information Security Management Systems - Requirements ISO 27002:2013: Code of Practice for Information Security Controls ISO 27701:2019: Extension for Privacy Information Management ISO 27018:2019(E): Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors	
These standards set requirements for establishing, implementing, maintaining and continually improving an information security management system.	
ISO 27001/27002 Requirements & ISO 27701 Applicability	How Prevalent Helps
15: Supplier Relationships	
15.1 Information security in supplier relationships "Objective: To ensure protection of the organization's assets that are accessible by suppliers."	Prevalent offers security, privacy, and risk management professionals an automated platform to centrally manage the supplier risk assessment process and determine third-party compliance with IT security and data privacy requirements across the vendor lifecycle. The Platform employs both standard and custom ISO-based questionnaires to help collect evidence and provides bi-directional remediation workflows, 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 **& ISO 27701 6.12.1.1** "Control: 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 automated assessments and an environment to include and manage documented due-diligence evidence.

ISO 27001/27002 Requirements & ISO 27701 Applicability	How Prevalent Helps
15.1.1 a) "identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;"	The Prevalent Platform enables organizations to automatically tier suppliers according to their inherent risk scores, set appropriate levels of diligence, and determine the scope of ongoing assessments. Organizations can also categorize vendors with rule-based logic based on a range of data interaction, financial, regulatory and reputational considerations.
15.1.1 b) "a standardised process and lifecycle for managing supplier relationships;"	Prevalent delivers a programmatic process for managing risks across every stage of the vendor lifecycle: • Sourcing and selection – Access a central repository of risk insights for thousands of potential vendors • Intake and onboarding – Centralize vendor onboarding and management • Inherent risk scoring – Improve risk visibility to prioritize vendors • Risk assessments – Automate and accelerate the vendor risk assessment process with built-in templates, reporting and remediation management • Continuous monitoring – Validate vendor security controls with continuous cyber, business, reputational and financial risk intelligence • Performance and SLA management – Centrally monitor, manage and report on vendor performance and contracts • Offboarding and termination – Securely wind down business relationships with assessment templates and reporting
15.1.1 e) "processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;"	The Prevalent Platform includes 75+ pre-defined assessment templates, the ability to import offline assessments or build custom questionnaires with risk and control elements relevant to your business.
15.1.1 h) "handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;"	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact of supply chain breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.

ISO 27001/27002 Requirements & ISO 27701 Applicability	How Prevalent Helps
15.1.1 i) “resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;”	The Prevalent Third-Party Risk Management Platform includes unified capabilities for assessing, analyzing and addressing weaknesses in supplier business resilience plans. This enables you to proactively work with your supplier community to prepare for pandemics, environmental disasters, and other potential crises.
15.1.1 l) “conditions under which information security requirements and controls will be documented in an agreement signed by both parties;”	The Prevalent Platform enables organizations to collaborate on documents and certifications, such as NDAs, SLAs, SOWs and contracts, with built-in version control, task assignment and auto-review cadences. Manage all documents throughout the vendor lifecycle in centralized vendor profiles.
15.1.1 m) “managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.”	With the Prevalent Platform, organizations can leverage customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more.
15.1.2 Addressing security in supplier agreements **& ISO 27701 6.12.1.2** "Control: 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 provides a detailed assessment on how an organization has implemented information security controls and applied additional privacy-based controls to manage and support their products and services. 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. The Prevalent Platform also centralizes agreements, contracts and supporting evidence with built-in task and acceptance management, plus mandatory upload features to simplify document and supplier agreement management.

ISO 27001/27002 Requirements & ISO 27701 Applicability	How Prevalent Helps
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 the ISO industry standard framework and/or custom questionnaires). The platform includes built-in workflow capabilities that enable 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. Organizations can assess third parties against cybersecurity, SLA performance, and other topics, and correlate findings with the results of continuous outside monitoring for a complete view of risks.
15.1.2 g) "information security policies relevant to the specific contract;"	The Prevalent Platform enables organizations to assess suppliers on information security criteria using a specific ISO questionnaire or a custom assessment, with flagging and tagging of risks for follow-up. All contract documentation is centrally housed in the Platform.
15.1.2 m) "right to audit the supplier processes and controls related to the agreement;"	The Prevalent solution provides a simple, trackable, repeatable mechanism to perform controls audits, including a built-in risk register, reporting and remediation guidance.
15.1.2 n) "defect resolution and conflict resolution processes;"	Bi-directional workflow in the Prevalent 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 solution ensures suppliers implement the exact, agreed-upon requirements with regular tracking and verification.
15.1.3 Information and communication technology supply chain **& ISO 27701 6.12.1.3** "Control: 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 & ISO 27701 Applicability	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.
15.1.3 f) "obtaining assurance that critical components and their origin can be traced throughout the supply chain;"	With the Prevalent Platform, organizations can identify relationships with third parties, 4th parties and Nth parties to reveal dependencies and information paths.
15.2 Supplier service delivery management "Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements."	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 Monitoring and review of supplier services **& ISO 27701 6.12.2.1** "Control: Organizations should regularly monitor, review and audit supplier service delivery."	The Prevalent Platform enables organizations to gain visibility into vendor contract status, contact information, risk and compliance status, performance metrics, and more via centralized dashboards – while also leveraging PowerBI integration for custom reporting. Armed with these insights, teams have visibility into whether or not a supplier is meeting is agreed-upon requirements.
15.2.1 a) "monitor service performance levels to verify adherence to the agreements;"	With the Prevalent Platform, organizations can customize surveys to make it easy to gather and analyze necessary performance and contract data in a single risk register. Prevalent identifies key contract attributes relating to SLAs or performance, populates those requirements in the Platform, and assigns tasks to you and your third party for tracking purposes.
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 relationships between third, fourth, and Nth parties.

ISO 27001/27002 Requirements & ISO 27701 Applicability	How Prevalent Helps
15.2.1 h) "ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster"	Organizations can leverage Prevalent's built-in business resilience assessment questionnaire to understand supplier incident response, disaster recovery and communications plans. Review and approve assessment responses to automatically register risks, or reject responses and request additional input.

Meeting ISO 27036-2 Third-Party Risk Management Standards

Although the entire ISO 27036-2 standard is applicable for supplier relationships, this table highlights only the most prominent controls.

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.

ISO 27036-2 Requirements	How Prevalent Helps
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.
6.2.2.2 Organizational project-enabling processes / Infrastructure management process / Activities b) Define, implement, maintain and improve contingency arrangements to ensure that the procurement or the supply of a product or service can continue in the event of its disruption caused by natural or man-made causes.	Prevalent provides a built-in business resilience assessment questionnaire to evaluate supplier incident response, disaster recovery and communications plans. Review and approve assessment responses to automatically register risks, or reject responses and request additional input.
6.2.3.2 Project portfolio management process / Activities a) Define, implement, maintain and improve a process for identifying and categorizing suppliers or acquirers based on the sensitivity of the information shared with them and on the access level granted to them to acquirer's or supplier's assets, such as information and information systems;	The Prevalent Platform enables organizations to automatically tier suppliers according to their inherent risk scores, set appropriate levels of diligence, and determine the scope of ongoing assessments. Organizations can also categorize vendors with rule-based logic based on a range of data interaction, financial, regulatory and reputational considerations.
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.

ISO 27036-2 Requirements	How Prevalent Helps
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 800-53r5, SP 800-161r1, and NIST CSF v1.1 Standards and Frameworks

This chapter addresses NIST Special Publication 800-53r5, SP 800-161r1 and the NIST Framework for Improving Critical Infrastructure (CSF) v1.1.

The National Institute of Standards and Technology (NIST) is a federal agency within the United States Department of Commerce. NIST's responsibilities include establishing computer and information technology-related standards and guidelines for federal agencies. Because NIST publishes and maintains key resources for managing cybersecurity risks applicable to any company, nearly 50% of private sector organizations have also adopted their guidelines, making NIST publications the primary standards for evaluating IT controls.

Although several NIST special publications have specific controls that address third-party supplier IT security, the most applicable are:

- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- SP 800-161 Rev.1: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- Cybersecurity Framework v1.1: Framework for Improving Critical Infrastructure Cybersecurity

These guidelines complement one another, so organizations that standardize on one special publication can cross-map to the others – in effect meeting multiple requirements using a single framework.

NIST SP 800-53r5, SP 800-161r1 and NIST CSF v1.1 Summary

SP 800-53 Rev. 5 has expanded and refined supply chain security and privacy guidelines beyond Rev. 4 by establishing an entirely new control group, SR-Supply Chain Risk Management. It also requires organizations to develop and plan for managing supply chain risks by:

- Using formal risk management plans and policies to drive the supply chain management process
- Emphasizing security and privacy through collaboration in identifying risks and threats, and through the application of security and privacy-based controls
- Requiring transparency of systems and products (e.g., lifecycle, traceability, and component authenticity)
- Increasing awareness of the need to pre-assess organizations, and to ensure visibility into issues and breaches

NIST SP 800-53 is considered the foundation upon which all other cybersecurity controls are built, but with SP 800-161r1, NIST outlines a complementary framework to identify, assess, select, and implement risk management processes and mitigating controls specific to supply chain risks. Together, SP 800-53 and supplemental SP 800-161 control guidance present a comprehensive framework for assessing and mitigating supplier risks.

The Cybersecurity Framework is another NIST publication that applies to third-party risk management and supply chain security. The Framework leverages existing security frameworks, such as CIS, COBIT, ISA, ISO/IEC and NIST, to avoid creating an undue burden on organizations to address requirements. Specific supply chain risk management subcategories identified in the CSF include:

- ID.SC-1: Identify, establish, assess, and manage cyber supply chain risk management processes, and ensure that organizational stakeholders agree.
- ID.SC-2: Identify, prioritize, and assess suppliers and third-party partners of information systems, components, and services using a cyber supply chain risk assessment process.

- ID.SC-3: Implement appropriate measures in supplier and third-party partner contracts to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- ID.SC-4: Routinely assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- ID.SC-5: Conduct response and recovery planning and testing with suppliers and third-party providers.

Meeting NIST SP 800-53r5, SP 800-161r1 and NIST CSF v1.1 Standards and Frameworks

The following summary table maps capabilities available in the Prevalent Third-Party Risk Management Platform to select third-party, vendor, or supplier controls present in SP 800-53, with SP 800-161 and the Cybersecurity Framework v1.1 control overlays (bolded) applied to the table to illustrate cross-mapping. For a complete mapping, please download the NIST Compliance Checklist.

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
SP 800 53 Control with SP 800-161 Overlay **CA-2 (1)** Control Assessments | Specialized Assessments **CA-2 (3)** Control Assessments | Leveraging Results from External Organizations CSF v1.1 Applicable Controls ID.RA-1: Asset Vulnerabilities are identified and documented. DE.DP-4: Event detection information is communicated.	The Prevalent Third-Party Risk Management Platform includes more than 100 standardized risk assessment survey templates – including for NIST, ISO and many others — a custom survey creation wizard, and a questionnaire that automatically 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. Prevalent Vendor Threat Monitor (VTM) continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform by monitoring the Internet and dark web for cyber threats and vulnerabilities. It also correlates assessment findings with research on operational, financial, legal and brand risks in a unified risk register that enables centralized risk triage and response. With the Prevalent Platform, you can efficiently communicate with vendors and coordinate remediation efforts. Capture and audit conversations; record estimated completion dates; accept or reject submissions on an answer-by-answer basis; assign tasks based on risks, documents or entities; and match documentation and evidence to risks.

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
SP 800 53 Control with SP 800-161 Overlay **CA-7 (3)** Continuous Monitoring | Trend Analyses CSF v1.1 Applicable Controls ID.RA-1: Asset Vulnerabilities are identified and documented. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors. DE.CM-1: The network is monitored to detect potential cybersecurity events. RS.AN-1: Notifications from detection systems are investigated. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked 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. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support.
SP 800 53 Control with SP 800-161 Overlay **CP-2 (3)** Contingency Plan | Coordinate with External Service Providers CSF v1.1 Applicable Controls ID.BE-1: The organization's role in the supply chain is identified and communicated. **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. DE.AE-4: Impact of events is determined. RS.RP-1: Response plan is executed during or after an incident.	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact of supply chain breaches by centrally managing vendors, proactively conducting event assessments, scoring identified risks, and accessing remediation guidance. The Prevalent Platform includes unified capabilities for assessing, analyzing and addressing weaknesses in supplier business resilience plans. This enables you to proactively work with your supplier community to prepare for pandemics, environmental disasters, and other potential crises. In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals.

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
RS.CO-3: Information is shared consistent with response plans. RS.CO-4: Coordination with stakeholders occurs consistent with response plans. RS.AN-2: The impact of the incident is understood. RS.AN-4: Incidents are categorized consistent with response plans. RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	All risk intelligence is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
<u>SP 800 53 Control with SP 800-161 Overlay</u> **IR-4 (3)** Incident Handling | Supply Chain Coordination <u>CSF v1.1 Applicable Controls</u> **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors. DE.AE-4: Impact of events is determined. DE.AE-5: Incident alert thresholds are established. RS.RP-1: Response plan is executed during or after an incident. RS.CO-3: Information is shared consistent with response plans. RS.CO-4: Coordination with stakeholders occurs consistent with response plans. RS.AN-1: Notifications from detection systems are investigated.	The Prevalent Third-Party Incident Response Service enables you to rapidly identify and mitigate the impact supply chain breaches by centrally managing vendors, proactively conducting event assessments, scoring identified risks, and accessing remediation guidance. The Prevalent Platform includes unified capabilities for assessing, analyzing and addressing weaknesses in supplier business resilience plans. This enables you to proactively work with your supplier community to prepare for pandemics, environmental disasters, and other potential crises. In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals. All risk intelligence is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
RS.AN-2: The impact of the incident is understood. RS.AN-4: Incidents are categorized consistent with response plans. RS.MI-2: Incidents are mitigated. RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	
SP 800 53 Control with SP 800-161 Overlay **IR-5** Incident Monitoring	Prevalent Contract Essentials is a SaaS solution that centralizes the distribution, discussion, retention, and review of vendor contracts. It also includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With Contract Essentials, your procurement and legal teams have a single solution to ensure that key contract clauses are in place, and that service levels and response times are managed.
SP 800 53 Control with SP 800-161 Overlay **IR-6 (1)** Incident Reporting | Supply Chain Coordination CSF v1.1 Applicable Controls **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. RS.CO-2: Incidents are reported consistent with established criteria.	All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
SP 800 53 Control with SP 800-161 Overlay **IR-8** Incident Response Plan	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. The Incident Response Services provides the foundation to be well prepared for board and executive questions regarding the impact of supply chain incidents;

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
	and demonstrate proof of your third-party breach response plan with auditors and regulators.
SP 800 53 Control with SP 800-161 Overlay **PM-16** Threat Awareness Program CSF v1.1 Applicable Controls ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources. ID.RA-3: Threats, both internal and external, are identified and documented. ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked 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. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
SP 800 53 Control with SP 800-161 Overlay **PM-31** Continuous Monitoring Strategy	Prevalent VTM reveals third-party cyber incidents for 550,000 actively tracked 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. Prevalent then normalizes, correlates and analyzes information from across multiple inputs, including inside-out risk assessments and outside-in monitoring from Prevalent Vendor Threat Monitor and BitSight. This unified model provides context, quantification, management and remediation support. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
	scoring model based on likelihood of an event and its impact.
SP 800 53 Control with SP 800-161 Overlay **RA-1** Policy and Procedures	The Prevalent Platform includes more than 100 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. With the Prevalent Platform, you can automatically generate a risk register upon survey completion, ensuring that the entire risk profile (or a role-specific version) 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. Then, you can take actionable steps to reduce vendor risk with built-in remediation recommendations and guidance.
SP 800 53 Control with SP 800-161 Overlay **RA-3** Risk Assessment CSF v1.1 Applicable Controls ID.RA-1: Asset Vulnerabilities are identified and documented. ID.RA-3: Threats, both internal and external, are identified and documented. ID.RA-4: Potential business impacts and likelihoods are identified. ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. **ID.SC-2:** Suppliers and third party partners of information systems, components, and services	The Prevalent Platform includes more than 100 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. 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. In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform provides cyber security, business, reputational and financial monitoring –

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
are identified, prioritized, and assessed using a cyber supply chain risk assessment process CSF DE.AE-4: Impact of events is determined. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
SP 800 53 Control with SP 800-161 Overlay **RA-7** Risk Response	The Prevalent Platform features built-in guidance to remediate control failures or other identified risks to levels acceptable level to your organization. Prevalent also enables risk assessors to communicate with third parties about remediations, document conversations and updates, and store supporting control documentation in a centralized repository.
SP 800 53 Control with SP 800-161 Overlay **RA-9** Criticality Analysis	Prevalent offers an inherent risk assessment questionnaire with clear scoring based on eight criteria to capture, track and quantify risks for all third parties. The assessment criteria include: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation Using the inherent risk assessment, you can automatically tier suppliers, set appropriate levels of further diligence, and determine the scope of subsequent, periodic assessments. Rule-based tiering logic enables suppliers to be categorized based on a range of data interaction,

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
	financial, regulatory and reputational considerations.
SP 800 53 Control with SP 800-161 Overlay **SA-4 (3)** Acquisition Process | Continuous Monitoring Plan for Controls CSF v1.1 Applicable Controls PR.IP-2: A System Development Life Cycle to manage systems is implemented. DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	In addition to facilitating automated, periodic internal control-based assessments, the Prevalent Platform also provides cyber security, business, reputational and financial monitoring – continually assessing third parties to identify potential weaknesses that can be exploited by cyber criminals. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.
SP 800 53 Control with SP 800-161 Overlay **SI-4 (1)** System Monitoring | Integrated Situational Awareness CSF v1.1 Applicable Controls DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.AE-3: Event data are collected and correlated from multiple sources and sensors. DE.AE-4: Impact of events is determined. DE.CM-1: The network is monitored to detect potential cybersecurity events. DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events. DE.DP-4: Event detection information is communicated. RS.CO-3: Information is shared consistent with response plans.	Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform 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 in a unified risk register that enables centralized risk triage and response. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

SP 800-53 r5 Control Number with SP 800-161r1 and CSF v1.1 Cross-Mapping	How Prevalent Helps
RS.AN-1: Notifications from detection systems are investigated.	
SP 800 53 Control with SP 800-161 Overlay **SI-5** Security Alerts, Advisories and Directives CSF v1.1 Applicable Controls ID.RA-1: Asset Vulnerabilities are identified and documented. ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources. ID.RA-3: Threats, both internal and external, are identified and documented. RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).	Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform 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 in a unified risk register that enables centralized risk triage and response. All risk intelligence in the Prevalent Platform is centralized, correlated and analyzed in a single risk register that automates reporting and response, and features a flexible weighted scoring model based on likelihood of an event and its impact.

The below table includes an extract of the new SP 800-53 Supply Chain Risk Management control and how the Prevalent Platform addresses each requirement. For a complete mapping, please download the NIST Compliance Checklist.

SP 800-53 r5 Supply Chain Risk Management (SR) Controls	How Prevalent Helps
SR-1 Policy and Procedures	Prevalent Program Design Services define and document your third-party risk management program. You get a clear plan that accounts for your specific needs while incorporating best practices for end-to-end TPRM.
SR-2 Supply Chain Risk Management Plan	Prevalent Program Optimization Services help you to continually improve your Prevalent Platform deployment, ensuring that your TPRM program maintains the flexibility and agility it needs to meet evolving business and regulatory requirements.
SR-3 Supply Chain Controls and Processes	Prevalent Program Design Services define and document your third-party risk management program. You get a clear plan that

SP 800-53 r5 Supply Chain Risk Management (SR) Controls	How Prevalent Helps
	accounts for your specific needs while incorporating best practices for end-to-end TPRM.
SR-5 Acquisition Strategies, Tools, and Methods	Prevalent helps procurement teams reduce cost, complexity and risk exposure during vendor selection. Our RFx Essentials solution provides centralized distribution, comparison, and management of RFPs and RFIs. It also helps you get ahead of potential supplier risks with demographic, 4th-party, and ESG scores – plus optional business, reputational, and financial risk insights. As a result, you're able to take an important first step toward tackling risk in the third-party lifecycle. Once supplier selection is complete, Prevalent Contract Essentials centralizes the distribution, discussion, retention, and review of vendor contracts. It also includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With Contract Essentials, procurement and legal teams have a single solution to manage vendor contracts, simplify management and review, and reduce cost and risk..
SR-6 Supplier Assessments and Reviews	The Prevalent Platform includes more than 100 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 and business resilience controls. Prevalent VTM continuously tracks and analyzes externally observable threats to vendors and other third parties. The service complements and validates vendor-reported security control data from the Prevalent Platform 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 in a unified risk register that enables centralized risk triage and response.
SR-8 Notification Agreements	With the Prevalent Platform, you can collaborate on documents, agreements and certifications, such as NDAs, SLAs, SOWs and contracts, with built-in version control, task assignment and auto-review cadences. You can also manage all documents throughout the vendor lifecycle in centralized vendor profiles.
SR-13 Supplier Inventory	Prevalent offers an inherent risk assessment questionnaire with clear scoring based on eight criteria to capture, track and quantify risks for all third parties. Assessment criteria include: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk)

SP 800-53 r5 Supply Chain Risk Management (SR) Controls	How Prevalent Helps
	• Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation Using the inherent risk assessment, you can automatically tier suppliers, set appropriate levels of further diligence, and determine the scope of subsequent, periodic assessments. Rule-based tiering logic enables suppliers to be categorized based on a range of data interaction, financial, regulatory and reputational considerations.

The below table includes a breakout of the supply chain-specific controls in the Cybersecurity Framework v1.1 and how Prevalent helps address each control. For a complete mapping, please download the NIST Compliance Checklist.

Cybersecurity Framework v1.1 Supply Chain Risk Management (SR) Controls	How Prevalent Helps
ID.SC-1: Identify, establish, assess, and manage cyber supply chain risk management processes, and ensure that organizational stakeholders agree.	Prevalent helps define and document your third-party risk management program with expert professional services. With our help you can build a clear plan that accounts for your specific needs while incorporating best practices for end-to-end TPRM.
ID.SC-2: Identify, prioritize, and assess suppliers and third-party partners of information systems, components, and services using a cyber supply chain risk assessment process.	Prevalent help onboard, profile, tier and score inherent risks across all third parties as a critical first step in the onboarding and prioritization stages of the vendor lifecycle.
ID.SC-3: Implement appropriate measures in supplier and third-party partner contracts to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	With Prevalent, you can use dedicated and custom contract assessment questionnaires to enable comprehensive reviews by identifying potential breaches of contract and other risks. Customizable surveys make it easy to gather and analyze necessary performance and contract data in a single risk register.
ID.SC-4: Routinely assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Prevalent delivers a comprehensive solution to address all information security topics as they pertain to supply chain partner security controls.
ID.SC-5: Conduct response and recovery planning and testing with suppliers and third-party providers.	Prevalent helps your team identify and mitigate the impact supply chain breaches by centrally managing vendors, conducting proactive event assessments, scoring identified risks, and accessing remediation guidance.

The Prevalent Difference

NIST requires robust management and tracking of third-party supply chain security risk. SP 800-53r5, SP 800-161r1 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, assess, and manage supply chain risk.

Prevalent can help by:

- Formalizing your third-party risk management program with industry best-practice guidance, adding consistency and repeatability to how you identify, manage, remediate, and monitor supply chain risks across the vendor lifecycle
- Reducing the cost and complexity of third-party risk management with a managed services team that can handle vendor onboarding, assessment, and management
- Comprehensively assessing vendors against NIST requirements and many other regulations, guidelines, and frameworks – as well through an extensive survey template library
- Continuously monitoring your third parties for cybersecurity, business, reputational, or financial risks that can impact their ability to deliver products and services
- Delivering the reporting required to demonstrate compliance inside and outside the organization
- Accelerating incident response by rapidly identifying and mitigating the impact of supply chain breaches through event collection, scoring identified risks, and accessing remediation guidance

National Institute of Standards and Technology

NIST SP 800-66r2

This chapter addresses NIST Special Publication 800-66r2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 was developed to help healthcare delivery organizations (HDOs) understand the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and provide a framework to support its implementation. The HIPAA Security Rule applies to any organization managing electronic protected health information (ePHI), whether they are a covered entity or a business associate (e.g., third-party vendor, supplier or partner). The rule requires organizations to:

- Ensure the confidentiality, integrity, and availability of all ePHI that they create, receive, maintain, or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against impermissible uses or disclosures of ePHI that are reasonably anticipated
- Ensure compliance by their workforce

NIST SP 800-66-r2 Third-Party Business Associate Risk Assessment Requirements

The HIPAA Security Rule includes provisions that require covered entities to conduct risk assessments, including:

1. Risk Analysis (R) – 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
2. Risk Management (R) – 163.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

The Security Rule goes on to recommend seven steps to include in a comprehensive risk assessment process. The table below maps Prevalent solution capabilities to each step, illustrating how a third-party risk management solution can help to address these best practices.

NOTE: This information is presented as summary guidance only. Organizations should review NIST 800-66r2 and HIPAA Security Rule requirements in full on their own in consultation with their auditors.

Health Insurance Portability and Accountability Act	
HIPAA Security Rule Implementation Guidance	
Recommended Steps	Tasks
1. Prepare for the Assessment	*Understand where ePHI is created, received, maintained, processed or transmitted.* *Define the scope of the assessment.*
How Prevalent Can Help Prevalent partners with you to build a comprehensive third-party risk management (TPRM) program based on proven best practices and extensive real-world experience. Our experts collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence, to termination and offboarding.	

Recommended Steps	Tasks
Prevalent can identify fourth-party and Nth-party subcontracting relationships by conducting a questionnaire-based assessment or by passively scanning the third party's public-facing infrastructure. The resulting relationship map depicts information paths and dependencies that could expose your environment to risk. Suppliers discovered through this process are continuously monitored for financial, ESG, cyber, business, and data breach risks, as well as for sanctions/PEP screening. Once third and fourth parties are identified, you can leverage the 125+ pre-defined assessment templates available in the Prevalent Platform to assess third-party business associates against NIST, HIPAA or other requirements.	
2. Identify Realistic Threats	*Identify the potential threat events and threat sources that are applicable to the regulated entity and its operating environment.*
How Prevalent Can Help Prevalent continuously tracks and analyzes external threats to 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. All monitoring data is correlated to assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting and response initiatives. Monitoring sources include: • 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 covering 550,000 companies • A database containing 10+ years of data breach history for thousands of companies around the world • 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 • A global network of 2 million businesses with 5 years of organizational changes and financial performance • 30,000 global news sources • A database containing over 1.8 million politically exposed person profiles • Global sanctions lists and 1,000+ global enforcement lists and court filings	
3. Identify Potential Vulnerabilities and Predisposing Conditions	*Use internal and external sources to identify potential vulnerabilities. Internal sources may include previous risk assessments, vulnerability scan and system security test results (e.g., penetration tests), and audit reports. External sources may include internet searches, vendor information, insurance data, and vulnerability databases.*
How Prevalent Can Help Prevalent normalizes, correlates and analyzes information across inside-out risk assessments and outside-in monitoring. This unified model provides context, quantification, management and	

Recommended Steps	Tasks
remediation support for risks. It also validates the presence and effectiveness of internal controls with external monitoring.	
4.-6. Determine the Likelihood (and Impact) of a Threat Exploiting a Vulnerability; Determine the Level of Risk	*Determine the likelihood (Very Low to Very High) of a threat successfully exploiting a vulnerability.* *Determine the impact (operational, individual, asset, etc.) that could occur to ePHI if a threat event exploits a vulnerability.* *Assess the level of risk (Low, Medium, High) to ePHI, considering the information gathered and determinations made during the previous steps.*
How Prevalent Can Help The Prevalent Platform enables you to define risk thresholds and categorize and score risks based on likelihood and impact. The resulting heat map enables teams to focus on the most important risks.	
7. Document the Risk Assessment Results	*Document the results of the risk assessment.*
How Prevalent Can Help With Prevalent, you can generate risk registers upon survey completion, integrating real-time cyber, business, reputational and financial monitoring insights to automate risk reviews, reporting and response. From the risk register, you can create tasks related to risks or other items; check task status via email rules linked to the platform; and leverage built-in remediation recommendations and guidance. The solution automates third-party risk management compliance auditing by collecting vendor risk information, quantifying risks, and generating reports for dozens of government regulations and industry frameworks, including NIST, HIPAA and many more.	

Mapping Prevalent Capabilities to NIST SP 800-66r2 HIPAA Security Rule Requirements

NIST SP 800-66r2 presents security measures that are relevant to each standard of the HIPAA Security Rule. The table below identifies specific business associate measures and maps Prevalent capabilities that help to satisfy the requirements.

NOTE: This information is presented as summary guidance only. Organizations should review NIST 800-66r2 and HIPAA Security Rule requirements in full on their own in consultation with their auditors.

Health Insurance Portability and Accountability Act	
HIPAA Security Rule Requirements	
Key Activity & Description	How Prevalent Helps
5.1.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1)) ***HIPAA Standard:*** *A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.*	
1. Identify Entities that are Business Associates Under the HIPAA Security Rule • Identify the individual or department who will be responsible for coordinating the execution of business associate agreements or other arrangements. • Reevaluate the list of business associates to determine who has access to ePHI in order to assess whether the list is complete and current. • Identify systems covered by the contract/agreement. • Business associates must have a BAA in place with each of their subcontractor business associates. Subcontractor business associates are also directly liable for their own Security Rule violations.	Prevalent identifies fourth-party relationships through a native identification assessment or by passively scanning the third party's public infrastructure. The resulting relationship map depicts information paths and dependencies that could open paths into an environment. Prevalent offers a pre-contract due diligence assessment with clear scoring based on eight criteria to capture, track and quantify inherent risks for all third parties and business associates during onboarding. Criteria includes: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation From this inherent risk assessment, your team can centrally manage all business associates; automatically tier suppliers; set appropriate levels of further diligence; and determine the scope of ongoing assessments.

Key Activity & Description	How Prevalent Helps
2. Establish a Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met • Maintain clear lines of communication between covered entities and business associates regarding the protection of ePHI as per the BAA or contract. • Establish criteria for measuring contract performance.	Prevalent helps to centrally measure third-party KPIs and KRIs to reduce risks from gaps in vendor oversight by automating contract and performance assessments. When a third party is found to be out of contract compliance, the Platform automates contract assessments and offboarding procedures to reduce your organization's risk of post-contract exposure.
3. Written Contract or Other Arrangement • Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a)… • Execute new or update existing agreements or arrangements as appropriate. • Identify roles and responsibilities. • Include security requirements in business associate contracts and agreements to address the confidentiality, integrity, and availability of ePHI. • Specify any training requirements associated with the contract/agreement or arrangement, if reasonable and appropriate.	Prevalent centralizes the distribution, discussion, retention, and review of vendor contracts. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. Key capabilities include: • Centralized tracking of all contracts and contract attributes such as type, key dates, value, reminders, and status – with customized, role-based views • Workflow capabilities (based on user or contract type) to automate the contract management lifecycle • Automated reminders and overdue notices to streamline contract reviews • Centralized contract discussion and comment tracking • Contract and document storage with role-based permissions and audit trails of all access • Version control tracking that supports offline contract and document edits • Role-based permissions that enable allocation of duties, access to contracts, and read/write/modify access With these capabilities, you can ensure that the right clauses – such as security protections over ePHI and training – are in the contract, and that they are enforceable and efficiently communicated to all stakeholders.

Key Activity & Description	How Prevalent Helps
5.4.1 Business Associate Contracts or Other Arrangements (§ 164.314(a)) ***HIPAA Standard:*** *(i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable. (ii) A covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3). (iii) The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.*	
1. Contract Must Provide that Business Associates Will Comply with the Applicable Requirements of the Security Rule Contracts between covered entities and business associates must provide that business associates will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the business associate creates, receives, maintains, or transmits on behalf of the covered entity.	Prevalent centralizes the distribution, discussion, retention, and review of vendor contracts. It also offers workflow capabilities to automate the contract lifecycle from onboarding to offboarding. With these capabilities, you can ensure that the right clauses – such as security controls enforcement, auditability, incident response, notifications, fourth-party subcontractor arrangements, etc. – are in the contract, and that they are enforceable and efficiently communicated to all stakeholders.
2. Contract Must Provide that the Business Associates Enter into Contracts with Subcontractors to Ensure the Protection of ePHI In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section.	
3. Contract Must Provide that Business Associates Will Report Security Incidents • Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI as required by § 164.410. • Maintain clear lines of communication between covered entities and business associates regarding the protection of ePHI as per the BAA or contract. • Establish a reporting mechanism and a process for the business associate to use in the event of a security incident or breach.	In addition to contract lifecycle management, Prevalent offers a Third-Party Incident Response Service that enables teams to rapidly identify and mitigate the impact of third-party breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance. Customers can also access a database containing 10+ years of data breach history for thousands of companies around the world. The database includes types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications. Combined with continuous cyber monitoring, it provides organizations with a comprehensive view of external information security risks that can impact operations.

Key Activity & Description	How Prevalent Helps
4. Other Arrangements The covered entity complies with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).	In addition to ensuring that business associate contracts contain provisions for assess fourth-party risks, Prevalent identifies fourth-party relationships through a native identification assessment or by passively scanning the third party's public infrastructure. The resulting relationship map depicts information paths and dependencies that could open paths into an environment.
5. Business Associate Contracts with Subcontractors The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	

The Prevalent Difference

Prevalent can help organizations apply the principles of NIST SP 800-66r2 to address HIPAA Security requirements for business associates. The Prevalent Third-Party Risk Management Platform:

- Delivers comprehensive pre-contract due diligence assessments to calculate the inherent risk that business associates bring to a relationship
- Simplifies contracting processes to ensure that all business associate key performance indicators (KPIs) and ePHI provisions are in place and tracked
- Profiles and tiers all third parties, right-sizing ongoing due diligence according to criticality
- Maps fourth parties to understand risk among subcontractors
- Adds workflow to automate the assessment, risk scoring and remediation process
- Continuously monitors business associates for cyber, business, reputational and financial risk, and correlates risks against assessment results and validate findings
- Automates incident response processes, speeding time to resolution
- Includes compliance and risk reporting by framework or regulation

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."[2]

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.

[2] 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.

System and Organization Control (SOC) 2

This chapter reviews the AICPA trust services criteria used in SOC 2 audits.

AICPA SOC 2 Summary

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) developed trust services criteria for organizations to use as a framework for demonstrating the confidentiality, integrity and availability of systems and data.

Organizations familiar with System and Organization Control (SOC) 2 audits will recognize that these trust services criteria are used to report on the effectiveness of their internal controls and safeguards over infrastructure, software, people, procedures, and data:

- **Security:** Protecting information and systems against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Availability:** Ensuring the availability of information and systems for operation and use to meet the entity's objectives.
- **Processing integrity:** Ensuring that system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality:** Protecting information designated as confidential to meet the entity's objectives.
- **Privacy:** Ensuring that personal information collected, used, retained, disclosed, and disposed meets the entity's objectives.

Organizations across multiple industries use SOC 2 reports to demonstrate due diligence to clients, differentiate themselves from competitors based on their security posture, or be proactive with auditors in measuring compliance against data protection regulations.

However, with 61 criteria across more than 300 points of focus, it can quickly become overwhelming for organizations standardizing on a SOC 2 report to understand how to evaluate third parties for control weaknesses that could result in a business disruption.

Meeting SOC 2 TPRM 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.

AICPA Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy	
Established by the Assurance Services Executive Committee (ASEC) of the AICPA for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems (a) across an entire entity; (b) at a subsidiary, division, or operating unit level; (c) within a function relevant to the entity's operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.	
Trust Services Criteria	How Prevalent Helps
CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
Communicates Objectives Related to Confidentiality and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.	The Prevalent Third-Party Risk Management (TPRM) Platform enables two-way dialogue about risks, reporting and remediations between organizations and their third-party vendors, suppliers and partners centrally in the system. In addition, the Platform enables reporting, policy documents, contracts and supporting evidence to be stored for dialogue, attestation and sharing. Together, these capabilities ensure that organizations have a single repository for visualizing and managing risks, vendor documentation and remediations.
Communicates Objectives Related to Privacy and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.	
CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	The Prevalent TPRM Platform enables organizations to automate the critical tasks required to assess, manage, continuously monitor and remediate third-party security, privacy, compliance, supply chain and procurement-related risks across every stage of the vendor lifecycle – from onboarding to offboarding. The solution includes the ability to issue and manage point-in-time risk assessments using more than 75 different templates, analyze the results, as well as continuously monitor third-party cyber, business, reputational, and financial risks for a holistic view of third parties. Built-in reporting templates ensure that security and risk management teams can communicate risk assessment results to executives and other decision-makers and stakeholders.

Trust Services Criteria	How Prevalent Helps
CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.	
Assesses Changes in Vendor and Business Partner Relationships — The risk identification process considers changes in vendor and business partner relationships.	The Prevalent Platform leverages customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more during offboarding to ensure that as agreements change, so do responsibilities. In addition, Prevalent offers Contract Essentials, a solution that centralizes the distribution, discussion, retention, and review of vendor contracts. It includes workflow capabilities to automate the contract lifecycle from onboarding to offboarding.
CC9.2: The entity assesses and manages risks associated with vendors and business partners.	
Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	Prevalent Contract Essentials helps vendor management, procurement and legal teams simplify the process of establishing and negotiating contract terms and SLAs, managing redlines, and securing approvals through workflow. The solution is fully integrated with the complete TPRM Platform ensuring that organizations can manage vendor contracts with the same discipline that they manage vendor risks.
Assesses Vendor and Business Partner Risks — The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.	The Prevalent Platform enables organizations to automate the critical tasks required to assess, manage, continuously monitor and remediate third-party security, privacy, compliance, supply chain and procurement-related risks across every stage of the vendor lifecycle – from onboarding to offboarding.
Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	With the Prevalent Platform, security and risk management teams can assign tasks related to managing assessments risks manually, or leverage a pre-packaged library of ActiveRules to automate a range of tasks normally performed as part of the assessment and review processes – such as updating vendor profiles and risk attributes, sending notifications, or activating workflow – utilizing if-this, then-that logic.
Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.	The Prevalent Platform enables vendor management teams to establish requirements to track and to centralize SLA and performance reporting against those requirements through a single reporting and analytics dashboard.

Trust Services Criteria	How Prevalent Helps
Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing issues identified with vendor and business partner relationships.	The Prevalent Platform features reporting that reveals risk trends, status and exceptions to common behavior for individual vendors or groups with embedded machine learning insights. With this capability, teams can quickly identify outliers across assessments, tasks, risks, etc. that could warrant further investigation.
Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.	The Prevalent Platform leverages customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more during offboarding.
Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.	The Prevalent Platform enables risk management and compliance teams to automatically map information gathered from controls-based vendor assessments to regulatory frameworks including ISO 27001, NIST, CMMC, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, SOX, NYDFS, and more to quickly visualize and address important compliance requirements.
Assesses Compliance with Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	
P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	
Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	Prevalent includes built-in assessments for data protection regulations such as GDPR, CCPA, HIPAA and NYDFS. Results from these assessments are mapped into a central risk register where security and risk management teams can visualize and take action on potential risks to data, and compare a vendor's actions against their contractual obligations.
Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The Prevalent Platform includes built-in remediation guidance and recommendations. Security and risk management teams can efficiently communicate with vendors and coordinate remediation efforts through the Platform, capture and audit conversations, and record estimated completion dates.

Trust Services Criteria	How Prevalent Helps
P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.	
Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The Prevalent Third-Party Incident Response Service enables security and risk management teams to rapidly identify and mitigate the impact of data privacy incidents by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
Reports Actual or Suspected Unauthorized Disclosures — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.	

The Prevalent Difference

The AICPA SOC 2 report is an industry-standard framework for IT services companies to assess their controls over customer data. Since some organizations that lack internal resources for responding to security assessments will provide a SOC 2 report to their customers instead, it can be time consuming and complex for teams to map SOC 2 report results into a risk management solution for proper risk tracking.

With Prevalent, you can address SOC 2 third-party risk management requirements by:

- Assessing third parties with a comprehensive SOC 2-based questionnaire
- Automatically generating a risk register upon survey completion to zero-in on potential areas of concern
- Creating an audit trail that maps documentation and evidence to risks and vendors
- Reporting against SOC 2 compliance

We also offer a SOC 2 Report Review Service, which is a managed service delivered by the Prevalent Risk Operations Center (ROC) that transposes SOC 2 report control exceptions into risks in the Prevalent Third-Party Risk Management Platform. The resulting unified risk register enables coordinated risk response and remediation following a standardized approach and ensures that you have a comprehensive profile of all vendors – even for those that submit a SOC 2 report in lieu of a full security assessment.

Shared Assessments Standard Information Gathering (SIG) Assessment

This chapter addresses the SIG Core and SIG Lite questionnaires.

SIG Summary

The Standard Information Gathering (SIG) questionnaire is an industry standard third-party risk assessment curated by Shared Assessments that measures risks across 18 domains. The SIG enables organizations to leverage a library of vetted questions mapped to controls and regulatory guidance in order to simplify and standardize third-party risk management and compliance.

There are two versions of the SIG:

- **SIG Core:** A detailed 825-question assessment meant to provide a deep understanding into how a third party secures information.
- **SIG Lite:** A simplified 150-question assessment that offers a basic level of assessment due diligence to be conducted preliminarily before a more detailed assessment is performed.

Using the SIG Questionnaire for Third-Party Risk Management Assurance

Prevalent leverages the SIG as standardized content in the Prevalent Exchange Network and Prevalent Legal Vendor Network, and includes both the SIG Core and SIG Lite assessments in the Prevalent Third-Party Risk Management Platform.

The Prevalent Difference

The SIG provides a robust assessment for tracking and remediating third-party risk. Prevalent can help simplify the use of the SIG by:

- Automating the collection and analysis of SIG questionnaire answers and supporting evidence in a single platform.
- Further simplifying regulatory and security framework reporting with additional built-in control mappings.
- Improving visibility into vendor risks with machine learning analytics and reporting.
- Validating SIG findings with continuous cyber, business, reputational and financial insights.
- Reducing risk by centralizing risk remediation guidance.

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.

Conclusion

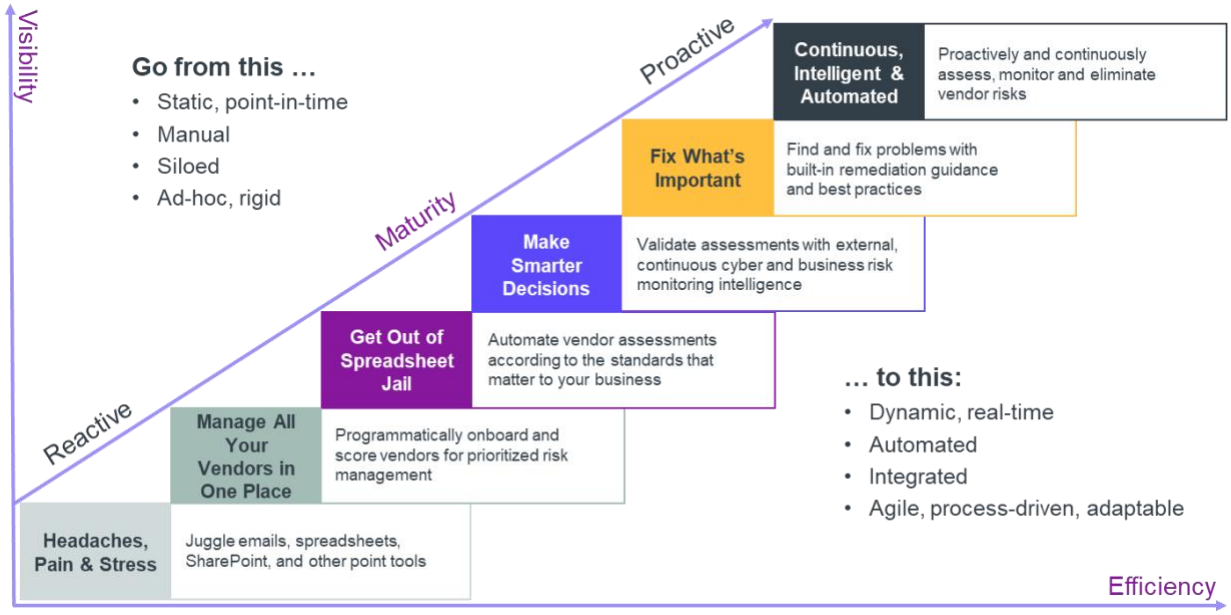
Regulatory compliance is an important driver of third-party risk management program design and implementation. While regulatory guidance varies slightly across governing authorities and standards bodies, all agree that conducting a risk assessment, with proper due diligence before and during the lifecycle 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 and suppliers throughout the third-party lifecycle. 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.