THE **ULTIMATE**

THIRD PARTY RISK MANAGEMENT **DICTIONARY**

A Glossary of Terminology for Third Party Risk Management

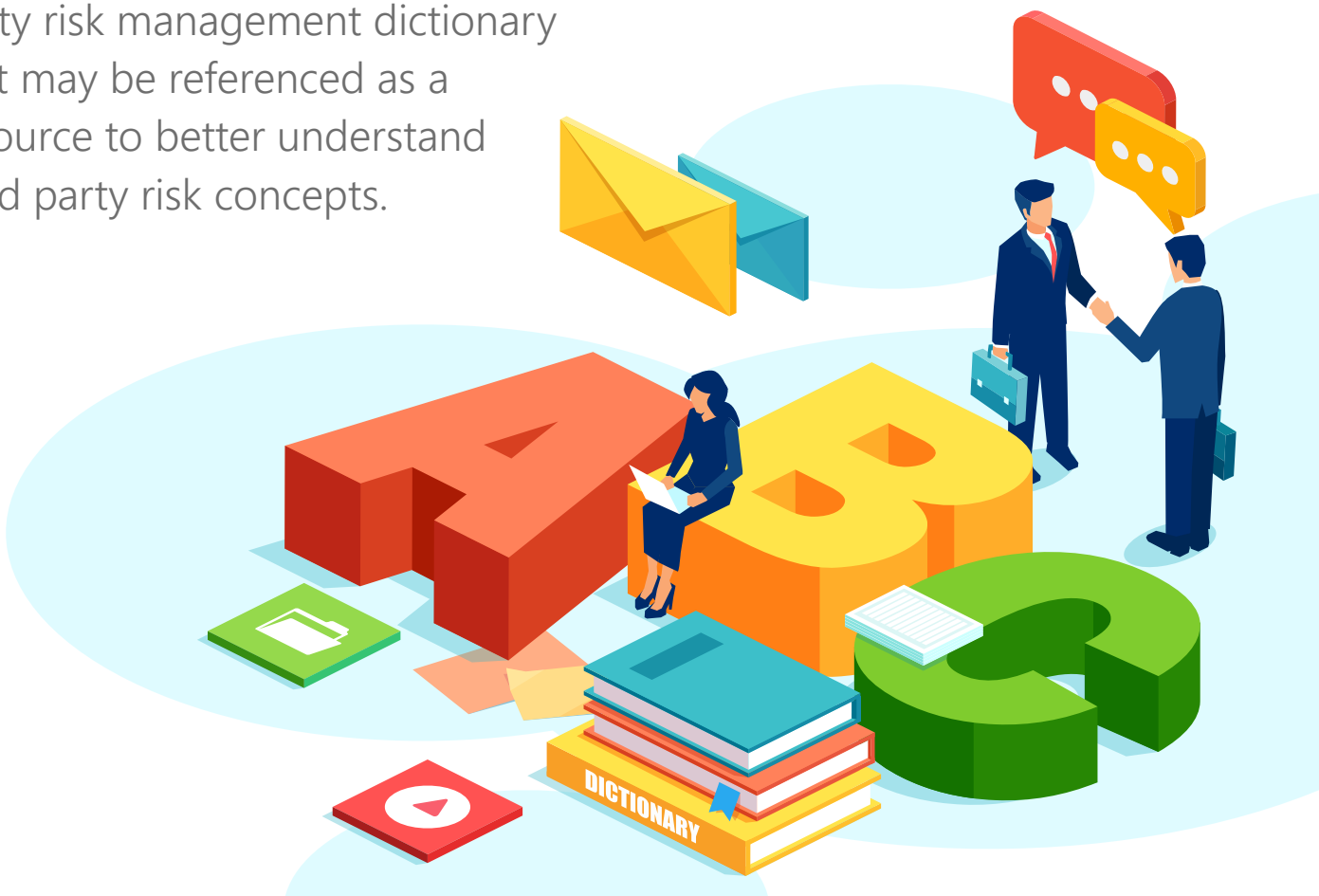
venminder

THE **ULTIMATE**

THIRD PARTY RISK MANAGEMENT **DICTIONARY**

A Glossary of Terminology for Third Party Risk Management

This eBook is your go-to third party risk management dictionary that may be referenced as a resource to better understand third party risk concepts.



ARTICLES OF INCORPORATION

A document used to verify the company type and often the company ownership structure.

AUDIT

An official inspection of a vendor risk management program to ensure compliance. An audit can be done by an internal audit team or by an external team (e.g., examiners or auditors).

AVAILABILITY

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

BACKGROUND CHECK POLICY

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

BOARD

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.

BUSINESS CONTINUITY PLANNING (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 IMPACT ANALYSIS

In relation to business continuity and disaster recovery planning, it's used to identify the gaps between what the business requires and what the actual resources and capabilities are.

BUSINESS IMPACT RISK

Determines if the vendor is critical or non-critical to an organization.

CARVE-OUT METHOD

In relation to SOC reporting, the carve-out method is used when controls at the vendor's vendor (fourth party) have been excluded from the SOC audit. It's appropriate for a vendor to use the carve-out method for supporting services provided to the vendor that are required for normal operations. The third party vendor should provide documentation supporting their own due diligence and vendor management practices. **Note:** It's still always encouraged to review your fourth party vendors regardless if 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.

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 process of managing any change to the organization with a new process, program, project or procedure that affects either the enterprise, a department or both.

CIA INFORMATION SECURITY TRIAD

An information security triad standing 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.

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 controls that management of the service organization (vendor) assumes will be implemented by the subservice organizations (fourth party vendor) and are necessary to achieve the control objectives stated in management's description of the service organization's system.

COMPLEMENTARY USER ENTITY CONTROLS

SOC reports will usually include Complementary User Entity Controls. These are controls that the vendor has included within its system and rely on the user entity (you) to implement in order to achieve the vendor's control objectives.

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

COMPLIANCE RISK

A risk that is present if the vendor's adherence to laws, regulations, guidelines and industry expectations isn't meeting standards.

CONFIDENTIALITY

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

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 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

Negotiation must be conducted prior to signing the vendor contract in order to limit an organization's liability, set expectations for both parties (the organization and the vendor) and develop right to audit language and service level agreements (SLAs).

CONTRACT PROVISIONS

Written terms or conditions in a contract.

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.

CREDIT RISK

Another term for "financial risk", it's the risk present in the vendor relationship if there is a decline in earnings, pending litigation or many changes at the vendor company that impacts their overall financial condition.

CRITERIA

In relation to SOC reporting, the criteria define whether an audit is a "Type I" or "Type II" examination.

CRITICAL VENDOR

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

1. The sudden loss of the vendor would cause a significant disruption to the business.
2. The sudden loss would impact customers.
3. The time to restore service without the vendor is greater than one business day or greater than what the organization's business continuity plan (BCP) calls for as a recovery time.

CRITICALITY

The probability that using an outsourced product or service will cause severe events which may pose risk on the organization or organization's customers.

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.

CUSTOMER NOTIFICATION PROCESS

Establishing a formal process that defines who and how customers will be notified when a customer impacting event occurs (e.g., data breach).

CYBERSECURITY PLAN

Helps protect an organization and the vendor from potential vulnerabilities (e.g., data breach). Identifies the vendor's cybersecurity posture by discovering any weaknesses, and from there, gives you the information needed to effectively communicate to the vendor any requests to have their controls strengthened.

DATA BREACH

Intentional or unintentional access to sensitive information through 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.

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.

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 up to resumption of standard operations.

DUE DILIGENCE

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 as well as updated periodically throughout the vendor relationship. It involves collecting and thoroughly analyzing vendor documentation (e.g., financial, SOC, BCP/DR reviews).

ENFORCEMENT ACTION

When a governing regulatory body takes legal action and/or fines an organization for not following the guidance by which they're mandated.

ENTERPRISE RISK MANAGEMENT (ERM)

Considers all of the different categories of organizational risk to set policy standards and determine the organization's risk appetite (e.g., credit risk, compliance risk, interest rate risk, vendor risk).

EVERGREEN

A contract provision within the agreement which automatically extends or renews the agreement term after the initial term has been met.

EXAMINER

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

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," if 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-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.

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 such as the NCUA, FDIC, OCC, CFPB and more.

FFIEC APPENDIX J

Guidance within the FFIEC IT examination handbook that addresses the importance of strengthening the resiliency of outsourced technology services.

FINANCIAL RISK

Another term for "credit risk," it's the risk present in the vendor relationship if there is a decline in earnings, pending litigation or many changes at the vendor company that impact their overall financial condition.

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).

FOURTH PARTY VENDOR

Often referred to as "subservice provider" or "subcontractor", 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.

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. It should be noted that 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 do not 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.

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

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. It's a recommended approach for larger organizations.

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, if the Inclusive method was used, 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

The "first impression" risk upon first glance at a vendor's due diligence.

INITIAL DUE DILIGENCE

Another term for "vendor vetting" and "third party selection". 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.

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).

INTEGRITY

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

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.

IVR/CALL ROUTING FLOWS

Illustrate the flow an incoming call will take on an organization's automated voice system.

KPI

Key performance indicators are used to identify and measure organizational success in meeting objectives.

KRI

Key risk indicators designed to guide management of risk levels throughout the organization.

LEADERSHIP

Management and the board must take an active role in third party risk management.

LOGICAL ACCOUNT MANAGEMENT POLICY

Policy covering access to information systems, data and applications.

MANAGEMENT ASSERTION

In relation to SOC reporting, management at your vendor states what the system is at a high level and attests to what management has written in the System Description and Control Environment. This is required to be in a SOC report. The auditor then expresses an opinion on whether or not 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. It's not always about what is in the SOC audit. It can many times be about what isn't included in the audit.

MATTERS REQUIRING ATTENTION (MRA)

MRAs are considered a deficiency that is identified and requires some form of corrective action.

MAXIMUM TOLERABLE DOWNTIME (MTD)

In relation to business continuity planning, MTDs specify the maximum period of time that the vendor can be down before the organization's survival is at risk.

MERGER & ACQUISITION

The process of combining two or more companies into one. This often happens with vendors.

MONITORING ACTIVITIES

Related to SOC reports, 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 whom protects and oversees credit unions by insuring deposits, protecting members who own credit unions and regulating the institutions.

NETWORK DIAGRAM

Illustration showing the flow of activity between tasks.

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.

OCC BULLETIN 2013-29

The "gold" standard to third party risk management. It provides a vendor risk management lifecycle that is encouraged to be followed.

OFAC CHECK

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

ONGOING MONITORING

An important pillar of third party risk management. For as long as an organization is leveraging an outsourced vendor, they must maintain ongoing monitoring. This includes periodic reviews of vendor due diligence, frequent monitoring of SLAs and addressing risk issues.

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

In relation to SOC reporting, in the opinion of the auditor, a determination is made regarding whether a control is operating effectively and provides reasonable assurance that the control objectives stated in management's description of the vendor's system were achieved.

OPERATIONAL RISK

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

OTHER RISK

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

OUTSOURCING

Utilizing a company or entity to provide a product or service to an organization or an organization's customers 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.

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.

PENETRATION TESTING

A test performed to exploit any weaknesses in a system.

PILLARS OF THIRD PARTY RISK MANAGEMENT

Six fundamental elements in risk management identified as selecting a vendor, risk assessment, due diligence, contractual standards, reporting and ongoing monitoring.

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

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 fairly 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 of the lines of business yet flexible enough that it allows for the addition of new third parties or products.

QSA LETTER

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 (RPO)

In relation to business continuity planning, RPOs assist with understanding the age of files that must be recovered from backup storage for normal operations to proceed if they had suddenly been disrupted.

RECOVERY TIME OBJECTIVES (RTO)

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.

REGULATOR

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

REGULATORY RISK

Determining the risk rating based on guidance like FDIC FIL-44-2008 and OCC Bulletins 2013-29 and 2017-7, to help better understand the risk a vendor poses to the organization based on specific categories (e.g., strategic, compliance, operational, financial). Determines the vendor's risk rating which is often high, moderate or low risk.

REPUTATIONAL RISK

Risk present if the vendor interacts directly with an organization's customers or members. Also, the

risk posed by a vendor engaging in poor business practices or turning a deaf ear to customer complaints.

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.

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

The Scope of a SOC (control objectives and related controls) is 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

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'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.

SERVICE ORGANIZATION OR SERVICE PROVIDER

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

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).

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

A 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

A 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 TSCs based on the vendor's defined scope.

SOC 3

A SOC 3 report is 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 how mature or effective their cybersecurity risk program is.

SOCIAL ENGINEERING

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

SSAE 18

As of May 1, 2017, SSAE 18 is the new 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 other standards, 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

Risk present if the vendor offers products or services that aren't compatible with the organization's strategic goals, can't be effectively monitored by the organization or don't provide an adequate return on investment.

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 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.

SUBSERVICE PROVIDER

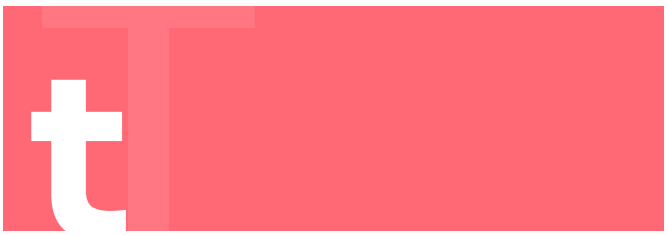
Often referred to as "subcontractor" or "fourth party," it's a company or entity with whom a third party vendor has a direct written contract with to provide an outsourced product or service on behalf of the third party vendor's organization.

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.



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.

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 is the front line or business unit who are managing third party relationships daily. The second is the independent risk management function like compliance or third party risk departments. The third line in the independent audit function who reviews the first line and second line to verify work product accuracy and effectiveness of the controls in place.

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. Many programs will write a vendor out of scope if they answer "yes" to any of the following questions:

1. Are they a government agency?
2. Are they a utility company?
3. Based on your policy, do they fall below a certain threshold dollar amount?
4. Are they an office supply or food delivery company?
5. Are they a licensing company?
6. Is the spend so minimal or such a limited one time use that it's below any reasonable risk threshold?

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 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.

TRANSACTIONAL RISK

Risk that 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:

1. **Security –** The system is protected against unauthorized access (both physical and logical).
2. **Availability –** The system is available for operation and use as committed or agreed.
3. **Processing Integrity –** System processing is complete, accurate, timely and authorized.
4. **Confidentiality –** Information designated as confidential is protected as committed or agreed.
5. **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

A Type I SOC report includes the System Description and Management Attestation concerning the presentation and design of controls within the service organization. Type I reports audit controls as of a point in time.

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 (how well are they working). Generally speaking, controls must be in place for at least six months in order for a Type II report to be issued.

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

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.

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 third party risk 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

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 the industry regulations, etc.

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 is 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" in recent years, is 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 deal lifecycle.

VENDOR RISK MANAGEMENT LIFECYCLE

Every vendor relationship has a deal cycle that should include the following stages:

1. **Planning –** Building out the vendor management policy, program and procedures documentation.

2. **Due Diligence and Third Party Selection –** Implementing pre-contract due diligence expectations as part of the vendor selection process, aka vendor vetting.

3. **Contract Negotiation –** Negotiation is done to help limit an organization's liability, set expectations for all parties involved, include right to audit provisions and define due diligence expectations.

4. **Ongoing Monitoring –** During the entire vendor relationship, ongoing monitoring and due diligence must be performed to assess any new risk issues that may arise, continue to monitor SLAs and thoroughly analyze due diligence.

5. **Termination –** When it's time to end a contract, there must be steps outlined that include the plan to replace the vendor or bring the function back in-house and how any data will be returned or destroyed.

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.

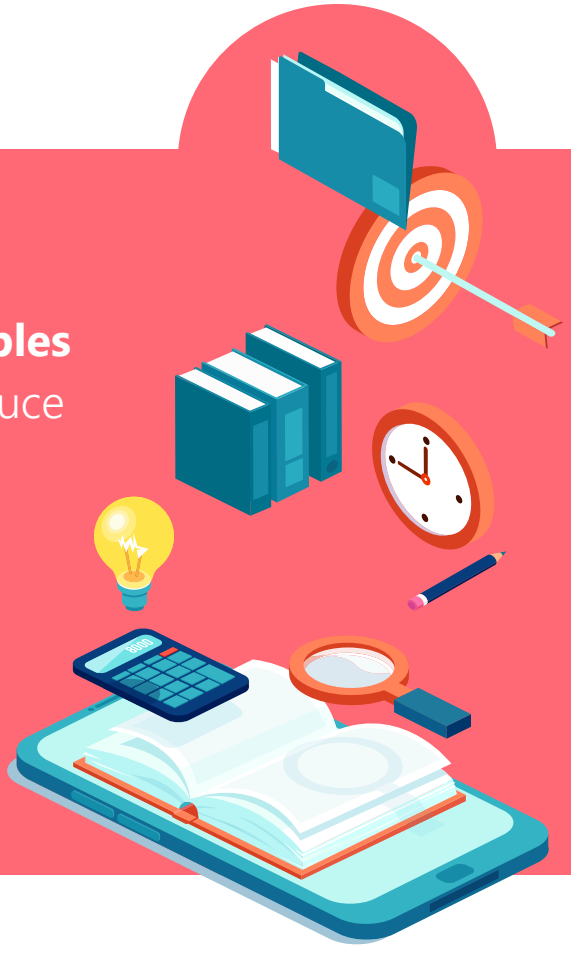
VULNERABILITY ASSESSMENT/ VULNERABILITY TESTING

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

Z

Z SCORE

The Altman Z score determines a company's likelihood of bankruptcy.



venminder

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

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.