Policy Reference & Name:	AEMP10 – Third-Party Management
Effective Date:	December 7, 2021
Policy Sponsor:	Senior Vice President and Chief Procurement Officer
Policy Custodian:	Vice President, Third-Party Risk Management
Policy Overseer:	Vice President, Vendor Risk Oversight
Approval Requirement:	Approval Level Required: Level 1 Level 1: Risk Committee of the AXP Board of Directors Level 2: Enterprise-wide Risk Management Committee Level 3: Operational Risk Management Committee Level 4: Policy Signatories
Level 4 Policy Signatories:	1. Policy Sponsor – SVP and Chief Procurement Officer 2. Policy Overseer – Vice President, Vendor Risk Oversight
Policy Scope:	AXP Company Management
Next Scheduled Review	
Target Approval Date:	December 2022
No Later Than:	February 2023
Changes to Previous Policy:	1. Enhanced language throughout the document to clarify scope, applicability, and key terms. 2. Revised roles and responsibilities to reflect the current first line operating model. 3. Updated Alternate Practice key terms, supporting requirements and implementation date. 4. Updated Section 9 to reflect effective date of policy requirements 5. Removed Appendix 1 to appropriately outline service categories in the Standards as operational execution 6. Removed Appendix 2 which is the 2020 version of the policy and not obsolete given the current state of the program

Table of Contents:

1.0 OVERVIEW AND PURPOSE

Overview: American Express Company ("American Express", "AXP", the "Company"), engages Third Parties in the course of its business activities to improve performance, manage costs, enhance good or service offerings, gain strategic or operational advantage, access market expertise, and evaluate industry best practices among other reasons. The use of Third Parties by the Company requires risk management practices to ensure goods and services are delivered in a sound manner and consistent with applicable laws. The American Express Board of Directors and Management are responsible for ensuring activities undertaken by third parties on behalf of American Express are (1) conducted in compliance with applicable laws, rules, regulations (including those intended to protect consumers), regulatory guidance, and American Express policies, (2) subject to appropriate risk management standards (security, privacy, consumer protection, etc.), as if American Express were conducting those activities directly, and (3) procured and consumed in a cost-effective manner and in support of American Express business and strategic objectives. The term "Third Party" includes frequently used terms such as "supplier", "vendor", "outsourcing" and "service provider" among others and it encompasses all Non-affiliated and Affiliated entities which have a business arrangement with American Express.

Purpose: This Policy sets forth the procurement, risk management, and contracting framework for managing Non-Affiliate Third-Party relationships commensurate with their risk and complexity. In addition, the Policy sets guidelines for identifying, measuring, monitoring, and reporting the risk associated with Third Parties through the life cycle of those relationships which includes planning, Third-Party selection, due diligence, contracting, ongoing monitoring, and termination. Furthermore, the document outlines the roles, responsibilities, and accountability for the management and oversight of the risk associated with these relationships.

This Policy is not intended to supersede, replace, or modify legal or regulatory requirements.

2.0 SCOPE

All third-party relationships held by American Express Company and its direct and indirect subsidiaries and Controlled Entities as defined by *AEMP37 Controlled Entity Governance Policy* (including Joint Ventures providing products or services to American Express) are in scope for this Policy and its requirements as defined in *Section 5.0 Policy Requirements*, unless otherwise stated.

This Policy applies to all American Express colleagues in all Business Unit globally and outlines management activities based on the category, risk of the service, and complexity of the relationship with the following types of Third Parties:

- **AXP Affiliates** – Internal entity that is under common control of American Express. Additional related requirements in *AEMP57 Transfer Pricing Policy*
- **Non-Affiliate Third Parties -** external entities which have a business arrangement with American Express including, but are not limited to, providers of goods and services.

For a list of categories of Third Parties covered in this Policy, please refer to the *Procurement Standard* or the *Third-Party Risk Management Standard ("TPRM Standard")*. Specific Third-Party relationships may follow the requirements of Alternate Practices as defined in *Section 3.0 Key Definitions* and outlined in the *Alternate Practices Standard*.

The following relationships are not considered to be third-party and therefore **out of scope** for this Policy:

- Charitable Contributions: payments to charitable entities
- Colleague T&E Spend on Corporate Card: Internal/Colleague T&E
- Customer (Consumer and Corporate): Person or entity who utilizes American Express' products and/or services. This does not include other relationships American Express may have with such individuals or entities, such as third-party relationships
- Government Regulators: Government oversight bodies (FRB, OCC, etc.) in their capacity overseeing AXP practices and compliance with regulatory requirements
- Insurance (Corporate Assets): Insurance products purchased by American Express to insure its own business and assets
- Investments and Market Risk Management Activities: Institutions which accept client's funds as deposits, operating cash or other forms of investments. Entities, such as banks regulated in jurisdictions in which AXP legal entities are located in, with which American Express enters into financial transactions, e.g.: foreign exchange, interest rate, equity derivatives and reverse repos
- Merchant Membership Rewards (Pay with Points or Points Transfer Agreements): Reward pay with points and points transfer. This does not include Membership Rewards Merchandise Partners
- Merchant Card Acceptance Agreements: American Express acquisition of a merchant used strictly for card acceptance
- Mergers and Acquisitions as defined in *AEMP40 – Merger & Acquisition Deal Approval Policy*
    - Third parties of American Express-acquired companies are in scope for this Policy and integration must be planned, documented, and then approved.

3.0 KEY DEFINITIONS

Alternate Practice: Process to manage specific categories of services with unique characteristics that require atypical risk management considerations across one or more phases of the lifecycle. Third Parties providing services in these specific categories are managed in adherence to the *Alternate Practice Standard* and are subject to review for operating effectiveness by Third-Party Risk Management.

Approved Services and Suppliers List (ASL): A listing of Third Parties that provide one or more of the goods and/or services managed by Strategic Sourcing & Business Enablement which have already satisfied applicable due diligence and Contract requirements. The purpose of the ASL is to build effective spend leverage, improve Third-Party risk management, and reduce administrative costs associated with Third-Party maintenance. Using a Third Party included in the ASL may reduce time to market. American Express colleagues are to make every effort to utilize the ASL.

Bypass: Occurs when an American Express colleague fails to meet the requirements of this Policy by not engaging Global Supply Management (GSM) prior to entering into a relationship with a Third Party for any good or service or otherwise fails to comply with Third-Party Risk Management requirements including, but not limited to signing or otherwise agreeing to legal or any contract terms as defined in this section, directs a Third Party to provide services, or pays for services without complying with the requirements in this Policy.

Contract: A binding agreement including specific terms of engagement between American Express and one or more third parties. The following types of American Express Contracts are not an exhaustive list and are referenced in hierarchical order:

- **Master Agreement:** A Contract which contemplates a long-term relationship with a third party. Master Agreements contain legal terms and conditions required to establish the rules of engagement with the Third Party. Master Agreements include Master Services Agreement, Master Agency Agreement, Master License Agreement, and Master Hosted Services Agreement among other types of agreements. Commercial terms and ongoing purchase of goods or services are typically covered in separate SOW, Exhibits, or like-documents as described below
- **Exhibit/Statement of Work (SOW):** A SOW which may also be referred to as an Exhibit, Work Order, Schedule, or other equivalent term, typically covers the commercial terms and conditions of the service to be provided by a Third Party and details the specific goods or services to be provided to one or more American Express business units (BUs), or function within a given Affiliate, as well as other relevant information including performance standards applicable to the service(s) provided. Exhibits or SOWs are generally appended to executed Master Agreements.
- **Purchase Order** A Contract with a third party which states key terms of the purchase transaction, generally including commodity description, price, quality, quantity, shipping terms, delivery terms, and any special agreements. A Purchase Order may be issued standalone, or as a subsidiary document under another Contract, such as a Master Agreement or SOW. A variety of processes or systems may be used for Purchase Order issuance, e.g., Ariba, or Oracle.
- **Service Level Agreement:** A Service Level Agreement (SLA) refers to a duly executed contract by American Express with a third party that details the associated performance standards. SLAs may be specified in one or more separate Exhibits of a Master Agreement. In some instances, an SLA could also be included the Master Agreement.

Contract Amendment: A change to an existing agreement (of any type) where both parties mutually agree to modify the terms. This may include adding additional services, changing existing services or modifying service levels, extending the term of the agreement, or modifying legal terms.

Findings: Risks identified during due diligence and ongoing monitoring of a Third Party when the Third Party's control environment does not meet AXP's control expectations. Findings also include third-party control or internal operational deficiencies identified during Third-Party Risk Management Quality Assurance reviews. Refer to Section 5: Additional Program Requirements for additional information about the management of Findings.

Risk Designations: A designation provided to each third party based on the significance, risk, and complexity of the engagement with a Third Party. Engagements with Third Parties, and Third Parties can be designated Critical, High, Moderate, or Low risk.

Risk Pillar Subject Matter Experts (SMEs): The control groups across the first and second lines of defense which set expectations and provide oversight for their respective Risk Pillar (defined below).

Risk Pillars: These pillars represent the different types of risk that are present in third-party relationships and are identified in the risk assessment process and managed throughout the lifecycle of Third-Party relationships.

Core Risk Pillars: The Core Risk Pillars represent the three main types of risk inherent to Third-Party relationships. Relative to the TPRM program Core Risk Pillars are used to capture underlying risks elements (Domain Risks) applicable to the good or service. Combined, the risk elements within each Core Risk Pillar, and the aggregation of the three Core Risk Pillars, are used to determine the risk of the engagement.

- Information Security: The risk of adverse events that may occur from third parties that access, process, collect, share, create, store and/or destroy AXP data and/or access to AXP systems.
- Resiliency: The risk of an inability to deliver goods and/or services that significantly impact AXP's ongoing operations or support AXP critical function(s) and/or applications.
- Compliance: The risk that occurs when a Third Party does not have appropriate compliance management processes to ensure adherence to applicable laws and regulations. Note: Relative to determining the risk of the engagement, Compliance represents an aggregation of Domain Risk Pillars as further defined below and covered in the *TPRM Standard*.

Domain Risk Pillars: Represent additional risks that need to be identified and managed for each third-party relationship. Domain Risk Pillars are aggregated into the Core Risk Pillars to determine the risk of the engagement.

- Privacy: The risk of adverse events from Third Party processing of personally identifiable info (PII).
- Anti-Corruption: The risk of corruption arises from offering, giving, receiving or soliciting, directly or indirectly, anything of value in order to gain an undue advantage or influence improper action by another party.
- Sarbanes Oxley Act (SOX): The risk if a third party initiates financial transactions on behalf of AXP or if a third party impacts AXP's financial statements.
- Strategic: The risk from impact to AXP's reputation/brand and risk from social responsibility requirements or when the third party's overall business strategy and goals conflict with AXP's.
- Financial Health: The risk of economic harm because a third party ceases or otherwise limits operations before AXP has realized a benefit from its payment to the third party.

Subcontractor: (Also known as "Fourth Party") An entity contracted by an American Express Third Party that is involved in the fulfillment of contractual obligations or provision of a product and/or service to American Express. The entity's product and/or service relates to or is in support of the services provided by the Third Party to American Express

- **Material Subcontractor:** A Subcontractor who processes American Express Secret or Restricted data; or where a disruption at the subcontractor could impact ability of the Third Party to deliver contracted products or services to American Express or if the Subcontractor is essential to the recovery of the service.

Third Party: A Third Party is an entity which has a business arrangement with American Express and is not otherwise outside of the scope of this Policy.

- **Affiliate:** Affiliates (e.g. TRS, AXP) are any entity that (i) directly or indirectly controls the Bank (e.g., has the power to vote 25% or more of the voting securities), or (ii) is under common control of American Express. Some BUs of American Express may also be referred to as Affiliates in this Policy (e.g.

American Express Technology). Affiliates are managed based on guidance and requirements defined in the *AENB 58 Transactions with Affiliates Policy* and in the *AEMP 57 Transfer Pricing Policy*.

- **Non-Affiliate:** External third party with a business arrangement directly or indirectly, through an Affiliate, with American Express.

Critical Third Party: A Third Party is designated "Critical" when: (i) the Business Impact Analysis (business process criticality) which takes in to consideration whether the services are not repeatable and are material and/or critical in supporting a core business processes such as authorizations, payments and remittance, settlements, funds availability and support (servicing, fulfillment and technologies); and (ii) the service may potentially have significant impact to the organization, operations or customers if the service is interrupted or there is a need to find an alternative to the Third Party. A Third Party can also be designated "Critical" at management's discretion for strategic reasons. Refer to the *TPRM Standard* for detailed criteria and methodology to determine risk designations.

Third-Party Engagement: The goods, services, functions, tasks, operations, and jobs provided to American Express by a Third Party under one contract (SOW, Purchase Order, Quote, etc.).

Third-Party Relationship: The interaction or arrangement between American Express and a Third Party which may involve one or more engagements spanning across Business Units and/or Company affiliate as well as any subcontractor/fourth-party arrangements for the purposes of risk aggregation.

4.0 ROLES & RESPONSIBILITIES

First Line of Defense: The first line of defense ("first line") sets and is responsible for the third-party management expectations, executing risk management practices, and managing compliance to, and execution of the Policy. The first line should take responsibility and be held accountable for effectively managing risks associated with their activities and manage the day-to-day execution of the program.

The first line will work toward constant improvement of the program and will adopt program changes to bolster its effectiveness and incorporate risk management best practices. The following functions are collectively considered part of the first line of defense:

Business Units (BUs):

- **Third-Party Relationship Managers (TRMs)** –TRMs identify product and service risks and enable American Express to manage risk and performance of third parties. TRM responsibilities also include adherence to *TPRM Standard* based on risk designation.
- **Engagement Owner** – Acts as the BU sponsor of the engagement with the third party and formally assumes ultimate accountability for the risk. The Engagement Owner is responsible for key decisions regarding third parties, such as approving Risk Acceptances and contracting based on risk level.
- **BU TLM Lead** – Appointed individual(s) which serve in a dedicated or designated capacity to manage third-party oversight; coordinate engagement ownership; and drive accountability across each BU. Key responsibilities of the BU TLM Lead include approving the inherent risk assessment and management plan, ensuring management plan adherence, assisting in exit and replacement planning, and timely termination of third parties from the inventory.

- **Operational Excellence (OE) Lead** – Oversees and manages the escalation of third-party risks within the BU and is accountable for adherence to risk strategy, including risk acceptance approvals demonstrating alignment with mitigating controls.
- **Executive Relationship Owner** – Senior leader designated to acts as the single AXP point of escalation across BUs for a given American Express' Critical Third Party.
- **Alternate Practices Owner:** The person or team responsible for the management of an engagement or relationship aligned to an Alternate Practice service. Responsibilities include documentation of the process to manage the category in accordance with *Alternate Practice Standard*, ensuring appropriate management throughout the Third-Party lifecycle including but not limited to a service risk assessment, and maintaining a current inventory of owned Alternate Practice engagements or relationships and ensuring appropriate data/reporting into the Third-Party Risk Management function for within the Alternate Practice category on an ongoing basis.

Global Supply Management (GSM):

- **Strategic Sourcing & Business Enablement (SS&BE)** – Works closely with BUs on category strategy, sourcing, business negotiation, and contract execution with respect to specific Third-Party categories. This group is accountable for the Third-Party selection process for those specific service categories, including partnership with TLM Operations to execute risk management requirements, consideration of risks applicable to contract terms.
- **Third-Party Lifecycle Management Operations (TLM Ops)** – Works with BUs in an advisory capacity for new and existing third-party relationships along the phases of the third-party lifecycle including planning, due diligence and third-party selection, ongoing monitoring and termination. Additionally, the Operations team owns technology capabilities and operational enablement of the program.
- **Third-Party Risk Management (TPRM) Function** – Responsible for ensuring appropriate program strategy, operating effectiveness, and risk reporting of the third-party portfolio to support identification, measurement, monitoring, and management of third-party risks within current regulatory guidance. TPRM is accountable for issue escalation to senior management and the board specific to aggregate and concentration risks. Additionally, TPRM ensures the ongoing operating effectiveness of the program execution through a quality assurance program over the scope of the Policy.
- **Third-Party Lifecycle Management Center of Excellence (TLM COE) –** Refers to the collective responsibilities between TLM Ops and TPRM relative to governing the process to manage risks associated with Third Party Relationships.
- **Payment Strategy & Operations (PS&O) –** Function in GSM responsible for issuing payments on all external expenditures incurred by American Express, including but not limited to, contract payments, purchase orders, invoices, sponsorships, quotes, and statutory payments among other spend commitments.

Risk Subject Matter Experts (SMEs): Risk SMEs are also separated into lines of defense. Both lines of defense have roles and responsibilities relative to the management of Third Parties. As part of the first line of defense, SMEs are accountable for establishing and maintaining risk management requirements applicable to their specific risk discipline and for supporting the implementation of standards relative to their specific area in an efficient and effective manner.

Affiliate Management: The teams within the banks and AXP responsible for the management and oversight of Affiliates that provide products and services to the Company. Responsibilities include due diligence, contracting, ongoing monitoring and data/reporting. Management requirements of Bank Affiliates are defined within the *AENB10: Vendor Management* and *AEMP57: Transfer Pricing Policies. Management* of AXP Affiliates is defined within the *AEMP57: Transfer Pricing Policy.*

Second Line of Defense: The second line of defense ("second line") within Global Operational Risk and Oversight (GORO) oversees risk-taking activities and assesses risks and issues independent of first line teams. The second line of defense establishes and monitors the Risk Appetite Framework (RAF) from the *AEMP50: Enterprise Risk Management Policy* to provide an independent assessment, along with credible challenge, to third-party processes, policies, standards, and oversight. The second line is responsible for identifying and assessing risks which may adversely impact American Express in the absence of proper controls, as well as monitoring the internal and external landscape to identify emerging risks, for inclusion in the first line risk mitigation framework.

Risk Subject Matter Experts (SMEs): Risk SMEs are also separated into lines of defense. Both lines of defense have roles and responsibilities relative to the management of Third Parties. As part of the second line of defense, Risk SMEs are accountable and responsible for oversight of process risk design and effectiveness in their respective risk area.

Vendor Risk Oversight (VRO): VRO is a second line of defense for TPRM. VRO is an independent risk management group which seeks to minimize operational risk vulnerabilities by overseeing third-party controls and ensuring monitoring mechanisms are effective. This is done through oversight activities within the Bank and BUs and generally includes ongoing monitoring and validation activities.

Third Line of Defense: The third line of defense ("third line") is the Internal Audit Group (IAG) which provides an independent review and objective assurance on the quality and effectiveness of the first and second lines of defense with respect to risk management, controls, and the risk governance framework for third parties in accordance with *AEMP 68: Internal Audit Policy.*

General Counsel's Organization (GCO): Provides legal advice and guidance with respect to legal requirements related to third party risk management and the contracting process.

Board of Directors of American Express: The Board of Directors of American Express is ultimately accountable for providing oversight to help ensure that the Company's processes for managing third-party activities are conducted in alignment with strategic and business objectives, in a safe and sound manner, and in compliance with applicable laws and regulations. This Policy shall be approved by the Board of Directors (which may act through a committee designated as an executive committee of the Board for this purpose).

- **Risk Committee of the Board of Directors (RC):** The RC consists of independent directors consistent with regulatory and industry requirements and reviews the adequacy of resources of the Company's risk management functions along with the Chief Risk Officer. Governance responsibilities of the RC can be found within the RC Charter.

Management Committees:

- **Enterprise-Wide Risk Management Committee (ERMC):** The senior-most management committee for risk management. The mission of the ERMC is to maintain and continuously improve risk management controls and processes to enable profitable growth, deliver outstanding customer service, and contain adverse risk-related events. Critical third-party approval escalations to the Board of Directors (or Board Committee) are first approved by the ERMC.

- **Operational Risk Management Committee (ORMC):** The ORMC implements and maintains an operational risk management framework and provides cross-functional perspective in order to increase effectiveness of operational controls.

- **Third-Party Risk Management Committee (TRMC):** The TRMC is a subsidiary committee of the ORMC which operates with concurrent AENB and Enterprise scope. The TRMC assists management and the Board through governance and oversight related to the maintenance and improvement of third-party management controls, in line with industry standards and regulatory requirements.

  The TRMC is responsible for defining the overall strategic focus and prioritization of the third-party management program and ensures effective processes are in place to manage risks. The TRMC reviews third-party risk exposures through ongoing reporting and escalations and makes recommendations, as appropriate, to the ORMC and the ERMC.

5.0 POLICY REQUIREMENTS

Third-Party Lifecycle: When American Express engages with Third Parties, the procurement and management of goods and services follow a continuous management lifecycle and the relationships with these Third Parties are managed according to their respective level of risk and complexity. Furthermore, this Policy applies to the establishment of new contracts between American Express and Third Parties, as well as renewals, extensions, or amendments of existing contracts. While both Non-Affiliate and Affiliate relationships are subject to oversight requirements, there may be specific differences in how Affiliates are managed, which are detailed in the TPRM Standard. The third-party management lifecycle process is comprised of two distinct phases:

- **Pre-Contract Phase:** The primary goal of the pre-contract phase is to plan for, identify and assess the risk of a third-party business arrangement and to negotiate a contractual arrangement with the selected third party(s) while aiming to achieve American Express's business objectives.

- **Post-Contract Phase:** The primary goal of the post-contract phase is to conduct ongoing monitoring activities to effectively oversee the Third-Party relationship, including risk and performance management. Additionally, part of the Post-Contract Phase, includes safe and sound termination and offboard of the Third Party when delivery of goods or services conclude or are no longer needed.

To ensure effective Third-Party risk management the pre and post contract phases are further segmented in five sub-phases that span across the lifecycle of Third-Party relationships. The specific tasks and requirements of each of the five phases are further defined in the *TPRM Standard* and the *Procurement Standard*. The following section describes the activities within each of the phases.

Contract Phase		Description of Activities
Pre-Contract	**I. Planning**	The Planning phase initiates when Business Units identify the need to engage a Third Party for a business arrangement including but not limited to procuring new goods or services, or to change or extend an existing engagement. As part of this phase, Business Units evaluate the benefits and disadvantages as well as the ability and capacity to engage a Third Party. A key step in this evaluation is consideration of Third Parties and services in the Approved Supplier List (ASL) which includes Third Parties that have previously been risk assessed. In addition, the Business Units engage Global Supply Management (GSM) to find and evaluate Third Parties that can fulfill the business need. Business units are required to have a completed a Service Risk Assessment (SRA) approved by the engagement owner any third-party engagement. This is applicable to all service categories and may be confirmed via GSM or Third-Party Risk Management per respective Standards.
	II. Due Diligence & Third-Party Selection	In the Due Diligence and Third-Party Selection phase, Business Units work with GSM to evaluate options to address their need considering the risk and complexity of the activity. Third Parties are evaluated through various procurement channels such as Sole Sourcing, Request for Proposal (RFP), Purchase Order (PO), among others. For certain Third-Party categories, in the event of procurement through an RFP, Business Units work with GSM to review proposals and select a Third Party. Third-Party selection is based on the overall value proposition. Among the things considered during selection are capacity to meet the specified requirements, best position to meet the business objectives, and ability to deliver the product or services in a safe and sound manner. An important consideration during the selection of a Third Party is the Third Party's willingness to accept an American Express B2B payment product. Upon selection of the Third Party, Business Units continue the Risk Assessment initiated in the Planning Phase, by incorporating information about selected Third Party in the Third-Party Risk Assessment (TRA). The TRA consists of a series of questions triggered based on responses to the SRA that capture information about the Third Party and any Subcontractors ("Fourth Parties") that will be used to fulfill the contractual obligation to American Express. Responses to the TRA, also determine controls applicable to the good or service, and the control documentation the Business Unit and the selected Third Party must provide as part of the due diligence process to demonstrate sound practices and adequate risk management. Due diligence activities typically include performing an assessment of the Third Party's controls relevant to the risks of the product or service. Evidence of the Third Party's controls is collected and measured against AXP's control expectations and risk appetite. If the required Third-Party controls fail to meet AXP's control expectations, these failures are documented as "Findings" that must be addressed prior to executing a contract. Failure to meet AXP control expectations may result in cancellation of the engagement with the potential Third Party. Depending on the type of Third-Party relationship, Business Units can proceed with the engagement by documenting a remediation plan or accept the risk associated with the selected Third Party as outlined in the *TPRM Standard*. The Risk Assessment of the proposed activity along with results of the evaluation of the Third Party's control environment determine the Residual risk of the engagement. Additionally, activities in the Due Diligence phase result in identification of risks that may need to be documented in the contract with the Third Party to determine responsibilities over these risks. To conclude this phase, the Business Units evaluates the risk of the engagement and the results of the due diligence to outline a plan to manage the engagement and the relationship with the Third Party through the entire lifecycle. Furthermore, depending on the risk of the engagement, the Business Unit may be required to document a plan to manage an eventual

		termination or replacement of the engagement with the Third Party. Relative to commercial terms of the engagement, during this phase the busines identifies measures to monitor delivery of services and determines.
	III. Contract Negotiation	The Contract Negotiation phase culminates pre contract activities. In this phase of the lifecycle, the risks identified during Due Diligence determine contractual requirements and negotiation strategy. To ensure favorable terms, GSM or the General Counsel's Organization (GCO) negotiate the legal, regulatory, and commercial terms and conditions of the relationship with the Third Party on behalf of the Business Units. A fully executed Contract or Purchase Order approved by SS&BE is required before a Third Party may begin to provide products and/or services. Contracts with Third Parties include, to the extent applicable, language for scope, timeline, responsibilities, assumptions, regulatory expectations, SLAs, Subcontractors, customer and information protection, fees, incentives, payment terms, termination, limitations of liability and indemnification. In instances where Findings are identified during due diligence, additional terms and conditions may be required in the Contract. For instances where the selected Third Party agrees to accept payment for goods or services using American Express B2B products, contract terms generally require acceptance of payment using an American Express payment product as a condition of doing business and Third Parties are required to complete an application to accept American Express payment cards. The Contract Negotiation Phase of the lifecycle concludes when a contract between American Express and a Third Party is executed. As previously mentioned, for SS&BE managed categories, only SS&BE has the authority to approve the execution of Contracts. For service categories managed outside of SS&BE, Contracts may be executed only by a colleague who has been authorized to do so by the Corporate Secretary's Office. Also, a colleague may only sign after relevant Business Unit leader approvals have been obtained per *AEMP 01 External Expenditure Authority Approval Policy*. Contracts negotiated by GSM are stored in a central contact repository. For contracts that are not negotiated by GSM, the Business Units should consult with GCO to ensure the contract is stored according to Records Management requirements.
Post-Contract	**IV. Ongoing Monitoring**	Ongoing Monitoring is the most extensive phase of the lifecycle as it encompasses management, monitoring, reporting, and if necessary, escalation of the Third Parties performance against contract terms and risk management requirements. During this phase, Business Units oversee the business arrangement and issue payments corresponding payments. In this phase, Busines units execute monitoring activities that are based on the risk and complexity throughout the duration of the Contract term to ensure risks associated with the engagement continue to be properly identified and managed and ensure the Third Party is adhering to the agreed-upon Contract terms. Examples of ongoing monitoring activities may include reconciliation of payments made for the service, tracking, and reporting of performance SLAs, risk metrics, oversee financial stability, review of audit reports, and address issues. Additionally, Business Units are required to re-assess the risk of the service on a frequency which is based on the risk designation of the engagement. Following re-assessment and validation of the risk, Risk SMEs may re-evaluate the Third Party's control environment. Other monitoring activities include identification of emerging risks and adverse events such as data breaches, maintenance of Business Continuity plans, and review and update of Exit Strategies and Management Plans. Critical Third-Party relationships require heightened monitoring requirements such as periodic business reviews and reporting to Management

		Committees and or Board of Directors. Ongoing Monitoring requirements are further outlined in the *TPRM Standard*.
	V. Termination	The Third-Party Lifecycle Management concludes when the Third-Party stops providing the goods or services to American Express. Termination of engagements can occur when the services conclude as planned, when the services provided by the Third Party have a defined purposes and expiration timeline, or prematurely due to poor performance, breach of contract, or because the services are no longer beneficial to either party. The Third-Party engagement undergoing termination may be transitioned to an alternative Third Party, transitioned in-house to AXP, or discontinued entirely. After making the decision to terminate the engagement, and if applicable, the relationship with the Third Party, Business Units engage GSM or GCO to initiate termination activities. During the Termination Phase, Business Units execute activities to ensure that the engagement terminates in an efficient manner. Depending on the risk and complexity of the engagement, Busines Units may execute a previously documented plan to transition or terminate the services. Engagements in which the Third Party has access to AXP data or systems, Business Units ensure retrieval or destruction of data and assets. For services that involved access to AXP systems, Business Units engage Information Security SMEs to ensure decommission of access. Certain relationships have specific termination requirements defined in the contract such as retrieval of intellectual property or release of source code in escrow accounts. For such terminations the Business Units work in close collaboration with GCO and GSM to ensure terminations occur according to contract requirements. An important step in the termination phase entails de-activation of any automatic payment directives or billing settlements previously scheduled with the Third Party.

Additional Program Requirements which span the end-to-end Third-Party Lifecycle:

Findings Management: The process to manage potential risks identified throughout the third-party lifecycle which details the requirements for disposition, resolution, reporting, escalation, and approvals needed to resolve the risks. Findings can be addressed in one of the following two ways:

- **Risk Extension:** Is a plan to remediate Findings identified during due diligence or ongoing monitoring activities by implementing a control to address the risk at a future date. Risk Extensions include implementation of the required control to address the risk with a specific remediation date that is monitored and tracked to closure.

- **Risk Acceptance:** Is a documented acceptance of the risk resulting from the Findings identified during due diligence or ongoing monitoring activities which cannot be remediated by the third party or the Business Unit is unable to remediate due to extenuating circumstances after attempted collection. Risk Acceptance requires approval as defined in the *TPRM Standard*

Engagement of a Critical Third Party: Critical Third Parties require heightened management and oversight given the importance to the Company. Prior to engaging and during the engagement with a Critical Third Party, Board, or Board Committee, review and approval is required. Reviews include but are not limited to:

- Contract Terms (new, changes, extensions, or renewals)
- Summary of due diligence results
- Disposition of Findings

- Risk Acceptances
- Summary of ongoing monitoring results
- Management actions to address significant deterioration in performance or address changing risks or material issues identified through Ongoing Monitoring
- Terminations of Critical Third-Party relationships

Alternate Practice: Third Parties providing services in these specific categories are managed in adherence to the *Alternate Practice Standard* and are subject to review for operating effectiveness by Third-Party Risk Management. General requirements for the Alternate Practice categories are as follows:

Alternate Practice Third-Party Relationship Inventory: Business Unit must report new or terminated relationships for Alternate Practice service categories to TPRM within 30 calendar days of service start date. Business Units must maintain accuracy of their inventory which is subject to validation by TPRM.

Alternate Practice Service Risk Assessment: Business Unit must complete and submit to TPRM a service risk assessment, at least annually, for each Alternate Practice service used by the business.

Business Unit Alternate Practice Procedure: Business Units must have a documented procedure aligned to lifecycle risk management requirements specified in this Policy and the corresponding Standards inclusive of timely reporting of current Third-Party inventory to TPRM.

Alternate Practice Category Approvals: Business Units must work with TPRM to determine if Alternate Practice is the most effective way to manage the risk. Documented approval must be obtained from the Vice President Third-Party Risk Management to introduce a new Alternate Practice service category or transition an Alternate Practice service category to be governed by the TLM program.

Third-Party Inventory: American Express must maintain a complete inventory of Third-Party relationships. The inventory must be readily accessible with complete and accurate third-party information. The owner of the respective listings must provide an attestation for the completeness and accuracy which includes the following:

- The listing of in-scope Affiliate relationships is maintained by the Corporate Secretary's Office
- The listing of Third Parties managed through Alternate Practices are maintained Alternate Practice Owners
- The listing of the remainder Third-Party relationships maintained by GSM

Third-Party Documentation Requirements: American Express maintains third-party documentation and records, as applicable, based on defined requirements consistent with third-party specific management requirements and in accordance with the *AEMP08 Global Records Management Policy*. Applicable requirements include but are not limited to:

- A master list of Third-Party relationships
- Approval to engage a third party

- Due diligence results, findings, and recommendations
- Copies of executed contracts and related amendments
- Meeting minutes from third-party interactions, which are required quarterly for Critical, semiannual for High and annually for Moderate risk services
- Regular risk management and performance reports required and received from the third party
- Regular reports to the Board, or Board Committee, and senior management on the results of internal control testing and ongoing monitoring of Critical Third Parties.
- Regular reports to the Board, or Board Committee and senior management on the results of independent reviews of American Express's overall risk management process.

Program Health Metrics Program Health Metrics should be defined and monitored on an ongoing basis to ensure the third-party management program and accountable parties are operating effectively against the goals and expectations. An example of a Program Health Metric may include AXP's measurement against the Risk Appetite Framework or program effectiveness as an output of Quality Assurance.

Aggregate Risk: Aggregation is a summation of relevant factors to drive risk management attention towards the highest risk areas. The program must aggregate risks at the service, third party and portfolio (concentration) levels to effectively determine due diligence requirements, ongoing monitoring requirements and to maintain regular reporting on risks.

- Service Risk Aggregation: The aggregation of inherent or residual risk of two or more engagements with the same Third Party to enable efficient and holistic ongoing monitoring.
- Third-Party Risk Aggregation: The aggregation of characteristics, attributes, or risk exposures of two or more engagements or Third-Party relationships for a holistic view of risk

Concentration Risk: Risk that considers third-party relationships collectively to drive transparency to risk exposure due to lack of diversification. Examples of concentration risk may be based on third-party usage, spend, service dependency, geographic, or Subcontractors. Thresholds must be defined for each applicable category to mitigate risk concentrations. Concentration risk must be considered when approving Critical engagements or relationships as well as regular reporting for monitoring across services.

Quality Control (QC): QC is an in-process control to ensure consistent application of standards, compliance with laws and regulations, and adherence to policies and procedures. QC seeks to significantly reduce or eliminate errors before they become systemic issues or have a negative impact on AXP's operations. QC review should be conducted concurrently with AXP activities and may be performed internally or outsourced to a Third Party.

Quality Assurance (QA): QA verifies established standards and processes are followed and consistently applied. The QA review should be performed after an activity is completed by an objective party. The results of the QA review are used to assess the quality of AXP's policies, procedures, programs, and practices in specific businesses. Additionally, results enable identification of operational weaknesses, risks associated with specific businesses, training needs, and process deficiencies.

Independent Review: Independent reviews must be conducted periodically on the TPRM program is conducted by the second line of defense as defined in the *AEMP66 Global Risk Oversight Policy* and the *AEMP50 Enterprise Risk Management Policy*.

Training and Communication: American Express must provide AEMP10 training and communications, as needed, to colleagues engaged in the third-party lifecycle. Training should provide colleagues a foundational understanding of AEMP10.

6.0 EXCEPTION/CONFLICT/INTERPRETATION RESOLUTION

Escalations: Escalations due to deviations from this Policy must follow the process defined in the TPRM Standards. When the Policy or corresponding Standards are not adhered to and program requirements are not executed as defined in this Policy, there must be timely escalation to Third-Party Center of Excellence function within GSM who will evaluate the escalation and coordinate evaluation of the matter with applicable Risk Pillar SMEs or applicable risk committees, as defined in the TPRM Standards.

When a risk appetite metric exceeds its risk escalation threshold, the responsible Business Unit and the Global Operational Risk Oversight (GORO) teams must follow the RAF escalation procedures outlined in *AEMP50: Enterprise Risk Management Policy*.

Successive escalations of the same metric to the ERMC/RC can be suppressed for the following three months but are included in risk reporting if the Global Head of Operational Risk and Oversight and Chief Risk Officer (CRO) determine the root cause for the escalation remains the same. Additionally, risk appetite metrics monitored quarterly are escalated only once per quarter.

Process Exceptions and Approval Matrix: Requests for exceptions to this Policy must be documented with the reasons for the exceptions clearly identified and submitted to the Policy Custodian who is to consult the Policy Sponsor and GCO as necessary. Under extraordinary circumstances, completion of the requirements of this Policy may be postponed or exempted with approval from both the Chief Procurement Officer (Policy Sponsor) and the Chief Risk Officer to allow for engagements with Third Parties

Any questions regarding interpretation of this Policy should be directed to the Policy Custodian. For any matters of direct consumer compliance impact, the Policy Custodian works directly with the Policy Sponsor and with the Chief Compliance Officer or his/her designee for engagement, interpretation, and resolution. The Policy Sponsor reports any exceptions to this Policy to the TRMC or another applicable committee, as necessary, and exceptions must be approved by the Policy Sponsor.

7.0 POLICY APPROVAL REQUIREMENTS

This Policy is to be reviewed and approved by the Company's Board, or Board Committee, at least once annually and not more than 14 months from the approval date. Substantive revisions are approved by the Board, or Board Committee. Compliance and GCO are engaged when changes to this Policy occur to ensure consideration is given to the Company's legal inventory which is part of the Company's compliance risk assessment methodology.

8.0 ENFORCEMENT OF ISSUED POLICIES, STANDARDS, AND PROCEDURES

Procurement of goods and services for the Company must be conducted in adherence to all the requirements of this policy and applicable Standards to ensure proper documentation of the transaction, fiscal responsibility, ethical behavior, adherence to applicable regulations, and compliance with associated policies. In general, procurement of goods and services from Third Parties entails completion of one or more of the following activities:

- Purchase from the local online purchasing application (Ariba or Oracle)
- Purchase using an American Express Supplier Payment Product, such as, but not limited to, Buyer Initiated Payments (BIP), Corporate Purchasing Card (CPC), or vPayment (vPay)
- Purchase using an American Express Corporate Card in adherence *AEMP 26 Global Travel, Meetings, and Expense Policy*
- Early engagement of SS&BE or GCO prior to negotiations with the Third Party
- For new contracts, or renewal, extension, or amendment of existing contracts with a Third Party in the Categories defined in *Appendix 1*:
  - Risk assessment of the good or service
  - Due diligence on the selected Third Party
  - SS&BE and/or GCO negotiated legal and commercial terms as applicable

All colleagues are responsible for complying with the requirements of this Policy and associated Standards. To assure the effectiveness of the controls specified in this Policy, GSM performs regular Quality Control, Quality Assurance, and Control Testing of the processes involved in the management of Third Parties. **Noncompliance with this Policy or associated Standards and Procedures constitutes bypass as defined in Section 3 and is a breach of the terms of employment which may lead to disciplinary actions up to and including termination of employment, or termination of a Third-Party agreement.**

9.0 POLICY IMPLEMENTATION

The Requirements of this Policy are in effect as of January 21, 2022, for new and existing Third-Party relationships for all risk designations.

Implementation of **Alternate Practice** requirements will continue through ***July 1, 2022***. Until full implementation of this process, Third-Party engagements in the service categories in-scope for Alternate Practice will continue to manage third-party risk management requirements aligned with Third Party Risk Management.

10.0 RELATED POLICIES, REGULATORY GUIDELINES & SUPPORTING DOCUMENTS

This Policy is supported by applicable American Express Company policies available on The Square. Key supporting policies include but are not limited to:

Related Policy / Guideline	Reference in AEMP 10 (*i.e.*, this Policy) and Summary Explanation
• AEMP 01, External Expenditure Approval Authority	• Section 5.0, provides requirements for the third-party lifecycle and contracting
• AEMP 08, Global Records Management	• Section 5.0, describes documentation requirements for in-scope third-party relationships
• AEMP 37, Controlled Entity Governance, and AEMP 40, Merger & Acquisition Deal Approval	• Section 2.0, states that Joint Ventures are in scope for this Policy when providing products or services to American Express. • Section 2.0, states that Mergers & Acquisitions are out of scope for this Policy
• AEMP 47, Operational Risk Management	• Section 4.0 describes to roles of ERMC and ORMC in relation to third-party management
• AEMP 50, Enterprise Risk Management	• Section 5.0, specifies independent review requirements as part of the third-party lifecycle management program and Section 6.0, describes the escalation framework and risk escalation thresholds
• AEMP 57, Transfer Pricing	• Section 2.0, outlines scope for this policy and Section 3.0, provides the definition of Affiliate
• AENB 58, Transactions with Affiliates	• Section 3.0, provides the definition of Affiliate
• AEMP 62, Legal Entity Governance	• Section 3.0, provides the definition of Affiliate
• AEMP 66, Global Risk Oversight	• Section 5.0, specifies independent review requirements as part of the third-party lifecycle management program

The following policies / procedures are considered complementary to AEMP 10:

- Third-Party Risk Management Standard
- Alternate Practice Standard
- Third-Party Lifecycle Management Operating Procedures including Ongoing Monitoring
- Strategic Sourcing & Business Enablement Procurement Standard and Procedures
- Accounts Payable Standard
- American Express Code of Conduct
- AENB10 – Third-Party Management Policy and AENB58 - Transactions with Affiliates Policy of the U.S. Bank
- Relevant Third-Party management policies and procedures of other regulated legal entities of American Express, such as the American Express Services Europe Limited and American Express Payment Services Limited Outsourcing Management Policy, American Express Advanced Services Europe Limited Outsourcing Policy, etc.
- Relevant supporting Standards including but not limited to the Third-Party Risk Management Standard, Procurement Standard and Affiliate Standard.

Examples of applicable regulatory guidance includes:

- Office of Comptroller of the Currency (OCC) Bulletin 2013-29: Third-Party Relationships: Risk Management Guidance
- Federal Deposit Insurance Corporation (FDIC) FIL-44-2008: Guidance for Managing Third-Party Risk
- Consumer Financial Protection Bureau (CFPB) Bulletin 2016-02: Service Providers
- Federal Regulatory Agencies' Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers
- Federal Financial Institutions Examination Council (FFIEC): Supervision of Technology Service Providers
- Federal Reserve Board (FRB): SR 13-19: Guidance on Managing Outsourcing Risk
- International regulatory guidance such as the European Union Payment Services Directive, European Banking Authority (EBA) Guidelines on Outsourcing Arrangements, Payment Services Regulations, Electronic Money Directive, and Electronic Money Regulations, as well as relevant guidance published by the Reserve Bank of Australia, Bank Of Canada, Reserve Bank Of India, Banco de Mexico, Banco Central De La República Argentina, Modern Slavery Legislation (e.g. UK Modern Slavery Act, Australia Modern Slavery Act, etc.) and others.

11.0 REVISION HISTORY

This version of AEMP 10 supersedes the previous version, published on January 22, 2021. The changes from the previous version include:

Section in Policy	Update to AEMP10
Overview and Purpose	Enhanced language in the overview section to discuss reasons for engaging Third-Parties and included definition of "Third Party" to familiarize the reader with the different terms used for Third Parties. Sharpened language in the purpose section to articulate overall objective of the policy.
Scope	Simplified language clearly articulates the scope of the policy and further define that types of Third Parties the policy applies to.
Key Definitions	Sharpened language for most of the defined terms in this section. Introduced definition for three terms not previously defined and deleted terms defined in corresponding Standards.
Roles & Responsibilities	Improved description of the roles involved in the management of Third Parties and introduced three new roles in the first line of defense to reflect current operating model.
Policy Requirements	Updated description of lifecycle phases to eliminate procedural language and content discussed in the Standards. Updated general guidelines relative to Alternate Practice and changed structure of the section to delineate program execution requirements from program governance requirements.
Exception / Conflict / Interpretation Resolution	Minor updates to enhance description of requirements relative to escalation of Policy exceptions, conflicts, and interpretation.
Policy Approval Requirements	No changes to this section
Enforcement of Issued Policies, Standards, and Procedures	Significant update to this section to further define what constitutes non-compliance with the policy and consequences for bypassing its requirements.
Policy Implementation	Updated to reflect policy requirements are in effect given risk-based implementation is complete. Included guideline to manage categories in-scope for Alternate Practice until full implementation of the process.
Related Policies, Regulatory Guidelines & Supporting Documents	Updated references to include associated Standards and regulatory guidelines issued prior to publishing of the policy.
Appendices	Deleted Appendix 1 as the content will be covered in the TPRM Standard. Also deleted Appendix 2 which contained the previous version of the policy.
Revision History	Simplified language clearly articulates the scope of the policy and further define that types of Third Parties the policy applies to.

12.0 APPENDICES