Third-Party Lifecycle Management 2.0.

Third-Party Risk Assessment (TRA)

Guidance

Abbreviation Glossary

AEMP – AXP Management Policy

AXP – AXP Company

API – Application Programming Interface

BBB – Better Business Bureau

BFL – Business Function Location

BIA – Business Impact Analysis

BST – Business Self-Testing

CBF – Critical Business Function

CEG – Colleague Experience Group (HR)

COE – Center of Expertise (Excellence)

COERA – Center of Expertise (Excellence) Risk Assessment Report

CSOC – Complementary Subservice Organization Controls

CUEC – Complementary User Entity Control

DD – Due Diligence

DPIA – Data Protection Impact Assessment

EDA – Enterprise Digital Analytics

EPCC – Enterprise Privacy Choice Capability

FCPA – Foreign Corrupt Practices Act

FSRA – Financial Statement Risk Assessment

GCO – General Counsel Organization

GMS – Global Merchant Service

GNICS – Global Network and International Card Services

GNO – Global Network Operations

GNP – Global Network Partnership

GSM – Global Supply Management

ICFR – Internal Control over Financial Reporting

IPCR – Information Protection Contract Requirement

IRA – Inherent Risk Assessment

ITGC – Information Technology General Controls

LOBCO – Line of Business Compliance Officers

MCO – Market Compliance Officers

MFN – Most Favored Nation

OE – Operational Excellence

OOS – Out of Scope

PAR – Privacy Access Request

PII – Personally Identifiable Info

PRA – Privacy Risk Assessment

PRE-L – Pre-engagement Logical Assessment

PRE-P – Pre-engagement Physical Assessment or Pre-Physical Review

RAQ – Risk Assessment Questionnaire

RTO – Recovery Time Objectives

SAR – Subject Access Request

SDE – Sensitive Data Elements

SLA – Service Level Agreement

SME – Risk Subject Matter Experts

SO – Service Organization

SOE – State-owned or State-controlled Entity

SOX – Sarbanes Oxley Act (if a Third-Party initiates financial transactions on behalf of AXP or impacts AXP's financial statements)

SSO – Subservice Organization

SRF – Service Request Form

SS&BE – Strategic Sourcing and Business Enablement

TPP – Third-Party Processor

TPRM – Third-Party Risk Management

TRA – Third-Party Risk Assessment

TSM – Third-party Security Management

VTA – Vulnerability Threat Assessment

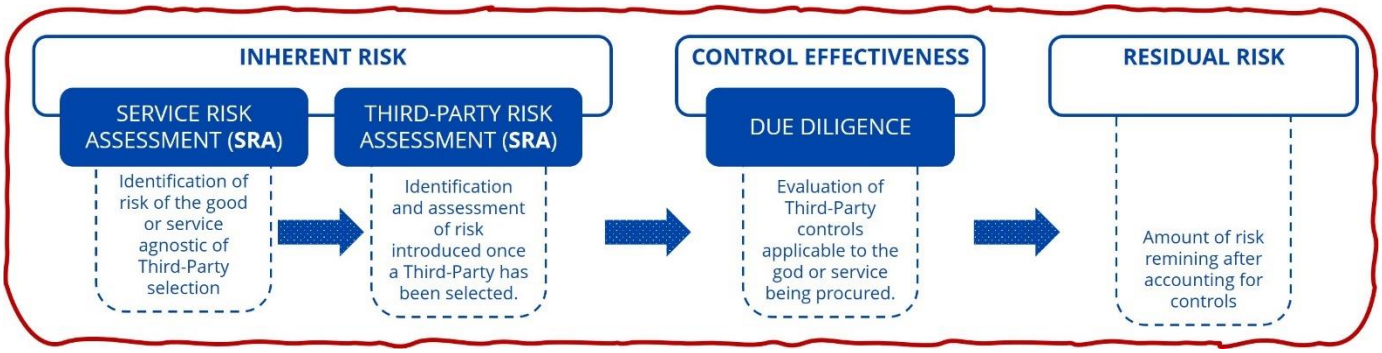
Useful Definitions

Risk Assessment Process (RAP)

The Third-Party Risk Management encompasses the processes to identify, measure, manage, monitor, and report Third-Party Risk. It is designed to set the parameters of a comprehensive and enterprise-wide risk management program to ensure effective management of Third-Party relationships.

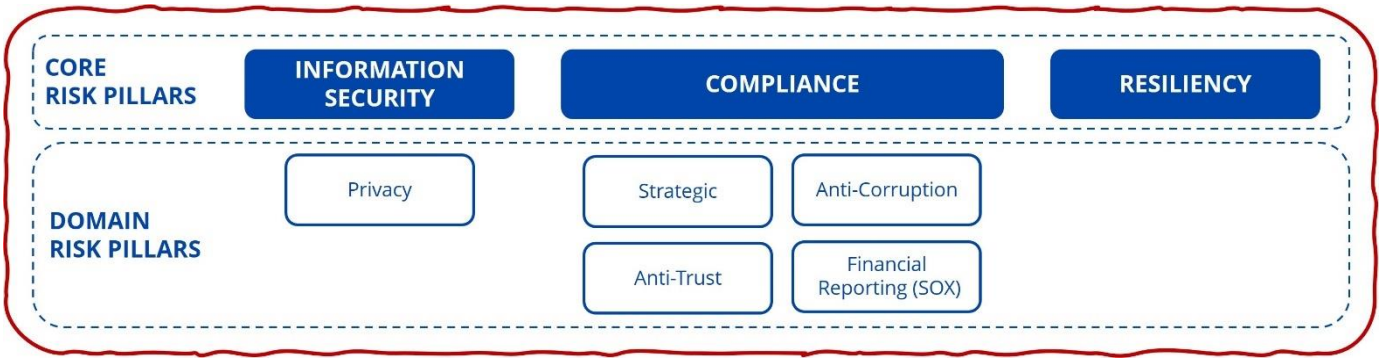
AEMP10 prescribes evaluation of the characteristics of each good or service (engagement) provided by a Third-Party to identify and measure the inherent risk of the activity. Assessing Third-Party Risk involves a sequence of interrelated activities designed to define the good or service being procured, capture its risk attributes, measure the level of risk, determine applicable mitigating controls, and identify unmitigated risk. Each activity within the Risk Assessment Process is made up of individual components that when aggregated enable AXP|PAYBACK to identify and measure risk.

Risk Assessment sequence of activities



Risk Pillars

A fundamental part of the process is identification, measurement, and management of the various risks inherent to Third-Party Relationships. To accomplish this objective, AEMP10 defines **Information Security** and **Technology**, **Resiliency**, and **Compliance** as the CORE RISKS involved when receiving goods or services from Third-Parties. Each of the Core Risk Pillars represent a sub-set of risks that include **Privacy Risk**, **Strategic Risk**, **Anti-corruption Risk**, and **Financial Reporting (SOX) Risk**, are defined as DOMAIN RISKS.



The Core and Domain Risk Pillars are embedded in the RAP and their applicability to a given engagement is captured using questions embedded within SRA and TRA.

Other risks included in the RAP but not considered in the measurement of risk include **Operational**, **Legal**, **Reputational**, **Sanctions**, **Financial**, **Anti-Trust**, **Model**, and **Concentration Risk**.

Risk Pillars definitions

- **Information Security**: The risk of adverse events that may occur from Third-Parties that access, process, collect, share, create, store and/or destroy AXP|PAYBACK data and/or access to AXP|PAYBACK systems.
- **Business Resiliency**: The risk of an inability to deliver goods and/or services that have significance to AXP|PAYBACK's ongoing operations or support AXP|PAYBACK critical function(s) and/or applications.
- **Compliance**: The risk that the Third-Party does not have appropriate compliance management processes.
- **Privacy**: The risk of adverse events from access to Personally Identifiable Info (PII).
- **Legal/Anti-Trust**: The risk of regulatory consequences from potential collaboration or confidential information sharing with a direct competitor that directly limits competition (Anti-Trust risk), or the risk that arises from non-standard clauses or limitations of liability (Contract/Legal Risk).
- **SOX**: The risk that arises if a Third-Party initiates financial transactions on behalf of AXP|PAYBACK or if a Third-Party impacts AXP|PAYBACK's financial statements.
- **Strategic (Reputational)**: The risk from impact to AXP|PAYBACK's reputation/brand and risk from social responsibility requirements or that the Third-Party's overall business strategy and goals conflict with AXP|PAYBACK's.
- **Operational (Process)**: Operational risks that impact AXP|PAYBACK, including but not limited to financial reporting, compliance and operations.
- **Operational (Model)**: The risk of adverse consequences due to fundamental errors within the operational model and/or the incorrect or inappropriate use of the model.
- **Credit (Financial Health)**: The risk of economic harm because a Third-Party cease or limited operations before AXP|PAYBACK has received benefit from the Third-Party.
- **Data Governance/Quality**: The risk of improper management of AXP|PAYBACK data by Third-Parties that may result in an inability to trust critical data and processes for their intended purposes, meet regulatory requirements, and support the development&execution of effective risk management practices.

Risk Pillar alignment to SRA and TRA

SRA (Third-Party Agnostic)	TRA (Includes selected Third-Party)
Core Risk Pillars: Information Security, Resiliency, Compliance	Incremental risk level introduced by outsourcing to a Third-Party. Domain Risk Pillars: Financial Health, Anti-Trust, Model, Reputational, Concentration
Domain Risk Pillars: Privacy, Anti-Corruption, SOX, Operational, Legal: Anti-Corruption, Data Risks	

IRA | Inherent Risk Assessment

Inherent Risk is defined as the amount of risk involved in a process or activity when controls are not in place and is a fundamental piece of TLM. Identifying and measuring Inherent Risk begins with the evaluation of the characteristics of the good or service being procured first captured in the SRA then further defined after selection of the Third-Party in the TRA. Combined, the SRA and TRA are referred to as the Risk Assessment Questionnaire (RAQ), which completion is required for procurement of all goods and services. Reponses to

the RAQ will determine the inherent risk score for outsourcing the function/service and will also define the due diligence required to mitigate the inherent risk.

SRA | Service Risk Assessment

Service Risk Assessment (SRA) is a set of questions intended to measure the inherent risk of performing the function/service.

The SRA is a series of questions designed to identify the existence of risk elements such as access to data, business continuity, interaction with AXP|PAYBACK customers, and compliance with laws and regulations applicable to the good or service being procured. Additionally, responses to the SRA determine the controls required to mitigate the risks associated with the good or service as well as the due diligence documentation is required to evidence these controls.

Completion of the SRA results in a risk score for each of the Domain and Core Risk Pillars identified during the questions. These scores are aggregated to determine the SRA Score (SRA risk rating). Completion of the SRA also generates questions in the TRA.

TRA | Third-Party Risk Assessment

Third-Party Risk Assessment (TRA) is an additional set of questions for outsourcing a service, which may increase the inherent risk, based on the Third-Party selected.

Similar to the SRA, the TRA consists of a series of questions triggered based on responses to the SRA that capture information about the Third-Party and any Fourth-Parties (Subcontractors), which will result in identifying and measuring risks associated with the Third-Party by calculating scores for the Information Security; Privacy; Compliance; Anti-Corruption; Anti-Trust; Sanctions; and SOX. The responses to the TRA determine what due diligence needs to be conducted on the Third-Party.

Overall Assessment Risk

The Overall Assessment Risk is the risk rating assigned to the proposed good or service captured in the engagement and calculated using the output of the SRA and TRA. Once both the SRA and TRA are completed the applicable Domain Risk Pillar scores are added and rolled-up to their corresponding Core Pillar to determine the **Risk Pillar Scores**. The Risk Pillar Scores and then averaged to determine the Overall Assessment Risk represented three risk levels:

- High Risk
- Moderate Risk
- Low Risk

Alternate Practice

The oversight of specific Third-Party relationships which are managed outside the central TLM program. The management of a Critical Third-Party by an Alternate Practice must meet Critical Third-Party management expectations (joint testing, management plan, board reporting, executive owner, etc.).

Third-Party Lifecycle Management 2.0.

Third-Party Risk Assessment (TRA)

Level 2 Questions

TRA is an additional set of questions for outsourcing a service, which may increase the inherent risk, based on the Third-Party selected. For example, factors such as: financial health, where services are provided from, type of Third-Party etc., may impact the inherent risk.

Domain Risk Pillars

The domain risk pillars are individual sub-risk pillars with weighted responses to each question that are calculated to result in a High, Moderate or Low value. Sub-domain pillars can also result in an "out of scope" result (when no risk or DD requirements trigger).

Third-Party Details

Majority of the questions within this section are auto-populated. Only below TP.06 and TP.13 will require your response.

1 **Q# TP.06 | Will this Service involve pre-payment of $1M+ for services to be delivered?**

Response option: YES | NO

2 **Q# TP.13 | Is the Third-Party engaging subcontractor(s) as part of the delivery of services to AXP|PAYBACK that will impact one or more of the following?**

Response option:

- Accesses; Handles; or Stores AXP|PAYBACK Sensitive Data (AXP|PAYBACK Secret & Restricted w/PII)
- They will provide the Same Service as the Contracted Third-Party
- Is a government-controlled Entity or Intermediary of a government-controlled Entity?
- A service disruption could impact the ability of the Third-Party to deliver services (only if BIA Tier is 0, 1, or 2)
- N/A – subcontractors do not impact any of the above options or no subcontractors support the delivery of services.

3 **Q# TP.13.1 | How many Material Subcontractor are involved in providing the requested service?**

Response option:

- 1
- 2
- 3
- 4
- 5 +

Information Security

4 **Q#L2 1.1 | Is the Third-Party one of the following, or is any of the following applicable?**

Purpose: To identify services that are OOS. If any option is selected other than None Apply, the Information Security pillar will become OOS and Descoping Question Validation will trigger (DD IS/IT 10 – IS)

Select appropriate option:

1. A courier service delivering only in sealed tamper resistant closed packages. *Note: If a courier providing more than point services and has access to PII info maintained on their systems; for payment, collection, or delivery then No.*
2. A Third-Party Processor (TPP) that performs actual bankcard transaction processing for a merchant (with no access to AXP|PAYBACK network or systems)?
3. A consulting/contractor arrangement (Uses AXP|PAYBACK Assets only, AXP|PAYBACK ADS IDs and uses AXP|PAYBACK processes) that is NOT Cognizant, Infosys, IBM Export Blue, Syntel, or Tata Consultancy Service (TCS)?
4. An outside counsel law firm with any necessary experts that are engaged and managed by the General Counsel's Office?
5. A fully separated investment in a Joint Venture or Controlled Entity, which are governed by American Express Management Policy (AEMP) 40, Merger and Acquisition Deal Approval and AEMP 37, Controlled Entity Governance, respectively?
6. A treasury counterparty (generally other banks), which are governed by AEMP 52, Enterprise-wide Institutional Credit Risk Management, and AEMP 50, Enterprise-wide Risk Management?
7. An external Business Partner that has executed licensing agreements with American Express Global Network and International Card Services for card issuance, merchant recruitment, or the provision of ATM network – GNS Outsourced Partners only?
8. An Airline & Lodging Membership Reward (MR) Point Transfer Agreement Partners where no more than First/Last Name, Partner Program #, and Points Transferred is being shared?
9. An OPT BLUE program / ONE POINT partners or External Sales Agent (ESA) or Aggregator services where no PII is shared and only Merchant acquisition confirmation is provided.
10. A Point of Sale (POS) installer/servicing vendor where the only data provided is merchant related data that has been classified as LP/AXP Public and/or LP/AXP Internal?
11. An international credit bureau that is Regulator Controlled and/or a Core National Agency?
12. An ICC Bank Partner where services involve Sales/Lead Generations of AXP/bank card application and no additional customer data elements collected on behalf of AXP|PAYBACK and customer information sharing has customer consent?
13. None Apply

5 **Q#L2 1.2 | Where is AXP|PAYBACK data stored as part of the service being provided?**

Purpose: The objective is to ascertain whether AXP|PAYBACK data will be physical hosted outside of an AXP|PAYBACK facility or if a Fourth-Party (Subcontractor) will have access to AXP|PAYBACK data via the Third-Party relationship, either directly from AXP|PAYBACK, or indirectly via the Third-Party.

Select appropriate option (select all that apply):

- On Premise at the Third-Party location.
- Cloud Storage including on premise cloud service.
- Fourth-Party data center-non cloud.
- Hosted at an AXP|PAYBACK facility.

6 **Q#L2 1.2.1 | Which cloud storage provider is being used as part of the service provided?**

Purpose: Determine whether the service is going to be offered/or managed in a cloud solution, or something other.

Response options (select all that apply):

- AWS (Amazon Web Services)
- Google Cloud
- Oracle
- IBM (International Business Management)
- MS Azure (Microsoft)
- Other (please provide comments for explanation)

7 **Q#L2 1.3 | How will AXP|PAYBACK data or Systems be accessed during the expected term of the service?**

Purpose: To understand the protocol of the AXP|PAYBACK data that is being sent, shared, or stored.

Response option (select all that apply):

- HTTPS (Hypertext Transfer Protocol Secure)
  HTTPS is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.
- SFT (Secure File Transfer)
  SFT provides file access, file transfer, and file management over any reliable data stream.
- API (Application Programming Interface)
  API acts as a medium between two communicating entitles or applications.
- MPLS (Multiprotocol Label Switching) Direct Connections
  MPLS is a networking protocol that uses a predetermined path to the destination router. In effect it creates a VPN type service that makes it logically impossible for data from one network to be mixed in or routed over to another network. However, it does not include encryption services, so the traffic is visible to service providers along the route.
- Unstructured Data (paper/fax/print)
  Unstructured data files often include text and multimedia content. For example, email messages, word processing documents, videos, photos, web and/or social media pages.
- AXP|PAYBACK issued laptop with AXP|PAYBACK access credentials
  AXP|PAYBACK laptop accessed with AXP|PAYBACK credentials (ADS ID / Password).

8 **Q#L2 1.4 | Is the Third-Party requesting any AXP|PAYBACK or Card Member (CM) data elements which fall within any of the following categories.**

Purpose: This question is part of the Enterprise Data Partnership Strategy (EDPS)*. Third-Party Partners are demanding a larger breath of data coupled with broader usage rights. Business Owners must determine whether Third-Party Partnerships comply with the Enterprise Data Sharing Principles.

Response option (select all that apply):

- Applicant & New Account Detail (e.g. name, application decision, approved account details, open date, channel of origin);
- Basic Transaction Information (e.g. charge date, amount, merchant name, merchant address);
- Card Account Information (e.g. account status, product type, payment type, MR points balance, authorized account signers);
- Card Account Number (i.e. 15-digit account number, digital account number, companion account number), Card Member / Prospect Status (i.e. user flagged as an AXP|PAYBACK CM user flagged as AXP|PAYBACK prospect);
- Credit Performance Data (e.g. risk scores);
- Customer Behavioral (e.g. recent transactions, benefits usage, offer redemptions);
- Customer Demographic (e.g. name, business name, email address, mailing address, phone number, status);
- Customer Interactions (e.g. servicing), Digital Information (e.g. cookie data, IP address, referring URL);
- Merchant Operational (e.g. merchant hierarchy, years doing business, MCC code);
- Proprietary Audience Segmentations (e.g. high-spending CMs, derived lifestyle attributes);
- Prospect Demographic (e.g. name, business name, email address, mailing address, phone number, status);
- Statement Information (e.g. balance amount, payment due date);
- None of the above.

*Enterprise Data Sharing Principles. Background: Industry, regulatory, & competitive drivers have significantly impacted data sharing. Third-Party Partners are demanding a larger breadth of data coupled with broader usage rights. Additionally, Customer consent-driven data sharing is becoming more prevalent. As such, "Should We" data sharing decisions have become more complex, with enterprise-wide implications. In support, the Enterprise Data Sharing Principles are designed to provide consistency, transparency and agility across the Enterprise for these types of decisions. The Principles will ensure that we are always taking a customer-first approach while protecting and elevating our trusted brand.

Compliance

9 **Q#L2 2.1 | Does the Third-Party provide modeling services and/or model development activities which impact AXP|PAYBACK processes and/or business decisions?**

Purpose: To identify if the Third-Party has or is using their own Risk Model. To confirm that the data used for model development and data inputs to the model are consistent, complete, and meet the AXP|PAYBACK Model Risk requirements.

Guidance to help identify a model:

1. Does your process develop, manage, or use any approach that produces a quantitative output?
2. Does this approach employ statistical, mathematical, economic, financial, machine learning, or artificial intelligence approaches that require subjectivity?
3. Is the approach used for analyzing business strategies, informing business decisions, identifying, and measuring risks, valuing exposures, conducting stress testing, assessing adequacy of capital, measuring compliance with internal limits, or meeting financial and/or reporting requirements and issuing public disclosures?

Note: If any of the conditions above are met, then answer **Yes**. If there are any doubts, consult the Model Risk Management Group @ mrmggoverance@aexp.com for additional guidance.

Response options: YES | NO

10 **Q#L2 2.2 | Is the Third-Party creating marketing and advertising materials?**

This question triggers when one of the **AMEP10 Service Categories** shown below is selected:

1. Account Fulfillment
2. Card Benefits
3. Collections and Credit Operations
4. Customer Service
5. Human Resource Services
6. Insurance (Colleague)
7. Insurance (Product Benefit)
8. Market Research
9. Market and Advertising*
10. Merchant Recruitment Partner
11. Payroll
12. Prepaid Cards/Re-Sellers
13. Public Relations
14. Sales
15. Sponsorship Experiential
16. Travel Agencies *

*Examples of marketing and advertising include Creating Sales, servicing or marketing collateral, or ad placement may include, but are limited to fliers, handouts, emails, advertisements, billboards, giveaways, or any other tangible or electronic material used in sales, servicing, marketing, or advertising on AXP|PAYBACK' behalf.

Purpose: To determine if the Third-Party has the ability to influence the customer by creating materials and information. Creating Sales, servicing or marketing collateral, or ad placement may include, but are limited to fliers, handouts, emails, advertisements, billboards, giveaways, or any other tangible or electronic material used in sales, servicing, marketing or advertising on AXP|PAYBACK' behalf.

Response options: YES | NO

11 **Q#L2 2.3 | Will the Third-Party use a Proprietary risk or response models/algorithms to perform their specific function/interaction with the customer?**

Purpose: To determine if the Third-Party has increased risk by using their own risk model. Engagement of LOBCO/MCO is suggested.

Response options: YES | NO

General Engagement

12 **Q#L2 3.1 | How many employees does the Third-Party have?**

Response options:

- < 10 employees
- 10-100 employees
- 101-500 employees
- 501-1000 employees
- >1000 employees

Privacy

13 **Q#L2 4.1 | Is Data shared between AXP|PAYBACK and the Third-Party?**

Purpose: This question helps to understand whether AXP|PAYBACK Personal Data is being shared between AXP|PAYBACK and/or the Third-Party in an identifiable format for a legitimate purpose.

Note: Collecting data from an AMEX|PAYBACK mobile application or AMEX|PAYBACK website also constitutes as **sharing** data.

Response options: YES | NO

14 **Q#L2 4.1.1 | Who will honor privacy choices?**

Purpose: This question identifies where privacy choices are provided by AXP|PAYBACK resulting in a reduced privacy risk score.

Response options:

- AXP|PAYBACK
- Third-Party
- Both AXP|PAYBACK & Third-Party
- Neither
- N/A

15 **Q#L2 4.1.2 | Who will provide adequate notice or consent/disclosure language to Data Subjects?**

Purpose: If the Third-Party collects data from Data Subjects/Individuals on behalf of AXP|PAYBACK then adequate notice or disclosures are required.

Response options:

- AXP|PAYBACK
- Third-Party
- Both AXP|PAYBACK & Third-Party
- Neither
- N/A

16 **Q#L2 4.1.3 | Does the Third-Party have a mechanism in place to receive Data Subjects Privacy rights and complaint requests and provide information about how their personal data is processed?**

Purpose: If the Data Subjects/Individuals ask, they'll be informed about how their Personal Data is processed and their rights and remedies.

Response guidance:

- Answer **Yes** only when the Third-Party is hosting the data and AXP|PAYBACK has no access to that data. In this case the Third-Party will be responsible for responding to individual's request.
- Answer **No** if Data Subjects/Individuals can contact AXP|PAYBACK to inquire about how their personal data is processed, or to update any of their information that is inaccurate or incomplete.

Response options: YES | NO

17 **Q#L2 4.1.4 | In the event of a Third-Party data privacy breach, will AXP|PAYBACK or the Third-Party provide notification to impacted individuals?**

Purpose: To determine that the business has a process for identifying who will be notified when and how the data subjects will be notified.

Response guidance: if Both AXP|PAYBACK & Third-Party are providing notification, select Third-Party and complete the required Due Diligence.

Response options: AXP|PAYBACK | Third-Party

18 **Q#L2 4.1.5 | Will personal data be collected by the Third-Party via any of the following means?**

Purpose: This question identifies inherent privacy risk associated with Third-Parties collecting Personal Data directly from individuals for, or, on behalf of AXP|PAYBACK, or if the data is being collected by the Third-Party from their own customers, purchased or accessed from other sources (not on behalf of AXP|PAYBACK).

Response option (select all that apply):

- Directly from individuals on behalf of AXP|PAYBACK - individual understands that data is being collected for use by AXP|PAYBACK
- From the Third-Party's customers/clients or via other sources and shared with AXP|PAYBACK - individual is not under the impression the collection is being done by AXP|PAYBACK
- Third-Party is collecting data from AXP|PAYBACK customers and individual is not under the impression that collection is done by AXP|PAYBACK
- Third-Party purchases or accesses PII and reselling/repurposing and is providing it to AXP|PAYBACK - Third-Party has no direct customer relationship
- Third-Party is accessing or purchasing PII from any source other than through a direct customer relationship and providing to AXP|PAYBACK

- Screen scraping, web scraping/web crawling, data harvesting technology
- Application Programming Interface (APIs)
- Biometric/facial recognition technology
- Real-time Geographic tracking/location technology
- Persistent tracking (aka cookies)
- Website, mobile app, bot, voice recognition software
- AXP|PAYBACK tag(s) on Third-Party's site(s)
- Third-Party's tag(s) on AXP|PAYBACK site(s)
- Other, please provide comments
- N/A - Not collecting data

19 **Q#L2 4.1.6 | Will data be processed for any of the following purposes?**

Purpose: To confirm the Third-Party discloses and or informs Data Subjects/Individuals that their data may be shared. If collected online, to ensure privacy disclosure and or privacy notice is provided to the Data Subjects/Individuals noting how data is processed (collection, access, use, sharing, storing).

Response option (select all that apply):

- Fraud prevention, maintain AXP|PAYBACK network security or to prevent and detect crime - e.g., One Time Password
- Data is transferred across country borders
- Automated decision making
- Big Data processing or matching/appending data to AXP|PAYBACK existing customer, merchant, employee and/or prospect information - i.e. large-scale processing of data
- Credit risk assessment and/or to determine credit eligibility
- Re-engineering or re-identifying individuals or businesses
- Systematic evaluation or monitoring based on automated processing or profiling
- Tracking individuals across multiple devices or consumer's device location
- Innovative use or application of technological or organizational solutions - e.g., using fingerprints/facial recognition for physical access controls
- Collecting or transmitting personal data in novel ways that involve every day connected devices
- Profiling or building behavioral profiles of the individual
- Predicting or evaluating behavior, personal preferences, location, health
- Predicting or evaluating performance at work, reliability and/or any other trait
- Predicting or evaluating economic situation
- Other, please provide comments

Anti-Corruption – Part 1

ACDD Questionnaire. The Third-Party is required to fill the ACDD questionnaire appropriately. If the Third-Party choose to answer **Yes** to the question, then they must provide additional information they believe would be helpful.

20 **Q#L2 5.1 | Is the Third-Party a government owned/controlled entity or a State owned/controlled entity?**

Purpose: To identify government owned or controlled entities that directly provide services to AXP|PAYBACK. State Owned Entity(s) (SOEs) can often appear to be private companies, but partially owned by the government. Examples include but are not limited to government owned banks, airlines, sovereign wealth funds, public pension funds and public utilities.

Response Guidance:

- Answer **Yes**, if the third-party is Government/State owned or controlled directly or indirectly by a government at any level (national, state, or local). Entities are treated as "government-owned," "state-owned", "government-controlled," or "state-controlled" if any level of government or any department, agency or instrumentality of the government holds 20% or more of the shares of the Third-Party or, if less than 20%, has control over the Board of Directors.
  Examples include, but are not limited to government lobbying services, arrange meetings between AXP|PAYBACK employees and government officials, assist AXP|PAYBACK in obtaining a government permit or license, or provide government-owned insurance benefit programs (e.g. United States Postal Service (USPS) will pick up customer prepared packages and ship them to AXP|PAYBACK's Card Manufacturer destinations).
- Answer **No**, if the third-party is not owned by the Government/State or the Government/State owns less than 20% of the third-party's shares and has no control over the Board of Directors.

Response options: YES | NO

*Please refer to TLM_AEMP10_Third-Parties and Categorization document for more details.

21 **Q#L2 5.2 | Is the Third-Party financially incentivized for achieving defined targets based on the service outsourced to them?**

Purpose: Identify if the third-party is financially incentivized with a payment, award, or other transfer of value for achieving defined targets based on the service that is outsourced to them. Serves as a filter to identify services that inherently prone to corruption.

Incentive: anything of value transferred (a) from AXP|PAYBACK to an external party or individual employees of that external party for achieving defined targets; or (b) to AXP|PAYBACK or individual AXP|PAYBACK employees from an external party for achieving defined targets.

Response Guidance:

- Answer **Yes** if the service provided is under a medium or higher risk performance-based incentive program that provides benefits in exchange for meeting certain sales, volume, timing, or other defined targets.
  - Medium Risk Incentive: includes governments with specific external parties (e.g. sales incentives, performance incentives, merchant acquirers)
  - Higher Risk Incentive: includes agreements with high risk external parties (government officials, government entities/SOEs)
- Answer **No** if the service in not under a performance-based incentive.

Response options: YES | NO

22 **Q#L2 5.3 | Are there any known incident, investigation, or allegation of bribery, corruption, fraud, money laundering, misrepresentation, or other similar activities related to the business entity or any associated persons within the past five years?**

Purpose: To comply with anti-corruption laws defined by the AEMP06.

Response options: YES | NO

23 **Q#L2 5.4 | Does the expected compensation of the Third-Party for its service vary significantly from industry or jurisdictional/local standards?**

Purpose: To understand whether the cost for a particular product or service meets local standards.

Response Guidance:

- Answer **Yes** if the Third-Party was evaluated under the SSBE contracting price reasonableness process, and gaps were raised, or the compensation for the service is above the standard range normally charged for similar services.

Response options: YES | NO

24 **Q#L2 5.5 | Is the Third-Party publicly traded on one of the recognized exchanges?**

Purpose: A public traded company is a company that offers its securities for sale to the general public through various stock exchanges (NYSE, NASDAQ). Companies that are publicly traded, are required to go through a series of requirements related to regulatory compliance.

Response Guidance: answer **Yes** if the third-party trades on one of the recognized exchanges (please refer to TLM_Recognized Exchanges document for more details).

Response options: YES | NO

25 **Q#L2 5.5.1 | Does the Third-Party provide services To or From a "high-risk" market?**

1. Bahrain
2. China
3. Mexico
4. Russia
5. United Arab Emirates
6. Venezuela

Purpose: This question serves as filter to identify countries with Beneficial Owners (BO) designations vs geographic high corruption / high risk countries as these are the identified markets where BO considerations exist.

Response options: YES | NO

26 **Q#L2 5.5.1a | Does Third-Party have any Beneficial Owners?**

Purpose: This question is utilized to determine if a Beneficial Owner is identified within the Third-Party and service provided is in a country tagged as BO designation.

Response guidance: Beneficial Owner = natural person or legal entity that owns ≥25% of the company

Response options: YES | NO

27 **Q#L2 5.5.1b | How many beneficial owners does the entity have?**

Response options: 1 | 2 | 3 | 4

Anti-Corruption – Part 2

28 **Q#L2 5.6 | How long has the Third-Party been in business?**

Purpose: To help determine reputable companies who have been in business for some time.

Response options:

- Less than a year
- Less than 5 years
- More than 5 years

29 **Q#L2 5.7 | How long has the Third-Party provided this type of service?**

Purpose: To help determine companies with longstanding reputations e.g. example, a company may have been in business for six months but is hired by AXP|PAYBACK to perform complex nuanced services.

Response options:

- Less than a year
- Less than 5 years
- More than 5 years

30 **Q#L2 5.8 | Was the Third-Party recommended by a government official, or an employee officer, agent, or other representative of a SOE?**

Purpose: To identify if any Third-Party was recommended by a government official (any level) or state-owned entity.

Response guidance: If so, name the affiliation and whether they are government official or employee, officer, agent, or another representative of a SOE.

Response options: YES | NO

31 **Q#L2 5.9 | Was the Third-Party recommended by a senior executive or officer of a private company?**

Purpose: to understand if there are any relationships between the Third-Party that will be engaging with AXP|PAYBACK and another private company, who could have an incentive for recommending the Third-Party to AXP|PAYBACK within the context of private bribery.

Response guidance: The senior executive or officer that should be listed is the executive or officer of the potential private company who made the recommendation, and who is not affiliated with AXP|PAYBACK or the Third-Party with whom AXP|PAYBACK is engaging.

Response options: YES | NO

Anti-Corruption – Part 3

Purpose: To understand whether any part of the relationship (service, entity headquarters, payments) will stem from country with heightened corruption risk. Heightened country risk will not render a relationship medium or high risk by itself, but if these questions are answered **Yes** in addition to other questions on the TRA, then jurisdictional risk will be a factor considered when the risk rating is finalized.

Please refer to TLM Geographic Corruption Risk Ratings document for more details.

32 **Q#L2 5.10 | Will payment for this service be sent to an address in a high-risk country?**

Response options: YES | NO

33 **Q#L2 5.11 | Is the Third-Party headquartered in a medium or high-risk country?**

Response options:

- Yes - High Risk
- Yes – Medium Risk
- No – Low Risk

34 **Q#L2 5.12 | Is the Third-Party providing a service or activity to a medium or high-risk country?**

Response options:

- Yes - High Risk
- Yes – Medium Risk
- No – Low Risk

35 **Q#L2 5.13 | Is the Third-Party providing a service or activity from a medium or high-risk country?**

Response options:

- Yes - High Risk
- Yes – Medium Risk
- No – Low Risk

Antitrust

36 **Q#L2 6.1 | Does the potential agreement with the Third-Party prohibit the solicitation and/or hiring of the Third-Party's employees by AXP|PAYBACK, or vice-versa?**

Purpose: The antitrust agencies are focused on competition in labor markets. The purpose of this question is to determine if the agreement contains any non-hire or non-solicit provisions and, if so, whether they are appropriately tailored to the third-party engagement and not overbroad/overinclusive. If yes, any third-party agreement that contains these provisions should be vetted by GCO Antitrust.

Response guidance:

- Answer **Yes**, if the potential agreement contains any non-hire or non-solicit provisions.
- Answer **No**, if the potential agreement does not contain any non-hire or non-solicit provisions.

Response options: YES | NO

37 **Q#L2 6.2 | Does the Third-Party (or subcontractor of Third-Party) compete with AXP|PAYBACK in any way?**

Purpose: To identify services that involve collaboration and/or information sharing with an AXP|PAYBACK competitor to consider any antitrust implications. If yes, the partnership should be vetted by GCO Antitrust.

Response guidance:

- Answer **Yes**, if the third-party competes with AXP|PAYBACK in any way.
- Answer **No**, if the third-party does not compete with AXP|PAYBACK in any way.

Response options: YES | NO

Sanctions

38 **Q#L2 7.1 | Sanctions Screen Results**

Response options:

- Alert
- No Alert

39 **Q#L2 7.2 | What is the Record Status?**

Response options:

- Confirmed PEP/Risk Match
- Duplicate Alert
- False Positive
- Generated in Error
- Inactive Third-Party Contract
- Match - Terminated
- Open
- Closed

40 **Q#L2 7.3 | What is the Alert Status?**

Response options:

- Open
- Closed

41 **Q#L2 7.4 | What was the Final Decision?**

Response options:

- No Match
- Match – Continued Relationship
- Match – Discontinued Relationship

42 **Q#L2 7.5 | What tool was used to perform the sanctions screen on the third-party?**

Response options:

- Bridger
- Other

43 **Q#L2 7.6 | Result ID Number**

Response options: *Freeform Text Box*

SOX

44 **Q#L2 8.0 | Are there any known issues with financial impacts related to this Third-Party engagement across AXP|PAYBACK?**

Purpose: To determine if the services being provided by the Third-Party has any financial risk associated with it.

Response Guidance: Consider Operation Risk Events (OREs) or issues identified by TLM/ Business including any audit findings related to the process with financials implications during the last 4 quarters.

Response options: YES | NO

45 **Q#L2 8.1 | If the service is currently being provided by an existing Third-Party, have there been any risk events or concerns raised with financial impacts related to the use of that Third-Party in the process?**

Purpose: To determine if the existing service provided by the Third-Party had any financial risk associated with it.

Response Guidance: Consider Operation Risk Events (OREs) or issues identified by TLM/ Business including any audit findings related to the process with financials implications during the last 4 quarters.

Response options: YES | NO