Prevalent™

The Third-Party Risk Management Compliance Handbook

Part I: Regulatory Requirements

An Important Note to Readers

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

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

Table of Contents

Executive Summary

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

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

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

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

Complying with TPRM Regulations, Guidelines and Standards

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

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

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

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

Summary Tables

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

Part I: Government Regulations (this document)

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

Part II: Industry Guidelines and Standards

Download Part II here.

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

How Prevalent Solutions Address Third-Party Compliance Requirements

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

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

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

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 was signed into law on June 28, 2018. The law aims to enhance privacy rights and consumer protection by regulating businesses' collection and sale of consumer data. The law establishes the rights of both the California Attorney General and private California residents to take legal action against businesses if they fail to comply.

While the CCPA is technically California state law, its reach will be felt far beyond the borders of that state. This outsized impact is due to the nature of the law itself; CCPA oversight is not limited to businesses headquartered in California, or even to businesses physically operating in California—the CCPA applies to consumer data collected from any resident of California. Given the fact that California is home to about 40 million people and would be the 5th largest economy in the world if it was its own country, the odds are good that if a business is collecting consumer data, they have collected the data of a California resident.

Due to the fluid nature of state residency in the United States, and the massive undertaking involved in tracking the residency of each and every consumer from whom data is collected, some firms are making the decision to treat every consumer as if they were a California resident, and are therefore preparing for blanket CCPA compliance across their businesses. But while these internal preparations are important, ensuring a business's compliance is not enough—organizations must ensure that their relationships with third parties fall in line with the CCPA.

Meeting CCPA Requirements

Not only does the CCPA regulate the scope and storage of consumer data by a business, it also sets restrictions on a business's ability to sell that data to third parties.

Section 1798.140(w) of the law defines third parties in the negative, as any party that is not the business, an individual contractually allowed to use the data, or a service provider (as defined by the CCPA). Some notable CCPA regulations on third parties include:

- **1798.115(d) –** "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to 1798.120."
- **1798.120(a) –** "A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out."
- **1798.120(b) –** "A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the right to opt out of the sale of their personal information."

The obligation for a business to provide explicit notice of sales and give consumers a chance to opt out, coupled with the restrictions on third parties to resell that info without doing the same, only emphasizes the need for a business to be able to identify which of their third parties are currently buying or utilizing consumers' data. Only once a business has identified the third parties to which they sell consumer data can they begin to take steps to ensure CCPA compliance, such as updating legal agreements with the third party or opening channels of communication in case of a breach.

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)	
Enhancing privacy rights and consumer protection by regulating businesses' collection and sale of consumer data.	
Best Practice	How Prevalent Helps
Discovery & Data Mapping	Prevalent supports scheduled assessments to identify data flows between relationships, identifying where data exists, where it flows, and who it is shared with outside the organization using a unique relationship mapping capability. Automatically generates a risk register highlighting key risk areas to bring visibility into data.
Self-Assessments	Prevalent conducts a Privacy Impact Assessment (PIA) targeted on the most sensitive business and privacy-related data and business processes with the highest risk. Evaluates the origin, nature and severity of the potential risk, and provides recommendations to mitigate identified risks ensuring future compliance with privacy regulations.
Vendor Risk Assessments	Prevalent assesses vendor data privacy controls against CCPA using the Prevalent Compliance Framework (PCF) and a dedicated CCPA survey. Specific questionnaire content helps to identify, and map risks identified during the assessment to controls for a clear view of potential hot spots.
Risk Response	Prevalent automates risk identification based on thresholds set in the platform. Accelerates response with pre-built workflow rules that escalate identified risks to the proper stakeholder for immediate review and disposition.
Compliance Tracking & Reporting	Prevalent reports against CCPA using the Prevalent Compliance Framework that automatically maps risks and responses to controls, provides a percent-compliant rating, and delivers stakeholder-specific reporting to bring visibility to data security.
Subject Access Requests	Prevalent enables vendors and business users to trigger subject access request (SAR) workflows based on requests they receive, using a proactive assessment to capture the relevant data. Leveraging the relationship map, risk and privacy teams can visualize who data is shared with and who is exposed to that vendor's data.

Best Practice	How Prevalent Helps
Contract Reviews	Prevalent provides a dedicated contract assessment in the platform, with the results available in a contracts risk register to raise risks related to the achievement of contract clauses. Having the capability to visualize breaches of certain contract requirements or clauses ensures that organizations have the insights they need when renewing contracts.

The Prevalent Difference

A growing number of damaging global data breaches involving personal data has resulted in increased regulatory activity to drive organizational accountability over data. As part of assessing their cybersecurity posture, organizations must be able to assess their readiness for compliance with privacy regulations and continuously improve their programs, but standard vendor risk management products lack the specific guidance required. Prevalent unifies security and privacy teams seeking to assess their vendors' and partners' compliance with privacy regulations through a single platform for all types of assessments. Specific to CCPA, Prevalent:

- Identifies internally and in the supply chain where data resides with unique data and relationship mapping capabilities.
- Assesses the potential exposure to a breach – inside and outside the organization – by integrating the results of internal controls-based assessments with external monitoring of vendor networks.
- Reports on readiness, compliance, and remediations using specific CCPA content – mapping the results to measure compliance.
- Integrates with a broader solution for vendor risk management to ensure all facets of risk – cyber, business, privacy, financial – are centrally managed.

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.	
Best Practice	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

Best Practice	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 asses 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.	
GDPR 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

GDPR is a set of laws designed to give EU citizens more control over their personal data and increase the obligations of organizations to deal with that data in transparent and secure ways. In fact, all organizations who collect, store, process, or transfer personal data of EU citizens must comply with this regulation. These data protection obligations extend not only to organizations operating within the EU, but also to any companies outside of the EU that offer goods or services to EU residents.

Under GDPR, regulatory authorities have greater power to act against companies that break this law, with fines totalling up to 4% of annual global revenue or 20 million euros, whichever is greater.

To be compliant with GDPR, organizations must take necessary steps to protect citizens' data in their care, including data that is shared with third parties. Because many data breaches occur through third-party relationships, GDPR clearly states that third parties (known as data processors) must handle data privacy and security in a way that is compliant to the regulation. In fact, under this legislation, they are legally obligated to comply with all aspects of the regulation to ensure consistency and true protection for customers.

Organizations should perform due diligence initiatives on a regular basis to ensure their third parties are actively engaged with GDPR requirements. Processes should include:

- Data privacy risk assessments for all third parties that have access to personal data
- Continuous monitoring of critical third parties
- Documented evidence to demonstrate compliance
- Audit trail capabilities

GDPR is far-reaching and impacts all industries. Organizations should take proactive measures and upgrade their third-party risk frameworks as per GDPR compliance to mitigate data privacy risk.

Meeting GDPR Requirements

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 28: Processor **Paragraph 1** "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 organizational 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."	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 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 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 lay out the requirements for a data protection impact assessment along with continuous monitoring of critical data processors (third parties). 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 CISOs 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.
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 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.

GDPR Requirements	How Prevalent Helps
Article 28: Processor **Paragraph 3** "Takes all measures required pursuant to Article 32"	See below
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: (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures** for ensuring the security of the processing.	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 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.

The Prevalent Difference

Maintaining GDPR compliance takes time and vigilance, especially when it comes to managing the relationship between organizations (data controllers) and their third parties (data processors). The regulation states that a policy for managing data privacy should be in place and contractually agreed upon by the controller and processor. Data processors should be assessed to comply with necessary GDPR privacy focused operational processes to ensure they have required processes in place.

Prevalent offers a GDPR questionnaire to determine third-party adherence across all GDPR components. The survey gathers information and documentation on all the data management and privacy operational processes a data processor needs to have in place for GDPR, based on the type of EU data they access. All answers can then be analyzed within the Prevalent platform to determine a third party's level of adherence for GDPR; identify any necessary action items; and track remediation efforts.

The Prevalent platform also includes a Data Mapping Assessment survey that identifies where data regulated by GDPR exists within an organization – both internally and with third-party vendors. It provides a clear picture of what the data is; how it comes into the organization; how it is used and stored; and who it is shared with outside the organization. With the platform's unique relationship management capabilities, organizations can create, query, and view data inventories and processing records. Combined with Prevalent's vendor assessment functionality, this delivers a comprehensive, internal and external view of compliance and related processes.

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 mitigate 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 Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996, but over the past two decades its scope has grown considerably in the form of legislative updates and enforcement actions. In its broadest terms, the purpose of HIPAA is to improve efficiency in the healthcare industry; to improve the portability of health insurance; to protect the privacy of patients and health plan members; and to ensure health information is kept secure and patients are notified of breaches of their health data.

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).

It states that the ePHI that an organization (known as a covered entity) creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. The HIPAA Security Rule sets forth general rules around security standards, including administrative, technical, and physical safeguards. Organizational requirements and documented policies and procedures round out the legislative specifications.

In its most basic form, the assessment, analysis, and management of risk provides the foundation of a covered entity's HIPAA Security Rule compliance efforts. This includes a heightened awareness to the risk posed by vendors.

The relationship and responsibilities between covered entities and their vendors is critically important. A covered entity contemplating a relationship with a vendor must create a contract, or Business Associate Agreement, that speaks to privacy and security assurances. **Evaluating a vendor's readiness to comply with the covered entity's security expectations is achieved through a vendor risk assessment.** The results of the assessment enable covered entities to identify appropriate security controls for reducing risk to the organization and its data and information systems.

With the enforcement of the HIPAA Omnibus Rule, business associates of covered entities are directly liable for compliance with certain requirements of the HIPAA Privacy and Security Rules.

Meeting HIPAA Security Rule Requirements

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."	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. 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, analyzed, and escalated to the proper channels.
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."	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.

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."	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, 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."	The Prevalent Assessment service simplifies compliance and reduces risk with automated collection, analysis, and remediation of vendor surveys using industry standard and custom surveys.
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.	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.

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.

Prevalent's Third-Party Risk Management solution can help covered entities meet this requirement by providing a complete framework for assessing the risk posed by business associates and other third-party vendors using HIPAA Privacy Rule and Security Rule-specific surveys. Our Assessment service enables covered entities to perform vendor risk assessments, including workflow and remediation management to mitigate and manage risks.

Vendor tiering enables business associates to be managed according to the risk they present with different assessments, frequencies, and scoring as warranted. Customizable surveys with documented evidence enable 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.

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	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.

• Physical devices and systems within the organization are inventoried • Supplier location of data centers (U.S./Canada-based vs international)	

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 2017-21 – Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29	
Bulletin 2013-29 Questions	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"	

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 Questions	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.

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.	
Best Practice	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.

Best Practice	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.	
Best Practice	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.

Best Practice	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 asses 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.	
Best Practice	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.

Best Practice	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 asses 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) requirement for all DoD contractors to achieve CMMC certification starting in October 2020.

CMMC Summary

On January 31, 2020, the Office of the Under Secretary of Defense for Acquisition and Sustainment in the United States Department of Defense (DoD) released v1.0 of the Cybersecurity Maturity Model Certification (CMMC). Developed to serve as a single cybersecurity standard for all future DoD acquisitions, CMMC requires that each of the more than 300,000 DoD contractors become CMMC certified beginning in October 2020, with a five-year phase-in and renewals every three years after that.

CMMC requires companies achieve third-party certification against cybersecurity and information 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 contractors must be certified in one of five levels, from Level 1 (lowest, Basic Cyber Hygiene) to Level 5 (highest, Advanced/Progressive) based on the Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for controlled unclassified information (CUI) from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204.7012. General information regarding the certification levels includes:

- **Level 1** – Applies to 285,000 DoD contractors and requires that the company report against 17 no-cost controls which are based on good business practices and standard cyber hygiene.
- **Level 2** – Transitional level for organizations with the resources to reach for Level 3.
- **Level 3** – Applies to contractors that are approved to touch controlled unclassified information (CUI) and requires those companies by law to demonstrate certification against all 110 controls in NIST 171.
- **Level 4** and **Level 5** apply to a very small percentage of all DoD suppliers.

Although certified auditors (C3PAOs) must assess DoD contractors in order to demonstrate compliance with their target level of certification, companies that are doing, or wish to do, business with the US federal government can assess themselves against the requirements as well.

Meeting CMMC Requirements

Please see the table below for a summary of the 17 CMMC requirements by domain and level. The Prevalent Third-Party Risk Management Platform has built-in questionnaires for each level, enabling C3PAOs to assess all DoD contractors, and contractors to assess themselves – especially for Level 1 compliance.

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

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

Federal Acquisition Regulation (FAR) Clause 52.204-21
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171
Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204.7012

Domain	Capability	Practice Number by Level of Certification				
		Level 1	Level 2	Level 3	Level 4	Level 5
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes	1.001 1.002 1.003 1.004	2.005 2.006 2.007 2.008 2.009 2.010 2.011 2.013 2.015 2.016	3.017 3.018 3.019 3.012 3.020 3.014 3.021 3.022	4.023 4.025 4.032	5.024
Asset Management (AM)	• Identify and document assets • Manage asset inventory			3.036	4.226	
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs		2.041 2.042 2.043 2.044	3.045 3.046 3.048 3.049 3.050 3.051 3.052	4.053 4.054	5.055
Awareness and Training (AT)	• Conduct security awareness training • Conduct training		2.056 2.057	3.058	4.059 4.060	
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management		2.061 2.062 2.063 2.064 2.065 2.066	3.067 3.068 3.069	4.073	5.074
Identification and Authentication (IA)	• Grant access to authenticated entities	1.076 1.077	2.078 2.079 2.080 2.081 2.082	3.083 3.084 3.085 3.086		

Domain	Capability	Practice Number by Level of Certification				
		Level 1	Level 2	Level 3	Level 4	Level 5
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared event • Perform post incident reviews • Test incident response		2.092 2.093 2.094 2.096 2.097	3.098 3.099	4.100 4.101	5.106 5.102 5.108 5.110
Maintenance (MA)	• Manage maintenance		2.111 2.112 2.113 2.114	3.115 3.116		
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport	1.118	2.119 2.120 2.121	3.122 3.123 3.124 3.125		
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions		2.127 2.128			
Physical Protection (PE)	• Limit physical access	1.131 1.132 1.133 1.134	2.135	3.136		
Recovery (RE)	• Manage backups • Manage information security continuity		2.137 2.138	3.139		5.140
Risk Management (RM)	• Identify and evaluate risk • Manage risk • Manage supply chain risk		2.141 2.142 2.143	3.144 3.146 3.147	4.149 4.150 4.151 4.148	5.152 5.155
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews		2.157 2.158 2.159	3.161 3.162	4.163 4.164 4.227	

Domain	Capability	Practice Number by Level of Certification				
		Level 1	Level 2	Level 3	Level 4	Level 5
Situational Awareness (SA)	• Implement threat monitoring			3.169	4.171 4.173	
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries	1.175 1.176	2.178 2.179	3.177 3.180 3.181 3.182 3.183 3.184 3.185 3.186 3.187 3.188 3.189 3.190 3.191 3.192 3.193	4.197 4.228 4.199 4.202 4.229	5.198 5.230 5.208
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections	1.210 1.211 1.212 1.213	2.214 2.216 2.217	3.218 3.219 3.220	4.221	5.222 5.223

The Prevalent Difference

CMMC certified auditors can leverage the Prevalent Third-Party Risk Management Platform with built-in questionnaires to assess all five levels of CMMC certification. With this access, certified auditors can:

- Invite clients into the Prevalent platform to complete their standardized control assessment in an easy-to-use, secure tenant
- Automate chasing reminders to 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 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 contractor can conduct a Level 1 pre-assessment prior to the formal audit to:

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

Conclusion

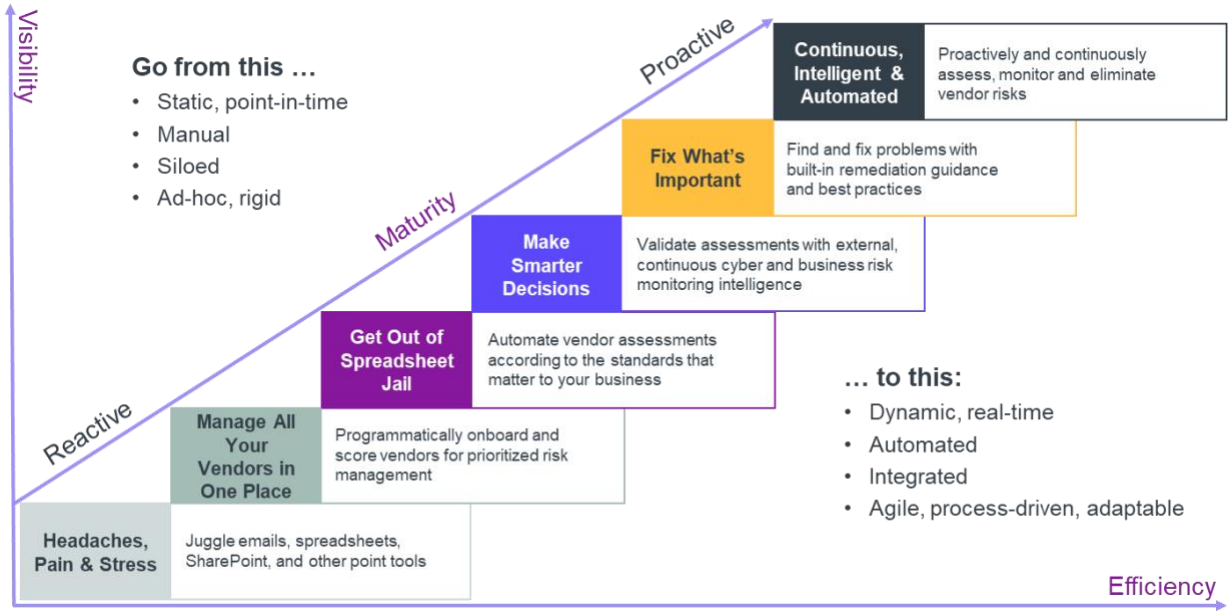
Regulatory compliance is an important driver of third-party risk management program design and implementation. While regulatory guidance varies slightly across governing authorities and standards bodies, all agree that conducting a risk assessment, with proper due diligence before and during the lifecycle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

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

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

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

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



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

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

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

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

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

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

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

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

About Prevalent

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

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

© Prevalent, Inc. All rights reserved. The Prevalent name and logo are trademarks or registered trademarks of Prevalent, Inc. All other trademarks are the property of their respective owners. 07/21