TOP THIRD-PARTY RISK MANAGEMENT **TERMS TO KNOW**

A Glossary of Terminology for Third-Party Risk Management

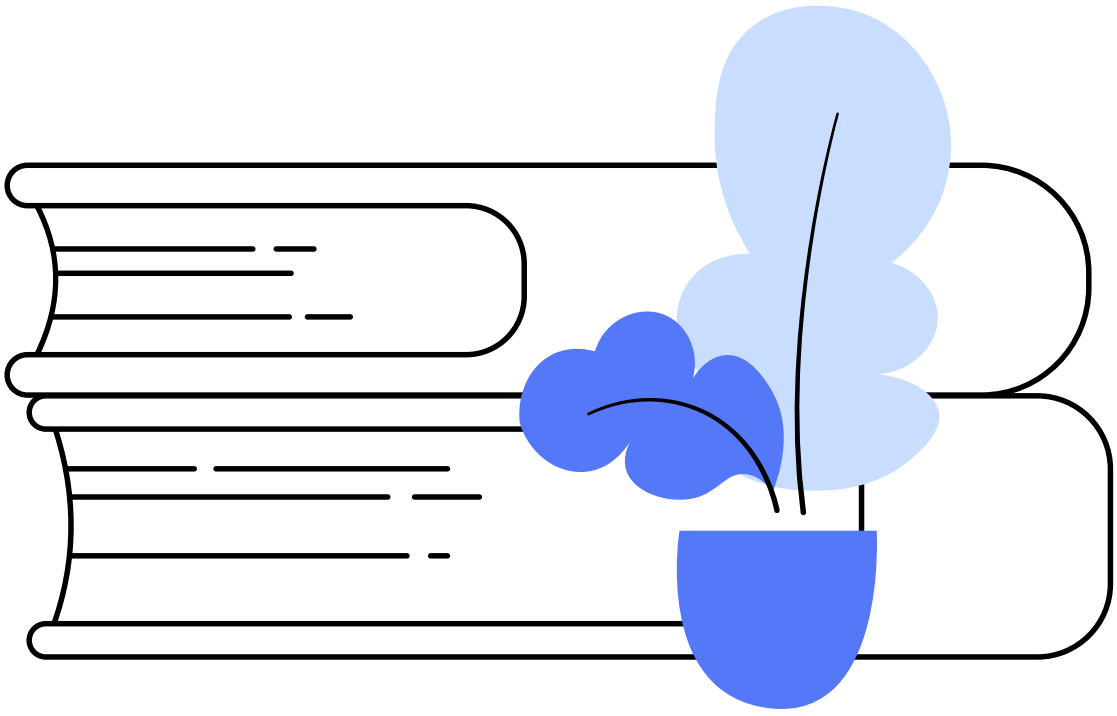
venminder

TOP THIRD-PARTY RISK MANAGEMENT

TERMS TO KNOW

A Glossary of Terminology for Third-Party Risk Management

This eBook is a helpful third-party risk management resource to better understand third-party risk concepts.



a

ARTICLES OF INCORPORATION
A document used to define the company type and often the company ownership structure.

ARTIFICIAL INTELLIGENCE (AI)
The capability of a computer to solve problems, make decisions, and perceive visual information like humans do. AI is a broad field of study encompassing machine learning, natural language processing, robotics, and more. AI systems can learn from data, recognize patterns, and make decisions with minimal human intervention.

AUDIT
The review of policies and procedures to assure compliance. An audit can be done by an internal audit team or by an external team (e.g., examiners or auditors).

AUDIT OPINION LETTER
Provided by a third-party audit and assurance firm in a financial audit that summarizes the scope of work completed by the audit firm and the findings of the audit. Includes a going concern opinion, an opinion on the internal controls, if reviewed, and discussion about information reviewed by the auditors.

AVAILABILITY
Part of the CIA Information Security Triad, it ensures that information is available when needed and only to authorized personnel.

b

BACKGROUND CHECK POLICY
Outlined procedures around employee background checks as part of the hiring process.

BANK SECRECY ACT (BSA)
Requires banks to assist government agencies in detecting potential illegal activity. Requires financial institutions to have a designated BSA Officer responsible for overseeing and monitoring such activities.

BILL OF MATERIALS (BOM)
A comprehensive inventory of the necessary raw materials, components, and instructions needed to create, produce, or fix a product or service.

BOARD OF DIRECTORS
A group that is directly involved in the oversight of a third-party risk management program and, in particular, oversees any activity related to high-risk or critical vendors. The board is ultimately responsible for all of the activities of the organization.

BUSINESS ASSOCIATE
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Business associates must follow the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations as the covered entity. Examples of activities that may require a business associate include data analysis, claims processing or administration, utilization review, and billing.

BUSINESS ASSOCIATE RISK

The risk of harm to individuals or to the covered entity resulting from the business associate's failure to comply with the HIPAA Privacy Rule and Security Rule requirements. This risk is of particular concern because business associates can have access to large amounts of protected health information.

BUSINESS CONTINUITY MANAGEMENT (BCM)

An umbrella term for a comprehensive program that encompasses business continuity (BC), disaster recovery (DR), and pandemic planning. It includes details such as recovery time objectives (RTOs), recovery point objectives (RPOs), and maximum allowable downtime, along with testing to ensure that those metrics are achievable.

BUSINESS CONTINUITY PLAN (BCP)

A plan to ensure that a business's significant operations and products/services continue to be delivered in a full, or at a predetermined and accepted, level of availability. The expected level of availability is typically outlined in the service level agreement (SLA) that the organization has with the vendor.

BUSINESS CONTINUITY RISK

Occurs when an outside event negatively impacts a third-party vendor's ability to conduct business and impacts your organization or customers as a result. Business continuity risk can occur when a vendor fails to test business continuity and disaster recovery plans and is unprepared for technology outages and failures.

BUSINESS IMPACT ANALYSIS (BIA)

A process used to identify and evaluate the potential effects of an interruption to business operations. It helps organizations identify the risks associated with potential disruptions, determine the likelihood of those disruptions occurring, and identify the necessary steps to minimize the potential impact of those disruptions.

C

CAMELS RATING

A supervisory rating system originally developed in the U.S. to classify a credit union's overall condition. It's now applied to every bank and credit union in the U.S. and is also implemented outside the U.S. by various banking supervisory regulators. The CAMELS results represent **C**apital adequacy, **A**sset quality, **M**anagement, **E**arnings, **L**iquidity and asset-liability management, and **S**ensitivity to market risk, which are generally considered highly confidential.

CARVE-OUT METHOD

This method is most common in SOC reporting and means that the subservice organization's controls are NOT included in the scope of the SOC report. The subservice's controls have been carved out and aren't applicable. When a vendor uses this method, it should provide its own due diligence and vendor management documentation. If the method is used for a critical subservice organization, it's recommended to review your fourth-party's SOC report during your due diligence review.

Note: It's still always encouraged to review your critical fourth parties whether the carve-out method is used or not.

CENTRALIZED MODEL

With this third-party risk framework, responsibility of vendor management rests with a single group, such as the compliance office or the third-party risk management team. This approach can ensure consistency but will often create some knowledge gaps with vendor managers by excluding them from the TPRM process.

CERTIFICATE OF GOOD STANDING

A certificate issued by the state to let everyone know the company is current on its tax obligation. The Better Business Bureaus (BBBs) will also issue certificates to businesses that operate ethically and don't have too many complaints.

CHANGE MANAGEMENT POLICY

The documented process for making changes to systems. It should include testing prior to change implementation. A change management policy should increase awareness and understanding of proposed changes across an organization to ensure that all changes are made in a way that minimizes negative impact to services and customers.

CIA INFORMATION SECURITY TRIAD

Stands for confidentiality, integrity, and availability. It's used to help better understand the vendor's approach to security and their overall posture on the CIA elements.

CLOUD SERVICE PROVIDER

Organizations providing cloud computing services and solutions to their customers. Cloud service providers typically provide access to cloud-based applications, platforms, storage, and other resources over the internet. These resources are generally hosted and managed by the cloud provider, which allows customers to access their services from anywhere without having to maintain and manage their own hardware and software.

COMPLAINT ESCALATION PROCEDURE

A process in place that defines how complaints will be handled in a variety of scenarios.

COMPLAINT MANAGEMENT

The process of establishing policies and procedures around managing and responding to any incoming customer complaints.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Found in SOC reports, these are the controls the vendor assumes will be implemented by the subservice organization (your fourth-party vendor) and are necessary to achieve the control objectives stated in the vendor's description of the service organization's system.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

SOC reports will usually include CUECs, which are your organization's responsibility to implement. CUECs will tell your organization what must be done to achieve the vendor's control objectives.

Beware: In these cases, the control objectives stated in the description can be achieved only if these CUECs are suitably designed and operating effectively (by you), along with the controls at the service organization (vendor).

COMPLIANCE

When your vendor needs to adhere to regulations, industry-specific standards, laws, or your organization's internal policies and procedures, compliance is a must. You should outline in the vendor contract how compliance will be achieved.

COMPLIANCE MANAGEMENT SYSTEM

The overall structure of an organization's compliance program which is often cited in examination reports. This structure provides the framework for adherence to all regulatory guidance and consumer protection laws.

COMPLIANCE OR REGULATORY RISK

This risk is present when your third party fails to comply with laws or industry-specific guidelines. Your organization is liable for your third party's compliance and can be subject to legal action if your third party violates regulations. Examples of compliance risks include violating consumer privacy laws or having insufficient cybersecurity practices.

CONCENTRATION RISK

Present when you use several high-risk or critical products or services from the same third party. If the third party suffers a major business interruption/failure, you'll be impacted more severely than if the products and services were provided by different third parties. Concentration risk can also occur when you use too many high-risk or critical vendors within a small geographic area as they'd be simultaneously affected by localized events.

CONFIDENTIALITY

Part of the CIA Information Security Triad, it's seeking to prevent unauthorized disclosure of information.

CONFIDENTIALITY AGREEMENT

In a confidentiality agreement (also known as a non-disclosure agreement or NDA), your organization and your vendor agree to keep certain information private and explain how each party will do that.

CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE (CAIQ)

An industry-accepted way to document what security controls exist in infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software as-a-service (SaaS) environments and is available through the Cloud Security Alliance (CSA). If your vendor has a CAIQ completed, you should have it assessed to ensure their posture aligns with your expectations, the cloud control matrix, and industry best practices.

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

Governing regulatory agency created to enforce federal consumer financial laws and protect consumers. Some of the agency's major responsibilities include enforcing UDAAP, taking consumer complaints, monitoring emerging consumer risks, etc.

CONTRACT

An agreement between two parties creating a legal obligation for an organization and vendor to perform specific activities. Each of the parties to the contract are legally bound to perform the specified duties outlined within the contract.

CONTRACT DURATION

This refers to the timeframe for your contract's duration and includes renewal terms, non-renewal terms, and termination notice periods.

CONTRACT MANAGEMENT

The administration of written agreements with third parties that provide an organization with products or services. It includes negotiating the terms of contracts and ensuring compliance, change management, and ongoing maintenance of the relationship. It's the process of coordinating contract creation, execution, and analysis for the purpose of financial benefit, service delivery, and risk management for an organization.

CONTRACT NEGOTIATION

Involves two or more parties deliberating over the contents of a contract to make a legally binding agreement. Negotiating a contract aims to achieve an agreement that fulfills both parties' needs, reduces liability, and sets expectations for both parties. It also develops important terms and conditions such as legal and regulatory compliance and defines service level agreements (SLAs). Contract negotiation must always occur before the contract is executed.

CONTRACT PROVISIONS

Written terms or conditions in a contract.

CONTROL ASSESSMENT

An examination of an organization's internal controls to determine whether they're effective in safeguarding assets and information, preventing and detecting errors and fraud, and ensuring the accuracy and completeness of financial reporting.

CONTROL OBJECTIVES

The "meat" of a SOC report is in the Control Objectives, Control Activities, Test Procedures and Results section of the report. Control objectives represent the purpose of the specified control activities at the service organization (vendor) and address the risks that control activities intended to mitigate if implemented properly. Control objectives are accomplished by designing, implementing, maintaining, and auditing an effective set of supporting control activities.

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)

A framework created for information technology (IT) management and IT governance. It's a supporting tool set that allows managers to bridge the gap between control requirements, technical issues, and business risks.

COVERED ENTITY

According to HIPAA, a covered entity is a healthcare provider, health plan, or healthcare clearinghouse. These can be individuals, organizations, and agencies. For further clarification, use the HHS Covered Entity Decision Tool.

CREDIT RISK

Another term for "financial risk," it exists when your third party has poor or declining financial health. Increasing costs, decreasing revenues, or losing a major customer can force your third party to discontinue a service or product that is crucial to your organization, or the vendor may go out of business entirely.

CRITICAL VENDOR

A vendor is deemed critical to the organization if any of the three statements below is true:

1. The abrupt loss of the vendor would cause a significant disruption to the operations.
2. The sudden loss of the vendor would impact customers.
3. If the time to restore the service is more than 24 hours, there would be a negative impact on the organization.

CRITICALITY

Refers to the impact that a product or service failure or prolonged, unplanned service interruption would have on an organization or its customer base.

CURE NOTICE

A notice used if a vendor fails to meet a contractual agreement and is a document that outlines specific details as to the requirement of curing any service level or product issues.

CYBER INSURANCE

Separate from general liability insurance, cyber insurance covers risks like data breaches, cyberextortion, cybercrime, and cyberwarfare. It should generally cover any costs associated with investigating a data breach, recovering the data, and addressing any legal and regulatory compliance issues. First-party cyber insurance covers your organization, while third-party cyber insurance covers events caused by third parties. Organizations should require third parties accessing their or their customer's data to have cyber insurance.

CYBER OR INFORMATION SECURITY RISK

Includes both cyber and physical security risk. It's present whenever you have a third party that accesses, transmits, or stores your organization's sensitive data or that has access to your privileged networks or facilities. The threat of third-party data breaches has grown as hackers have developed more aggressive and sophisticated ways to breach private networks. Any gaps in your third party's controls must be addressed to protect your organizational or customer data.

CYBERSECURITY INCIDENT

A security event that has actually or potentially jeopardized the confidentiality, integrity, or availability of an information system.

CYBERSECURITY INCIDENT & VULNERABILITY PLAYBOOKS

A step-by-step guide that outlines the actions to be taken by an organization in the event of a security breach.

CYBERSECURITY PLAN
A formalized set of policies and procedures designed to protect electronic information from unauthorized access or theft.

CYBERSECURITY REVIEW
An assessment of an organization's cybersecurity posture, risk management practices, and controls. A cybersecurity review aims to identify vulnerabilities and recommend steps to mitigate risks.

DATA BREACH
Intentional or unintentional access to sensitive information through human error or cyberattacks, such as phishing or malware.

DATA CLASSIFICATION AND HANDLING POLICY
Procedures that establish how data will be handled and protected in order to keep it secure.

DATA FLOW DIAGRAM
A visual showing the information or data flow being transmitted between different network segments across the organization.

DATA RETENTION AND DESTRUCTION POLICY
Process which identifies the record retention responsibilities of staff, volunteers, board members, and outsiders for maintaining and documenting the storage and destruction of the organization's documents and records.

DECENTRALIZED MODEL
With this third-party risk framework, various lines of business select and work with the vendor directly. The vendor risk or compliance teams may set the rules, but they rely entirely upon the front-line management to execute the rules. This isn't a recommended approach to third-party risk management as it proves to be inefficient with room for error.

DEPARTMENT OF JUSTICE (DOJ)
Enforcement actions often get referred to Justice when there is a clear violation of law.

DIAGRAM
As part of an organization's due diligence package, many consider creating diagrams that outline things like data flow, IVR/call routing flows, the network systems and organizational charts of affiliated companies and staff.

DISASTER RECOVERY (DR)
A subset of business continuity. The disaster recovery plan outlines the processes and procedures the vendor must perform to ensure resumption of standard operations after a business-impacting event like a severe storm or fire.

DISPUTE RESOLUTION
In case of future disputes, your vendor contract should outline how and where disputes will be heard and settled.

DOCUMENT COLLECTION PROCESS
The process used to formally collect vendor due diligence or other official documentation necessary for third-party risk management.

DUE DILIGENCE
The process of systematically validating the legitimacy and good standing of a vendor. It also formally evaluates the vendor's risk management practices and controls to ensure they are suitable for mitigating the risks associated with their product or service. Due diligence is a regulatory requirement and one of the most critical elements of third-party risk management. Risk-based due diligence should be completed before contract execution and updated periodically throughout the vendor relationship. It involves collecting and thoroughly analyzing vendor documentation (e.g., financial, SOC, BC/DR plan reviews).

ENCRYPTION

The process of encoding information by converting the original representation of the information, known as plaintext, into an alternative format to protect sensitive data.

ENFORCEMENT ACTION

A regulatory enforcement action is a legal or administrative action taken by a government agency to enforce a regulation.

ENHANCED DUE DILIGENCE (EDD)

Provides a closer examination of vendors, particularly in situations where anti-money laundering (AML) violations are a concern. EDD may also set a standard for increased scrutiny on vendors with foreign ownership or those associated with a politically exposed person (PEP).

ENTERPRISE RISK MANAGEMENT (ERM)

A holistic approach to managing risk across an entire organization. It involves identifying, analyzing, and responding to potential and actual risks that might affect the organization's ability to achieve its objectives.

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG)

This is an investment strategy that considers an organization's performance in environmental, social, and governance issues and financial performance. ESG investing focuses on organizations that are socially responsible and strives to make a positive impact on the environment and society.

ESG RISK

Risks related to an organization's impact on the environment, society, and how it's governed. These risks can affect an organization's reputation, financial performance, and share price. For example, an organization can face reputational risks if it's found to be polluting a local river, or it could face financial risks if it doesn't have the right policies to protect people in its supply chain from exploitation.

EVERGREEN

A contract provision within the agreement which automatically extends or renews the term.

EVIDENCE OF COMPLIANCE (EOC)

Typically, this is an examination conclusion or margin note in the exam report.

EXAMINER

Internal and external individuals who become a key component of an IT exam.

EXIT PLAN

Describes the roles and responsibilities of both the organization and a third party at the end of the relationship. As part of an exit plan, stakeholders will be consulted, data will be returned or destroyed, third-party access to networks, systems, and physical facilities will be de-provisioned, records will be retained, and equipment, assets, and intellectual property will be returned. It's important that exit plans include timing for all required activities and contingency plans in case the third party is unable or unwilling to fulfill their responsibilities.

EXIT STRATEGY

A plan of action for when the vendor relationship terminates, such as a replacement vendor or bringing the function back in-house. Included within the exit strategy is how the organization's data will be destroyed or returned.

FAIRNESS OF PRESENTATION

Related to SOC reporting, an auditor will determine if the vendor's system description is "fairly presented" and whether it accurately represents the system that was designed and implemented as of a specified date (Type I report) or over a specified period of time (Type II report).

FDIC FIL 3-2012

The FDIC set forth additional guidance on managing third-party payment processors and introduced increased monitoring and transactional testing requirements.

FDIC FIL 19-2019

The FDIC set forth expectations on financial institutions' contracts with third-party service providers.

FDIC FIL 44-2008

The FDIC set forth formal guidance on expectations for managing third-party risk and third-party payment processors. This guidance was rescinded and replaced by the Interagency Guidance on Third-Party Relationships: Risk Management.

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

A governing regulatory agency that assists with sustaining stability and confidence in financial systems by doing things like examining financial institutions, insuring deposits, managing receiverships, etc.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC)

All the major regulators have a seat at the FFIEC table as they mandate uniform principles, standards and report form for governing regulatory agencies.

FEDERAL RESERVE (THE FED)

A governing regulatory agency established on December 23, 1913 with the enactment of the Federal Reserve Act.

FEDERAL RESERVE ACT

U.S. legislation created in 1913 that created the current Federal Reserve System.

FFIEC APPENDIX J

Now a legacy term, this was important and relied upon guidance that was within the FFIEC IT examination handbook and addressed the importance of strengthening the resiliency of outsourced technology services.

FINANCIAL RISK

This risk exists when your third party has poor or declining financial health. Increasing costs, decreasing revenues, or losing a major customer can force your third party to discontinue a service or product that is crucial to your business, or they may go out of business entirely.

FINANCIAL STATEMENT

A document reviewed as part of initial and ongoing due diligence to determine the vendor's financial health (e.g., Form 10-K).

FINTECH

Financial technology, also known as fintech, is an industry that uses technology to improve financial services and make them more accessible. Financial technology includes a range of services such as mobile payments, money transfers, lending, and investing.

FOURTH-PARTY VENDOR

Your vendor's vendor. They're also often called "subcontractors," "subservice providers," or "Nth parties." It's a company or entity with whom a third-party vendor has a direct written contract to provide an outsourced product or service on behalf of the third-party vendor's organization.

GAP (BRIDGE) LETTER

A letter issued by the vendor that covers the "gap" between the last SOC report period end date and the date of the letter. It can be used by the user entity (you) as an interim assurance by management while waiting for the next audit report.

Note: The CPA firm who performed the audit is not attesting to anything in the gap letter. Once the auditors have issued their report and left the site, they don't know if the internal control environment has changed or not. Therefore, a gap letter is merely management's (management from your vendor) assertion that controls are still in place and operating effectively.

GENERAL DATA PROTECTION REGULATION (GDPR)

European regulation, effective May 25, 2018, that protects a customer's data and privacy. It requires anyone who collects, stores, and processes European customer data to increase their controls.

GEOPOLITICAL RISK

The risk of loss caused by political decisions, events, or conditions. This risk can occur when your vendor is located in a country or region vulnerable to political unrest, corruption, or human rights violations. The vendor's location could also be at risk of lax privacy and information security laws or other situations that could be harmful.

GOING CONCERN

Means that a business is assumed to meet its financial obligations when they become due. Audit firms will typically provide an opinion on an organization's going concern. If the audit firm states that the business will remain a going concern without issue, they'll operate without the threat of liquidation or dissolution for the foreseeable future. This means that the company will be a going concern or not in threat of liquidation or dissolution for at least the next 12 months.

GOVERNANCE

The process of setting and enforcing policies and procedures to ensure that an organization or group is operating effectively and efficiently. It involves making decisions about the strategies, objectives, and activities of the organization or group and monitoring and ensuring compliance with those decisions.

GRAMM-LEACH-BLILEY ACT (GLBA)

Requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. GLBA section 501(b) adds standards for financial institutions in administrative, technical, and physical safeguards for the following reasons:

- To ensure the security and confidentiality of customer records and information
- To protect against any anticipated threats or hazards to the security or integrity of records
- To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)

A set of guidelines and best practices for cybersecurity in the healthcare industry. It was developed by the National Institute of Standards and Technology (NIST) in collaboration with industry stakeholders.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

A federal regulation set forth by the U.S. Department of Health and Human Services which provides data privacy and security protections for protected health information (PHI). The regulation text includes both the Privacy Rule and Security Rule and sets standards for electronic healthcare transactions and types of identifiers. Covered entities include health plans, healthcare clearinghouses, and healthcare providers that transmit health information electronically.

HIGH-RISK VENDOR

A vendor who represents a great deal of risk to an organization based on the criteria laid out in risk management policies.

HITECH ACT

This 2009 act was established to expand the scope of the HIPAA Security Rule to cover a Covered Entity's Business Associates. The HITECH Act contains five goals, ranging from the improvement of quality, safety, and efficiency of healthcare to ensuring a patient's privacy and security.

HITRUST

A nonprofit, standards development organization that specializes in cybersecurity and provides assurance that organizations are meeting those standards.

HIGH-RISK VENDOR

A vendor who represents a great deal of risk to an organization based on the criteria laid out in risk management policies.

HYBRID MODEL

With this third-party risk framework, the vendor management office sets the guidelines and checks the results while working closely with the business units.

INCIDENT RESPONSE PLAN/INCIDENT MANAGEMENT POLICY

A policy that outlines procedures for detection, response, and resolutions of incidents as they can affect the confidentiality, integrity, and availability of information or an information system.

INCLUSIVE METHOD

In relation to SOC reporting, controls supporting normal operations provided by your fourth-party vendor are included within a SOC report. Controls of the fourth party are presented separately from those of the third-party vendor and their written assertions should also be included within the report.

INHERENT RISK

An assessed level of raw or untreated risk. It's the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap, or the amount of risk before the application of the risk reduction effects of controls. It's the most amount of potential risk an engagement could pose.

INITIAL DUE DILIGENCE

Another term for "vendor vetting" and "third-party selection." It's implementing pre-contract due diligence to evaluate and select a vendor to outsource a product or service to on behalf of the organization. It should always be completed prior to executing a new contract.

IN-SCOPE VENDORS

Third-party vendors that are required to comply with third-party risk management policies, processes, and practices.

INSURANCE DOCUMENTS
Required documentation that the vendor must have on file to protect both parties. Their insurance requirements are dependent on the nature of the business (e.g., liability insurance, workers' compensation insurance).

INSURANCE STANDARDS
As part of your vendor's contract, insurance standards stipulate that your vendor will be held accountable when an incident negatively impacts your organization's operations or finances.

INTEGRITY
Part of the CIA Information Security Triad, it's ensuring that data isn't modified by unauthorized means.

INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT
Final guidance issued by the FDIC, Federal Reserve Board, and OCC in June 2023 which states how supervised banking organizations should manage third-party relationships. Each agency had previously issued their own general third-party risk management guidelines, which were replaced with this final guidance.

INTERNAL AUDIT
Team who evaluates internal processes and procedures to verify compliance with governing regulations and the organization's policies and procedures.

ISO CERTIFICATION
These certifications, although not mandatory, provide a great indicator of internal process maturity at an organization. If an organization has passed an ISO 27001 audit, you may see the following certifications:

- **ISO 27001** – Creates an Information Security Management System (ISMS) making up the base of information security to build on.
- **ISO 27002** – Contains the controls to put in place once the ISMS is in place. Only ISO 27001 is available for an organization to achieve a certificate as ISO 27002 isn't a management standard, so a certificate is unavailable.

ISSUE
Any unexpected result or scenario requiring further evaluation or actions to mitigate risk. An issue can occur internally within your organization or externally with a vendor.

ISSUE MANAGEMENT
The process of identifying, managing, and tracking issues that arise and remediating them through a collaborative and centralized approach.

IVR/CALL ROUTING FLOWS
Standing for Interactive Voice Response, it illustrates the flow an incoming call will take on an organization's automated voice system.

KEY PERFORMANCE INDICATORS (KPIs)
Measurable values that organizations use to assess their vendor's progress towards long-term objectives. KPIs provide organizations with an indication of how well vendors are performing and identifies areas for improvement.

KEY RISK INDICATORS (KRIs)
Metrics used to measure how likely it is that a particular project or business activity will experience a negative outcome. KRIs help organizations to identify and track risks, and to make decisions about how to manage those risks.

KNOW YOUR CUSTOMER (KYC)
Establishing customer identification requirements and enhanced standards around account opening and monitoring.

LIABILITY INSURANCE

Also called third-party insurance, it's a fundamental part of your risk management system. It protects your organization from the risks of liabilities from lawsuits and protects the insured in the event they're sued for claims that fall within the coverage parameters of the insurance policy. Damage caused intentionally and contractual liability aren't covered under liability insurance policies as it provides coverage for legal fees, which can be quite expensive. This is particularly useful in "nuisance" lawsuits.

LOGICAL ACCOUNT MANAGEMENT POLICY

Policy covering access to information systems, data, and applications.

MANAGEMENT ASSERTION

In relation to SOC reporting, this is the statement that your vendor's management produces which describes what they expect their controls and services to accomplish for your organization. This is required to be in a SOC report. The auditor then expresses an opinion on whether management's assertion is accurate.

You should expect that issues or exceptions that have come to management's attention can result in management's assertion letter being modified. Look for "except for" or other exclusionary language that was added by management to the letter.

MATTERS REQUIRING ATTENTION (MRA)

Identified deficiencies that require some form of corrective action from senior management or the board.

MAXIMUM TOLERABLE DOWNTIME (MTD)

In relation to business continuity planning, MTD specifies the maximum period of time that the vendor can be down before the disruption in services could cause a significant or material loss.

MERGER & ACQUISITION

The process of combining two or more companies into one, which often affects vendor operations.

METRICS

Measurable units of data that are used to track performance. They are typically used to measure things such as customer satisfaction, website traffic, sales, and other key performance indicators.

MID-TERM VENDOR CONTRACT REVIEW

An assessment of a contract or agreement during its active period. It's usually conducted midway through the contract's duration to assess the progress of the agreement and to identify areas for improvement.

MOBILE DEVICE MANAGEMENT (MDM)

Policy or procedure designed to secure and protect mobile devices and make sure employees/vendors are using them correctly in order to mitigate the risk of exposing an organization's data and information.

MONITORING ACTIVITIES

In relation to SOC reporting, these are the processes used by management of a vendor to monitor the quality of internal control performance during the reporting period.

NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

A regulatory agency that protects and oversees credit unions by insuring deposits, protecting members who own credit unions, and regulating the institutions.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

An agency of the U.S. Department of Commerce that works to promote innovation and industrial competitiveness. It provides standards and technology-related services to businesses, government agencies, and other organizations.

NETWORK DIAGRAM

An outline of the network components, their data flow and hardening mechanisms.

NON-DISCLOSURE AGREEMENT (NDA)

Also known as a "confidentiality agreement," it's executed by all parties involved to protect trade secrets and other confidential information.

NONPUBLIC PERSONAL INFORMATION (NPI)

Includes any information that an individual provides to obtain a financial product or service unless that information is otherwise "publicly available." It can also include information obtained from a transaction or in connection with providing a financial product or service. This is defined in the Gramm-Leach-Bliley Act.

OCC BULLETIN 2013-29

It provided an overview of a third-party risk management lifecycle, from the initial planning stage to termination. This was rescinded and replaced with the Interagency Guidance on Third-Party Relationships: Risk Management.

OCC BULLETIN 2017-7

Supplemental third-party risk management guidance to OCC Bulletin 2013-29.

OCC BULLETIN 2020-10

FAQs that supplemented and clarified the existing OCC Bulletin 2013-29. This was rescinded and replaced with the Interagency Guidance on Third-Party Relationships: Risk Management.

OFFICE OF FOREIGN ASSETS CONTROL (OFAC) CHECK

A check required by U.S. Treasury laws and the anti-money laundering statute that is performed on an organization to determine if it's owned or managed by a sanctioned person or nation.

OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

A governing regulatory body that oversees laws and charters, regulates, and supervises national banks, federal branches, and agencies of foreign banks in the United States.

ONGOING MONITORING

An important component of the third-party risk management lifecycle, which occurs for the duration of the vendor relationship. This includes periodic reviews of vendor due diligence and frequent monitoring of vendor risk and performance.

ON-SITE VISIT

Often referred to as "site visit," is an audit conducted on the vendor's/organization's premises to further evaluate their policies and procedures and determine if controls in place are sufficient.

OPERATING EFFECTIVENESS

A concept that refers to the ability of a business or organization to maintain its day-to-day operations in the face of disruption or emergency. It's a measure of how well an organization can respond to and recover from unforeseen events such as natural disasters, cyberattacks, and pandemics.

OPERATIONAL RESILIENCY

Risk present if the vendor's products, services, channels, and processes are critical to the organization's operations.

OPERATIONAL RISK
Present when a third party's product or service is necessary to maintain your organization's daily operations. Suppose a business-disrupting event occurs, such as a system failure or natural disaster, and interrupts normal operations. In that case, your third party must have adequate plans to continue service at agreed-upon levels or resume operations within a given time.

OTHER RISK
Risks present in addition to strategic, operational, transactional, financial, reputation, and compliance risk. The risks can be things like liquidity, interest rate, price, foreign currency translation, and country risks.

OUT OF SCOPE VENDORS
Refers to third parties that aren't governed by your third-party risk management policies, processes, and practices.

OUTSOURCING
Utilizing a company or entity to provide a product or service to an organization or an organization's customer on behalf of them.

OVERSIGHT
Another term used for "ongoing monitoring" and "due diligence," it's the process of thoroughly analyzing a vendor relationship by collecting and reviewing due diligence in order to find and address any risk posed to the organization.

P&P
How many in the industry often refer to "policies and procedures."

PANDEMIC PLANNING
A living document which is reviewed at intervals and revised if there is a change in global guidance or changes to national or international legislation related to communicable disease prevention and control. It includes evidence-based lessons learned from a global health crisis such as a viral epidemic.

PATCH MANAGEMENT
A documented strategy and policy for managing patches or upgrades for software applications and technologies. Software patches are often necessary to fix existing problems with software that are identified after the initial release. Many of these patches have to do with security, while others may have to do with specific functionality for programs.

PCI CERTIFICATION
A certification obtained in the PCI (payment cards industry) that is a data security standard (DSS). Once you have a PCI certification, it means you're now "PCI compliant" and can accept card payments as well as store, process, and transmit cardholder data.

PCI DSS
The payment card industry data security standards required of all credit, debit, and prepaid card issuers.

PENETRATION TESTING
The practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit.

PERSONALLY IDENTIFIABLE INFORMATION (PII)
Refers to any information that allows the identity of an individual to be indirectly or directly inferred.

POLICY
An internal document that asserts how the organization will manage third parties and risk. It's written at a board-level and should include the basic broad framework as to how third-party risk management is handled.

PROCEDURES

Often called the desktop procedures, the document is designed to be a step-by-step recipe for every facet of third-party risk but written in such a way that anyone could follow the steps and come to generally the same work product.

PROGRAM DOCUMENT

An internal document that lays out the concepts within the policy. It should be instructive to senior management and the lines of business, setting out in detailed steps what the business units need to know and what is expected throughout the organization to appropriately manage vendors. It should be strong enough to support all the lines of business, yet flexible enough that it allows for the addition of new third parties or products.

PROTECTED HEALTH INFORMATION (PHI)

Protected health information is any information about a person's physical or mental health, including medical conditions, treatments, and test results. It includes any information that could identify a person, such as their name, address, date of birth, or Social Security number.

QSA ASSESSOR

A PCI DSS qualified security assessor and means you've met security education requirements to be PCI compliant.

QUALITY ASSURANCE

The process of verifying a vendor's products and services are being provided at the highest level of quality to meet the organization's expectations.

RECORD RETENTION POLICY

A policy that details the length of time records will be maintained and includes when they can be discarded or destroyed.

RECOVERY POINT OBJECTIVES (RPOs)

In relation to business continuity planning, RPO is the interval of time that would pass during a disruption before the quantity of data lost during that period exceeds a predetermined maximum allowable threshold or "tolerance."

RECOVERY TIME OBJECTIVES (RTOs)

In relation to business continuity planning, RTOs help identify the targeted duration of time which the vendor must restore a business process, post-disruption, to avoid unacceptable consequences associated with business continuity.

REGTECH

Regulatory technology is a term used to describe the use of technology to help organizations comply with regulations. Regtech solutions automate processes such as reporting, monitoring, and compliance to help organizations save time and money.

REGULATOR

The government agency that regulates an industry (e.g., FDIC, OCC, CFPB, NCUA).

REGULATORY OR COMPLIANCE RISK

The risk present when your third party fails to comply with laws or industry-specific guidelines. Your organization is liable for your third party's compliance and can be subject to legal action if your third party violates regulations. Examples of regulatory risks include violating consumer privacy laws or having insufficient cybersecurity practices.

REPORT OF COMPLIANCE (ROC)
An official record of examination results. It's frequently associated with the PCI.

REQUEST FOR PROPOSAL (RFP)
A document that is shared during vendor vetting with a select group of known vendors, or could be published on an organization's website, as an attempt to find the correct vendor to meet an organization's specific business needs.

RESIDUAL RISK
The risk the organization is left with once the inherent risk is mitigated. It should never be higher than the inherent risk, but instead equal to or less than.

RESTRICTED USE REPORT
SOC reports are required to include a statement restricting the use of the report to management (vendor), user entities (you), and your auditors. User entities should know that when they're a "potential" client of a vendor; this statement relieves the auditor of responsibility of the suitability of the report for the product or services that are being contemplated.

RIGHT TO AUDIT PROVISION
This is considered critical language in vendor contracts. Without the provision, you may experience difficulties at your annual audit reviews, as the vendor can decline to cooperate in sharing due diligence material with you. The contract provision stipulates a vendor must allow you to conduct periodic assessments and have access to the information necessary to conduct the audit.

RISK APPETITE
A measure of an organization's willingness to take on risks in pursuit of its objectives. It's the level of risk the organization is willing to accept to achieve its goals. It's often expressed as a combination of financial, operational, and reputation risk that the organization is willing to accept.

S

SAFEGUARDS RULE
The FTC Safeguards Rule requires financial institutions to have measures in place to protect customer information from unauthorized access. This includes physical, technical, and administrative safeguards such as secure data storage, encryption, and employee training.

SAS70
In 1992, the Statement on Auditing Standards No. 70 was released and set the standards for SOC reporting. SAS70 is no longer applicable as it was replaced by the SSAE 16, which has been superseded with the introduction of the SSAE 18.

SCOPE OF A SOC
Defined by the service organization, not the auditor. Therefore, only findings identified in the failure to achieve a control objective included in the scope are disclosed in the auditor's opinion.

SCRIPTING POLICY
A policy that indicates how call center associates should be interacting with customers. This can be beneficial to have in place, especially if the organization has outsourced to a third-party call center.

SECRETARY OF STATE CHECK
A check performed on the vendor to validate authenticity of the business and that they're properly registered in the state.

SECURITIES AND EXCHANGE COMMISSION (SEC)

The goal of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

SENIOR MANAGEMENT

A team involved in overseeing third-party risk management. Findings should be directly reported to them.

SERVICE AUDITOR

In relation to SOC reporting, the SOC auditor should always be a properly licensed certified public accounting firm in order for the user entity (you) to rely on the audit of the vendor's controls. In a SOC report, the Service Auditor is the entity performing a SOC examination of the service organization's (vendor's) controls.

SERVICE AUDITOR'S REPORT

Commonly referred to as the "opinion letter" and is in relation to SOC reporting, the auditor will express an opinion on the fairness of the presentation of management's description of the system, on the suitability of the design, and, if a Type II audit, on the effectiveness of the controls during the exam period.

SERVICE LEVEL AGREEMENT (SLA)

An agreement between the organization and a vendor that focuses on performance measuring and the service quality agreed to by the organization and vendor. It may be used as a measurement tool, as part of the contract or as a stand-alone document.

SERVICE ORGANIZATION OR SERVICE PROVIDER

Other terms for "vendor." A company or entity providing an outsourced product or service to an organization.

SERVICE ORGANIZATION'S DESCRIPTION OF THE SYSTEM

In relation to SOC reporting, the organization's system is designed, implemented, and documented by the management of the vendor to provide user entities (you) with the services covered by the auditor's report and is comprised of the personnel responsible for using and operating the system; the procedures that guide personnel in the delivery of services to clients, processes used to initiate, authorize, record, and process transactions and the associated reporting system, as well as the overall technical infrastructure that supports, and is supported by, the organization's personnel, procedures, and processes. Components of the technical infrastructure include physical hardware, software, and data as well as the processes that monitor and report on non-transactional events within the system.

SIG AND SIG LITE QUESTIONNAIRES

A standard information gathering (SIG) questionnaire is a holistic tool provided for risk management assessments of 18 different areas of risk such as cybersecurity, IT, privacy, and data security (e.g., completed on critical business systems or high-risk vendors). A SIG Lite is a shorter version of the SIG questionnaire. Typically, it's used as a starting point to conduct an initial assessment of all service providers or on lower risk vendors (e.g., hosting websites, non-critical business systems).

SIGNIFICANT COMPANY FUNCTIONS

Separate departmental functionalities which operate in tandem to make overall business operations possible.

SOC

A system and organization controls report is an independent audit report performed by a public accounting firm. The report will attest to the existence and effectiveness of controls specified by the company being audited (the vendor). Basically, the report should tell an organization if a vendor has the right controls in place to safeguard their data and if those safeguards are actually working, based on the scope of the audit determined by the vendor.

SOC 1

Addresses internal controls that are relevant to a company's control environment over financial reporting. By definition, a SOC 1 is designed to review a vendor's financial and accounting controls and the systems that support them.

SOC 2

Addresses internal controls that are relevant to a company's internal control environment over the following five Trust Services Criteria (TSC):

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

By definition, a SOC 2 is designed to review a vendor's control environment in relation to the selected TSC based on the vendor's defined scope.

SOC 3

A high-level summary of the SOC 2 audit. It's not as detailed and often only requested during vendor vetting.

SOC FOR CYBERSECURITY

A report developed by the American Institute of Certified Public Accountants (AICPA) in 2017 that companies may provide upon request if someone is seeking to better understand the maturity and effectiveness of their cybersecurity program.

SOC FOR SUPPLY CHAIN

Overlaps with the SOC 2 in some ways, as they both include one, some, or all of the TSC. Like SOC for Cybersecurity, if you request the SOC for Supply Chain, review the following:

- Management's Description
- Management's Assertion
- Practitioner's (CPA) Report

SOCIAL ENGINEERING

The use of deceptive techniques, often based on a user's habits or environment, to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

SOCIAL ENGINEERING TESTING

Testing that focuses on human error within the organization, meaning testing employee vulnerability to common tactics (e.g., phishing email).

SSAE 18

The standard for SOC reporting. The SSAE 18 causes the SSAE 16 to be retired as 16 is covered within 18. It's a simplified standard covering many others, the SSAE 16 was just one. SSAE 18 is a series of enhancements aimed to increase the usefulness and quality of SOC reports. The purpose for the creation of the SSAE 18 was to clarify the auditing standards and to reduce duplication within similar standards covering examinations, reviews, and agreed-upon procedure engagements, specifically SSAE Nos. 10-17. These now fall under SSAE 18.

STATE OF INCORPORATION

A document that provides verification that the company is incorporated, is filing tax returns, and is a business.

STATUTORY LAW

Law that has been passed by state or federal government.

STRATEGIC RISK

Occurs when your third party's actions and/or decisions fail to help your organization meet its goals and objectives. For example, if your third party uses outdated technology, it may become difficult for your organization to perform normal operations.

SUBCONTRACTOR

Often referred to as "subservice provider" or "fourth party," it's a company or entity with whom a third-party vendor has a direct written contract with to provide an outsourced product or service on behalf of the third-party vendor's organization.

SUBJECT MATTER EXPERT (SME)

Someone who is a qualified or certified individual with a specific area of expertise.

SUBSERVICE ORGANIZATION

Sometimes referred to as fourth parties, simply put, a subservice organization (or subservice provider) is your vendor's vendor. These subservice organizations perform some of the services provided to user entities that are likely to be relevant to controls over financial reporting. A typical example would be the bill payment provider that is performing and delivering the bill payment service included as part of your internet banking contract.

SUBSIDIARY

A company that is controlled by a holding company.

SUITABILITY OF DESIGN

In relation to SOC reporting, it's when an auditor determines if controls in a SOC report are suitably designed and provides reasonable assurance that the control objective(s) are achieved.

SUPPLY CHAIN RISK MANAGEMENT

The process of identifying, assessing, and mitigating risks that could disrupt the supply chain. This includes risks associated with production, transportation, and other areas of the supply chain. It involves both proactive and reactive measures to ensure that operations are not disrupted.

TAX ID

A company's IRS tax identifier number that ensures they're registered with the IRS, state of incorporation, and the state in which they plan to do business.

TECHNOLOGY SERVICES PROVIDER (TSP)

A technology provider. This often includes internet service providers, cloud providers, etc.

TERMINATION CLAUSE

A stipulation in a contract that outlines the conditions under which either party is allowed to terminate the agreement. Such a clause typically states that either party can terminate the agreement with a certain period of notice and may include other provisions such as payment of damages or fees.

TEST OF CONTROLS

In relation to SOC reporting, it's the procedure that evaluates the operating effectiveness of control activities necessary for achieving the control objectives stated in management's description of the service organization's system in a SOC report.

THE LINES OF DEFENSE

The first line of defense is the business line, which is responsible for identifying and managing risks associated with a product or process. The second line of defense is the risk management and oversight function, which is responsible for making sure the controls in place are sufficient and effective. Finally, the third line of defense is the audit function, which is responsible for monitoring and assessing the risks and controls, as well as providing assurance to the board of directors.

THIRD-PARTY RISK MANAGEMENT (TPRM)

Often referred to as "vendor management" or "vendor risk management," it's the process of fully identifying all of the significant companies that aid in the delivery of a product or service to an organization or to an organization's customers on behalf of the organization. It involves controlling costs, driving service excellence, and mitigating risk to gain increased value throughout the vendor lifecycle.

THIRD-PARTY RISK MANAGEMENT LIFECYCLE

The third-party risk management lifecycle is a systematic process to identify, assess, mitigate, and monitor third-party risks throughout the relationship with a vendor. The lifecycle is divided into three core stages: onboarding, ongoing, and offboarding.

THIRD-PARTY RISK MANAGEMENT SCOPE

The process of identifying vendors who should be actively managed and the vendors who don't need to be actively managed. Typical out of scope third parties include:

- Government agencies
- Public utilities
- Sponsorships and donations
- Professional memberships and conference fees
- Media subscriptions

THIRD-PARTY SELECTION

Another term for "vendor vetting" and "initial due diligence," it's implementing pre-contract due diligence in order to evaluate and select a vendor to outsource a product or service to on behalf of the organization. It should always be completed prior to executing a new contract.

THIRD-PARTY RISK MANAGEMENT STRATEGY

This defines how an organization identifies and addresses risks posed by third-party relationships within a specific risk tolerance. For managing third-party risk effectively, a good third-party risk management strategy considers external factors such as regulatory requirements, best practices, customer expectations, internal objectives, resources, conditions, limitations, and risk appetite.

THIRD-PARTY VENDOR

A company or entity with whom the organization has a direct written contract with to provide an outsourced product or service on behalf of the organization.

THREAT MANAGEMENT

Approach to network and information security which integrates a number of different approaches to threats designed to mitigate the risk and protect the assets of an organization or individual.

TOTAL LIQUIDITY

Represents the total cash, cash equivalents, and access to immediate capital, such as an available line of credit or available term debt that it can draw to generate immediate cash. Total liquidity is one of the primary variables of an organization's financial health and profile.

TRANSACTIONAL RISK

Occurs when your organization fails to process a transaction correctly and it affects a customer. Any vendor's faulty delivery of a product or service can cause your organization transactional risk.

TRUST SERVICES CRITERIA (TSC)

Found in SOC 2 reporting and are defined as follows:

- **Security** – The system is protected against unauthorized access (both physical and logical).
- **Availability** – The system is available for operation and use as committed or agreed.
- **Processing Integrity** – System processing is complete, accurate, timely, and authorized.
- **Confidentiality** – Information is protected as committed or agreed and the unauthorized disclosure of information is prevented appropriately.
- **Privacy** – Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and criteria set forth in Generally Accepted Privacy Principles issued jointly by the AICPA and the Canadian Institute of Chartered Accountants.

TYPE I SOC REPORT

Type I reports audit controls as of a point in time, or a 'snap shot' of the presented controls. A Type I covers the design of controls placed in operation.

TYPE II SOC REPORT

It's only with a Type II SOC report that the auditor validates that the stated controls are in place and reports on the effectiveness of the controls over a period of time and assesses how well they're working. Generally speaking, controls must be in place for at least three months in order for a Type II report to be issued.

U

UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAP)

A regulation enhanced from the Federal Trade Commission (FTC) Section 5 as part of Dodd-Frank to include a new standard for "abusive." UDAAP has been the primary enforcement action used by the Consumer Financial Protection Bureau (CFPB), in particular.

USER ENTITY

In relation to SOC reporting, the client of a service organization, you (the organization) are the user entity.

V

VENDOR

Your vendor (also known as a "third party") is a business entity or individual that provides a product or service to your organization or to your customers on your behalf.

VENDOR INTERNAL CONTROLS

Measures put in place to help mitigate the potential risks associated with a particular activity or system. Risk controls include security protocols, safety procedures, and insurance policies. They help to reduce the chances of an incident occurring and limit the potential damage if it does occur.

VENDOR INVENTORY

A complete list of vendors that is typically requested from the Accounts Payable department on a regular basis. The vendor list is to be reviewed by the third-party risk management team to determine which vendors need actively managed and which vendors need written out of the third-party risk management scope.

VENDOR MANAGEMENT OFFICE (VMO)

The VMO is where all vendor management for the enterprise is centered. It consists of all the vendor management, third-party risk management, and certain organizational change management projects that arise from the purchase and implementation or installation of products or services.

VENDOR MANAGER / VENDOR OWNER

An individual who manages a vendor relationship daily by doing things like reaching out to the vendor with any questions, coordinating documents requests, completing risk assessments and due diligence reviews, staying abreast of the industry regulations, etc.

VENDOR PERFORMANCE

Vendor performance is the measurement of a vendor's ability to meet the requirements of a contract or agreement. It includes factors such as the quality of goods and services provided, delivery times, customer service, and cost effectiveness.

VENDOR RISK ASSESSMENT

Assists with analyzing new and ongoing vendor relationships in order to gauge the level of risk posed to the organization. It evaluates all of the considerations of outsourcing a product or service.

VENDOR RISK ASSESSMENT QUESTIONNAIRE

A questionnaire designed to formally assess the risk posed to an organization by doing business with a vendor. While there's no template provided by the regulators, it's encouraged to review regulatory guidance in order to determine the questions to include in the organization's VRA template and also develop a rating system.

VENDOR RISK MANAGEMENT (VRM)

Often referred to as "vendor management," or more accurately, "third-party risk management," it's the process of fully identifying all of the significant companies that aid in the delivery of a product or service to an organization or to an organization's customers on behalf of the organization. It involves controlling costs, driving service excellence, and mitigating risk to gain increased value throughout the vendor engagement.

VENDOR RISK PROFILING

The process of assessing third-party vendors for potential risk to an organization. It involves evaluating vendors' security policies, procedures, and processes, as well as their financial and compliance status. This allows organizations to identify and mitigate risks associated with third-party vendors.

VENDOR SCORECARD

A tool used to measure and evaluate the performance of a vendor or supplier. It's used to compare vendors on criteria such as cost, quality, customer service, and delivery. The scorecard helps organizations make informed decisions when selecting or retaining vendors.

VENDOR VETTING

Another term for "third-party selection" and "initial due diligence," it's implementing pre-contract due diligence in order to evaluate and select a vendor to outsource a product or service to on behalf of the organization. It should always be completed prior to executing a new contract.

VULNERABILITY

Weaknesses in information systems, system security procedures, internal controls, or implementation that could be exploited by external threats.

VULNERABILITY ASSESSMENT/VULNERABILITY TESTING

A test that identifies any security vulnerabilities in the infrastructure (e.g., computer, network, or communications).

VULNERABILITY MANAGEMENT

Ongoing practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.

WORKERS' COMPENSATION

Provides wages and medical benefits to employees who are injured in the course of employment. The employee gives up the right to sue their employer for negligence. Every state has a minimum coverage limit, and vendors will be required to meet the specific coverage for the state in which they have employees conducting business.

ZERO-TRUST MODEL

A security control used to ensure that your vendor's access to privileged networks and sensitive information is limited to the minimum requirements needed to perform normal operations. A contract may not mention a zero-trust model by name; however, it must have information regarding the vendor's security controls and how they effectively protect your information.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.