Prevalent™

White Paper:

Achieving Compliance with Third-Party Risk Management Regulatory and Framework Requirements with the Prevalent TPRM Platform

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

An Important Note to Readers **2**

Executive Summary **5**

Adherence to Compliance Requirements and Guidelines 5

Summary Table 5

How Prevalent Solutions Address Third-Party Compliance Requirements 6

New York State Department of Financial Services (DFS) NY CRR 500 ..... **7**

23 NY CRR 500 Summary 7

Meeting 23 NY CRR 500 Third-Party Risk Management Compliance Requirements 8

The Prevalent Difference 10

Office of the Comptroller of the Currency (OCC) Bulletins **11**

OCC 2013-29 / 2017-07 / 2017-21 Summary 11

Meeting OCC Third-Party Risk Management Compliance Requirements 11

The Prevalent Difference 15

Financial Conduct Authority (FCA) FG 16/5 Guidance **16**

FCA FG 16/5 Summary 16

Meeting FCA FG 16/5 Guidance 16

The Prevalent Difference 18

General Data Protection Regulation (GDPR) **20**

GDPR Summary 20

Meeting GDPR Requirements 20

The Prevalent Difference 22

European Banking Authority (EBA) Guidelines on Outsourcing Arrangements **23**

EBA Guidelines on Outsourcing Arrangement Summary 23

Meeting EBA Outsourcing Guidelines 24

The Prevalent Difference 28

Health Insurance Portability and Accountability Act (HIPAA) **29**

HIPAA Summary 29

Meeting HIPAA Security Rule Requirements....29
The Prevalent Difference....32
Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook....33
FFIEC IT Examination Handbook Summary....33
Meeting FFIEC IT Examination Handbook Guidance for Third-Party Risk Management....33
The Prevalent Difference....36
International Organization for Standardization (ISO) Information Security Standards....38
ISO 27001 / 27002 / 27018 Summary....38
Meeting ISO 27001 / 27002 / 27018 Third-Party Risk Management Standards....38
The Prevalent Difference....41
NIST SP 800-53r4 and NIST CSF v1.1 Standards and Frameworks....42
NIST SP 800-53r4 and NIST CSF v1.1 Summary....42
Meeting NIST SP 800-53r4 and NIST CSF v1.1 Standards and Frameworks....43
The Prevalent Difference....45
Conclusion....46
A Path to Maturing and Optimizing Your Third-Party Risk Management Program....46
About Prevalent....48

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 and security.

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, 61% of U.S. companies said they experienced a data breach caused by one of their vendors or third parties.

In the face of growing threats, regulators 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 regulatory compliance and deepen IT security controls.

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.

Adherence to Compliance Requirements and Guidelines

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. 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 and standards, 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
4. Monitor third parties to verify compliance

*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 and data privacy requirements, 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 Table

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.

Authority	Regulation & Guideline / Industry Standard & Framework	Assessment Required	Monitoring Required
Regulations			
NY DFS	**23 NYCRR 500**	✓	✓
OCC	Bulletin 2013-29	✓	✓
	Bulletin 2017-21	✓	✓
FCA	FG 16/5	✓	✓
EU	GDPR	✓	⊘
EBA	Guidelines on Outsourcing Arrangements	✓	✓
HHS	HIPAA Security Rule	✓	⊘
Guidelines			
FFIEC	**BCP Booklet: Appendix J**	✓	✓
	Information Security Booklet	✓	⊘
Industry Standards			
ISO	**27001:2013**	✓	✓
	27002:2013	✓	✓
	27018:2019(E)	✓	✓
NIST	SP 800-53R4	✓	⊘
	CSF 1.1	✓	✓

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 50+ 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 & risk status across the vendor landscape
- Deep data security auditing and business monitoring capabilities that allow 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.

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.

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 fulfill 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.

Office of the Comptroller of the Currency (OCC) Bulletins

This chapter of the whitepaper 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

Bulletin 2013-29 Requirements	How Prevalent Helps
Due Diligence and Third-Party Selection: "A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.	The Prevalent Assessment service offers security, privacy, and risk management professionals an automated platform to manage the vendor risk assessment process and determine vendor compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live reporting, and an easy-to-use dashboard for efficiency. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels.
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"	
Ongoing Monitoring: "Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk	The Prevalent Cyber & Business Monitoring service provides both snapshot and continuous vendor monitoring for immediate notification of

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”	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 allow 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 fulfill 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.

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.
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.

General Data Protection Regulation (GDPR)

This chapter of the whitepaper 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 totaling 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 readiness 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 readiness 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.

European Banking Authority (EBA) Guidelines on Outsourcing Arrangements

This chapter of the whitepaper 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 become 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.

These requirements represent a full set of controls implemented across the outsourcer organization and are well beyond the scope of a simple automated scan of external-facing infrastructure.

Prevalent's Third-Party Risk Management solution provides a complete framework for implementing management, auditing, and reporting related to third-party supplier risk.

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.

Workflows ensure assessments are managed to completion and re-assessments are automatically kicked off when required. The completed questionnaires and documentary evidence are easily managed, maintained and reported when needed internally or for examiners.

Risk scoring and analytics raise important risks that need to be addressed to the attention of those responsible for managing processors.

Reporting provides the compliance information necessary in multiple forms as required for different levels of the organization.

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. 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.

Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook

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

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

FFIEC IT Examination Handbook Summary

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

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

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

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

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

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

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

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

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

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

The Prevalent Difference

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

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

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

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

- Identifying factors contributing to and determining the institution's overall cyber risk
- Assessing the institution's cybersecurity preparedness
- Evaluating whether the institution's cybersecurity preparedness is aligned with its inherent risks

- Determining risk management practices and controls that are needed or require enhancement and actions to be taken to achieve the desired state
- Informing risk management strategies

International Organization for Standardization (ISO) Information Security Standards

This chapter of the whitepaper addresses the following ISO standards:

- ISO 27001:2013: Information security management systems (ISMS) - Requirements
- ISO 27002:2013: Code of practice for information security controls
- ISO 27018:2019(E): Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO 27001 / 27002 / 27018 Summary

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

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

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

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

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

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

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

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

ISO 27001:2013: Information Security Management Systems (ISMS) - Requirements ISO 27002:2013: Code of Practice for Information Security Controls	
These standards set requirements for establishing, implementing, maintaining and continually improving an information security management system.	
ISO 27001 / 27002 Requirements	How Prevalent Helps
15.1 Information security in supplier relationships "Objective: To ensure protection of the organization's assets that are accessible by suppliers."	The Prevalent Assessment service offers security, privacy, and risk management professionals an automated platform to manage the supplier risk assessment process and determine third-party compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live reporting, and an easy-to-use dashboard. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels.
15.1.1 Information security policy for supplier relationships "Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented."	The Prevalent Third-Party Risk Management platform provides a complete solution for performing assessments and an environment to include and manage documented due-diligence evidence.
15.1.2 Addressing security in supplier agreements "All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information."	The Prevalent Assessment solution ensures suppliers implement the exact, agreed upon requirements with regular tracking and verification.
15.1.2 (d) "obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;"	The Prevalent solution enables internal control-based assessments (based on industry standard framework questionnaires and/or custom questionnaires). The platform includes built-in workflow capability enabling assessors to interact efficiently with third parties during the due diligence collection and review periods. Robust reporting and audit capabilities give each level of management the information it needs to properly review the third party's performance.

ISO 27001 / 27002 Requirements	How Prevalent Helps
15.1.2 (m) "right to audit the supplier processes and controls related to the agreement;"	The Prevalent Assessment solution provides a simple, trackable, repeatable mechanism to perform controls audits.
15.1.2 (n) "defect resolution and conflict resolution processes;"	Bi-directional workflow in the Prevalent Assessment platform includes built-in discussion tools to enable communication with suppliers on remediating issues.
15.1.2 (p) "supplier's obligations to comply with the organization's security requirements."	The Prevalent Assessment solution ensures suppliers implement the exact, agreed-upon requirements with regular tracking and verification.
15.1.3 Information and communication technology supply chain "Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain."	Prevalent's TPRM platform provides a complete set of internal and external assessment and monitoring services to ensure a full view of a supplier's information, communications and product supply chain security posture.
15.1.3 (d) "implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;"	The Prevalent solution includes a mechanism to perform reviews; monitor compliance with agreed policies; and audit and generate regular reports for all levels of management.
15.2 Supplier service delivery management **15.2.1 Monitoring and review of supplier services** "Organizations should regularly monitor, review and audit supplier service delivery. Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly."	The Prevalent TPRM Platform unifies internal control-based assessments (based on industry standard framework questionnaires and/or custom questionnaires) with continuous vendor threat monitoring to deliver a holistic security risk rating, enabling organizations to zero-in on the most important or impactful risks. The platform includes built-in workflow capability enabling assessors to interact efficiently with third parties during the due diligence collection and review periods.

ISO 27001 / 27002 Requirements	How Prevalent Helps
15.2.1 (c) "conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;"	The Prevalent platform provides a simple, trackable, repeatable mechanism to perform audits along with a workflow and shared communication mechanism to track issues to resolution.
15.2.1 (g) "review information security aspects of the supplier's relationships with its own suppliers;"	The Prevalent solution provides a detailed map to visualize all relationships for each entity and other business entities (e.g., vendors / departments / datasets). This capability enables organizations to monitor the relationships between third, fourth, and Nth parties.

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

The Prevalent Difference

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

- A policy for managing risk should be in place;
- A policy should be codified in supplier agreements; and
- Suppliers should be managed and audited to the agreed requirements.

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

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

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

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

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

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

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

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

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

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

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

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

The NIST Cybersecurity Framework v1.1 document is divided into the framework core, the implementation tiers, and the framework profile. The framework core describes five functions of an

information security program: **identify**, **protect**, **detect**, **respond**, and **recover**. For organizations looking to establish or improve a cybersecurity program, this framework follows similar steps to that of NIST SP 800-53r4. Section 3.3, Communicating Cybersecurity Requirements with Stakeholders, explains how to use the framework to manage supply chain risk. Activities include:

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

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

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

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

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

NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1	
The NIST guidance provides high-level guidance for improving cybersecurity defenses.	
NIST CSF v1.1 Guidelines	How Prevalent Helps
Supply Chain Risk Management (ID.SC) **ID.SC-2:** Suppliers and third-party partners of information systems, components, and services are **identified, prioritized, and assessed using a cyber supply chain risk assessment process.**	Prevalent offers security, privacy, and risk management professionals an automated platform to manage the vendor risk assessment process and determine vendor compliance with IT security, regulatory, and data privacy requirements. It employs both standard and custom questionnaires to help collect evidence and provides bi-directional remediation workflows, live

	reporting, and an easy-to-use dashboard for efficiency. With clear reporting and remediation guidance, the platform ensures that risks are identified and escalated to the proper channels. In addition to facilitating automated, periodic internal control-based assessments, the platform also provides cyber security and business monitoring – continually assessing the third-party networks to identify potential weaknesses that can be exploited by cyber criminals. Prevalent also offers penetration testing as-a-service to help customers investigate vendor network operations at a much more granular level. With the integration of internal assessments, external cyber monitoring and penetration testing, organizations gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.
Supply Chain Risk Management (ID.SC) **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	The Prevalent Assessment solution can implement customized questionnaires that verify the vendor is meeting the detailed requirements of the contract.
Supply Chain Risk Management (ID.SC) **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	The Prevalent Third-Party Risk Management platform includes effective reporting to satisfy audit and compliance requirements as well as to present findings to the board and senior management. The entire risk profile can be viewed in the centralized live reporting console, and reports can be downloaded and exported to determine compliance status. Deep reporting capabilities include filters and click-through interactive charts. The solution includes a complete repository of all documentation collected and reviewed during the diligence process.
NIST CSF v1.1 Guidelines	How Prevalent Helps
Supply Chain Risk Management (ID.SC) **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers.	In addition to facilitating automated, periodic internal control-based assessments, the platform also provides cyber security and business monitoring – continually assessing the third-party networks to identify potential weaknesses that can be exploited by cyber criminals. Prevalent also offers penetration testing as-a-service to help customers investigate vendor network operations at a much more granular level. With the integration of internal assessments, external cyber monitoring and penetration testing, organizations gain a complete view of vendor risks plus clear and actionable remediation guidance to address those risks.

The Prevalent Difference

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

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

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

Conclusion

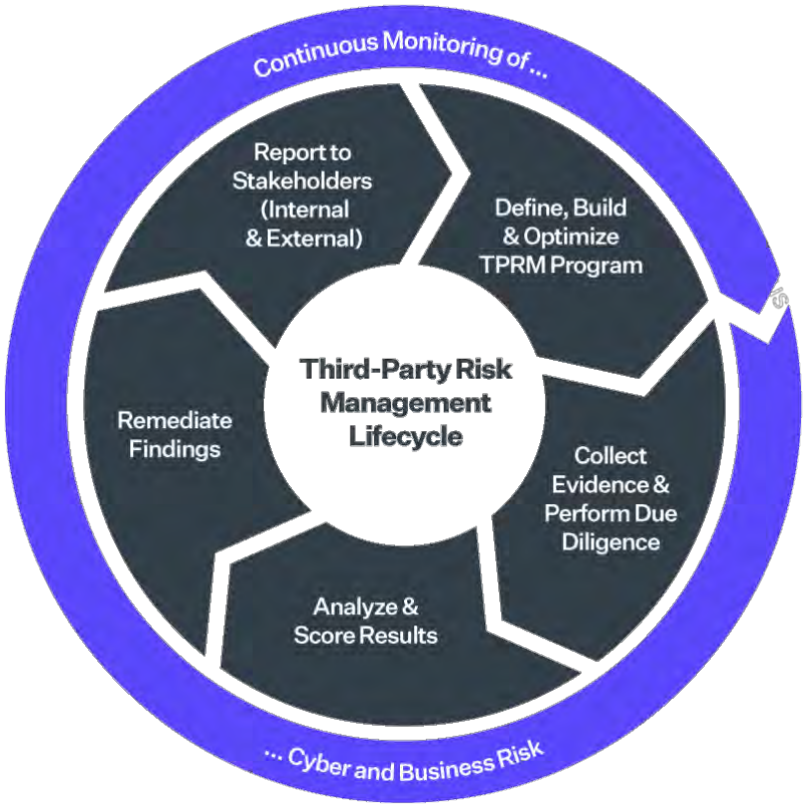
Regulatory compliance is an important driver of third-party risk management program design and implementation. While regulatory guidance varies slightly across governing authorities and standards bodies, all agree that conducting a risk assessment, with proper due diligence before and during the lifecycle 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, six-step process ensures greater TPRM visibility, efficiency and scale.

Key steps include:

1) Define and build a new program, or optimize your existing program, with expert advisory, maturity and assessment services. This step ensures you are assessing the right vendors according to criticality to the business and defines the right content to collect from the vendors based on regulatory framework or industry standard.

2) As you are defining, building, or optimizing your program, begin conducting continuous cyber and business monitoring of select vendors. This provides insights into potential vendor risks and can inform prioritization and risk awareness.

3) Choose between a Prevalent library of pre-defined assessments or the flexibility to build-your-own custom surveys. Prevalent offers advisory services to help decide which is right for your organization – with fully automated workflow for closed-loop vendor risk resolution.

4) To optimize analysis and scoring, set the importance of risk types to reflect the nature of the service provided and assessed. This ensures better visibility to prioritize remediation and a better, more complete score.

5) Map answers to control frameworks to measure compliance, and project future risks based on in-process remediations. Tie risks to business outcomes and provide prescriptive remediation recommendations to reduce risk.

6) Visualize compliance and risk status across the vendor landscape with assessor and executive-specific views.

Having strong policies in place as well as measuring and continuously monitoring risk associated with being out of compliance is part of the required Third-Party risk management lifecycle associated with most regulatory bodies. With Prevalent, you gain a 360-degree view of vendors – from the inside out and the outside in – to help manage regulatory compliance and align to industry standards and guidelines.

About Prevalent

Prevalent helps enterprises manage risk in third-party business relationships. It is the industry's only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly functioning, effective third-party risk program.

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