Third-Party Lifecycle Management 2.0.

Service Risk Assessment (SRA)

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

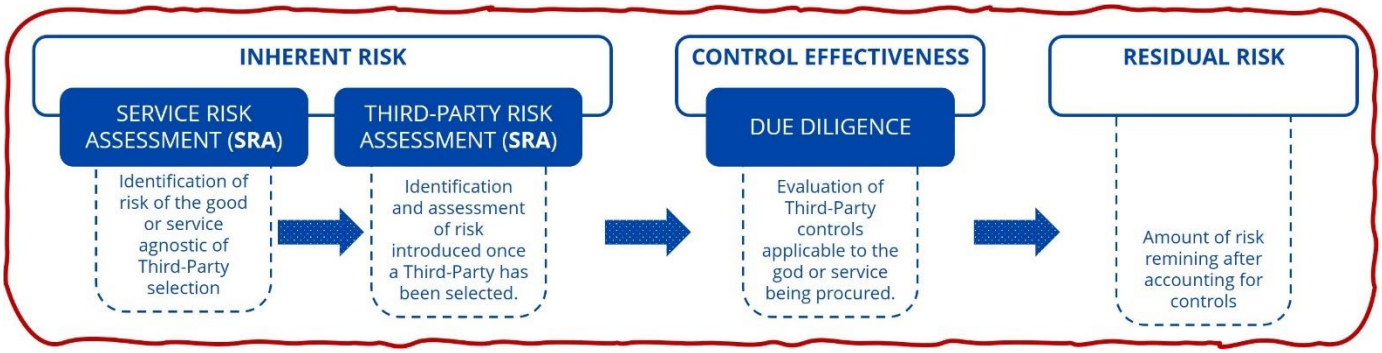
Useful Definitions

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.

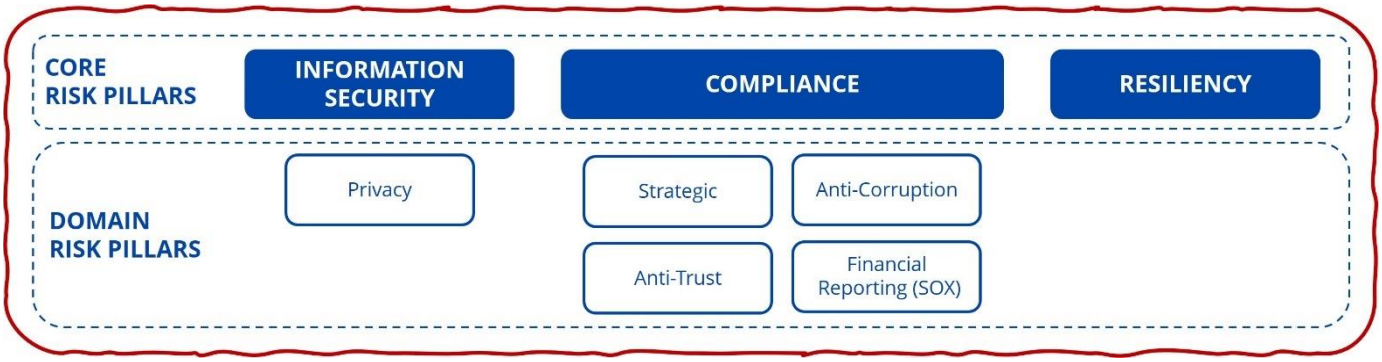
AEMP10 prescribes evaluation of the characteristics of each good or service (engagement) provided by a Third-Party to identify and measure the inherent risk of the activity. Assessing Third-Party Risk involves a sequence of interrelated activities designed to define the good or service being procured, 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.

Service Risk Assessment (SRA)

Level 1 Questions

The SRA guidance document is divided into two sections: the first section lists all the SRA questions that could potentially trigger, and the second section includes all the due diligence that could potentially trigger based on the responses to the SRA.

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 Due Diligence requirements trigger).

Section 1: SRA Level 1 Questions

Risk pillars are: 1. Service Details, 2. Information Security, 3. Privacy, 4. Resiliency, 5. Compliance, 6. Strategic, 7. Anti-Corruption and 8. SOX.

1. Service Details

1 **Q#S4| Countries Service will Be Provided to**

If the engagement is classified as new or existing with changes this field requires a response.

2 **Q#S5| Provide the PRSA ID for the process related to this service.**

Please choose the most fitting:

PR001985 LP Partner Acquisition (Poland)*****
PR002112 LP Campaign Management (Poland)******

*****_Partner Acquisition – all Vendors in CEG and Finance categories._

******_Campaign Management – all Vendors in Marketing and Technology (if the technology is used with the purpose of enhancing or generating more marketing to be sent to customers via any channel including digital ones, this would also include affiliate business models and or similar, games, etc. – anything where we are connecting with customers to increase revenues in any way)._

There should not be more than 1 PRSA ID allocated to a vendor (even though there are options to do so).

3 **Q#S6| Anticipated annual total spend**

Please enter the anticipated annual total spend. [USD exchange rate 0,2719].

4 **Q#S7| Anticipated total contract value**

Total contract value. [USD exchange rate 0,2719].

2. Information Security

5

Q#L1 1.1| Will the service involve accessing, processing, collecting, sharing, creating, storing and/or destroying any AXP|PAYBACK data (Company, employee, and/or customer information), and/or accessing AXP|PAYBACK systems?

Purpose: The purpose of this question is to identify services where AXP|PAYBACK data (not just PII) and/or AXP|PAYBACK systems are involved. Data Types will drive the AXP|PAYBACK Classification, if not captured correctly could compromise the company's brand, legal status and/or financial status. The data must be classified based on the potential impact to AXP|PAYBACK.

Processing: ANY ACTION taken in relation to Data|PII and includes collecting, storing, altering, accessing, viewing, using, transferring, receiving, sharing or destroying. Examples include, but are not limited to, AXP Card numbers, individual's name, date of birth, government-issued ID numbers, home address, email or IP address, bank account information, and location-based data.

Response Guidance:

- Select **Yes,** if the service involves accessing, processing, collecting, sharing, creating and/or destroying AXP|PAYBACK Data (not just PII) **or** the service involves accessing AXP|PAYBACK systems. This includes Infrastructure providers accessing the AXP|PAYBACK network. This may also include but is not limited to; AT&T, Verizon, British Telecom, IBM, EMC.
- Select **No,** if data is not shared and/or there is no access to AXP|PAYBACK Systems.

When to answer YES:

- Captures, receives, processes, and/or shares complete, partial, aggregated, masked, or unmasked PII.
- Services involving de-identified, or aggregated data (these are evaluated for collection practices, source of data and consent for use and may require additional contractual safeguards restricting the Third-Party from re-identifying individuals.

***Note**: Also answer YES even if the Third-Party will be using AXP|PAYBACK laptops or assets.*

When to answer NO:

- Does not process any Personal Data/PII or any other data that could identify an individual OR
- CV/Resume and cover letter from external job applicant or recruitment companies (i.e. shared with AXP|PAYBACK by recruitment companies)
- Mail and shipping services which receive and transport sealed parcel with AXP|PAYBACK's employee, customer or merchant mailing/shipping address information on the label (i.e. USPS, FedEx, UPS, DHL). This only applies to Third-Parties where AXP|PAYBACK does not send any lists of the names and addresses to the Third-Party. The service providers simply pick up and drop off sealed packages.
- Event Sponsorship in which no PII is shared or collected.
- Prepaid Cards with account numbers and security codes which do not tie to or identify an individual.
- Amex Gift Cards.
- International Currency Card (ICC) Bank Partners.
- International Distribution Bank Partners.
- International Membership Rewards Partners (Pay with Points).
- International Membership Rewards Partners (Non-Pay with Points-Merchants fulfilled).
- International Membership Rewards Partners (Points Transfers).

- International Credit Bureau (Regulator Controlled).
- International Credit Bureau (Core National Agency).
- International Insurance Partners (No Added Charge – NAC).
- International Insurance Partners (Carriers).
- International Insurance Partners (Legacy Carriers).

Examples - High Risk Use Cases

- Call center (collections or customer servicing), involving access to customer information and/or direct customer contact.
- Plastic production/card personalization, with access to AXP Card information.
- Direct Mail services such as direct mail and email marketing, customer statements, customer correspondence, remediation mailings, and merchant mailings.
- Back-office data processing such as imaging and keying of new account applications, card member account maintenance such as posting of credits and debits and account updates.
- Credit Agency identification of prospective card members or potentially past due card members.
- Database marketing when suppliers have access to complete, partial, or de-identified card member information for profiling purposes.
- Online sweepstakes or website services with PII collection.
- Event management/sponsorship partnerships collecting PII.
- Merchandise fulfillment w/ customer information.
- Payment processing services which require credit card numbers and customer and merchant information to handle credit card transactions and settlements between AXP|PAYBACK, merchants and other financial institutions.
- HR related services where AXP|PAYBACK employee data may be shared (i.e. employee name and date of birth or social security number/government ID).

6 **Q#L1 1.1.1 | What types and volume of AXP|PAYBACK data will be accessed, processed, shared, collected, created, stored and/or destroyed by the Third-Party during the course of the service?**

Purpose: The purpose of this question is to determine AXP|PAYBACK data types, the classification of selected data type(s) and the expected volume for each data classification identified as well as to identify services where AXP|PAYBACK non-public data and/or AXP|PAYBACK systems are involved (not just PII).

Response Guidance: The highest ranking AXP|PAYBACK Classification will auto-populate this field based on previously selected data types.

Response Options (Data types). Please refer to the TLM_Data Type Sheet file for further guidance:

- AXP Secret
- Primary (Restricted P1) Consumer, Employee, Merchant, Institutional
- Primary with Secondary Affiliation (Restricted P1-P2) Consumer, Employee, Merchant, Institutional
- Secondary (Restricted P1-P3) Consumer, Employee, Merchant, Institutional
- AXP Internal/Public
- AXP Internal only
- AXP Public only

LP/AXP Public

Information intended for public consumption and distribution. Information can be shared with the general public and may be distributed over public networks. Information requires no special security controls. Example: marketing brochures, public website content, published annual reports.

LP/AXP Internal

Information used to support normal business operations and is intended for use when conducting company business. Information is defined as non-sensitive, although requires appropriate controls. Example: unpublished creatives/marketing material, final policies and standards, organizational announcements, anonymized/ pseudonymized data (i.e. PAYBACK External Member ID, PAYBACK Reference ID, PAYBACK SCRID – external value is limited).

LP/AXP Restricted

Information is valuable and/or gives the company a competitive advantage. If it is misused, it could compromise the company's competitive advantage, customer or employee privacy, or the legal or financial status of the company. Access to this information is limited to specified groups. Example: GDPR defined Personal Data e.g.: contact information (name, email, work location, phone number), payroll information, business transactions, PAYBACK card/account- number, PAYBACK point balances.

LP/AXP Secret

LP Secret information is highly valuable, sensitive and gives the company competitive advantage. If it is misused, it could seriously compromise the company's competitive advantage, or the legal or financial status of the corporation. Access to this information is limited to named individuals or groups. Example: trade secrets, proprietary information, unpublished annual reports, authentication credentials (e.g. passwords, pass phrases, PINs); salary information, HR data.

Response Options (Volume). *Record = 1 record per person, per data classification, regardless of the number of data types associated to the individual. If 1 person is in the database multiple times, or includes multiple data types for the individual, it still equates to 1 record*:

- 10MM + records
- 1MM+ to 10MM records
- 500,001 to 1MM records
- 200,001 to 500,000 records
- 50,001 to 200,000 records
- 10,001 to 50,000 records
- 101 to 10,000 records
- 0 to 100 records

Concerns Third-Parties that have access to non-Public (i.e., AXP|PAYBACK Internal or AXP|PAYBACK Restricted or AXP|PAYBACK Secret) data pertaining to AXP|PAYBACK, its employees, customers and/or technology systems, and/or the purchase of technology software, cloud-based services or hardware. Examples include, but are not limited to, software licensors and online service providers (including "click-through" licenses), API access arrangements, plastic card manufacturers, data hosting / storage / destruction services, telecommunications or cloud computing services, or services related to processing of AXP|PAYBACK data.

PII data always is at least AXP|PAYBACK Business Restricted !

7 **Q#L1 1.2 | Will the service include an application?**

Purpose: To determine if the Third-Party service would include an application.

Response Guidance: Applications are programs or systems that are not only accessible/visible from the intranet but are also accessible from the internet. i.e. Web Application, Mobile Application, Cloud, Software, File Transfer Services, Infrastructure Providers.

Response options:

- Internet Facing (web/mobile) application
- Non internet facing application
- No application

Examples of Internet Facing Applications:

- Web Application: Accessed via the internet using your browser: Chrome, Internet Explorer, Firefox.
- Mobile Application: Examples include but are not limited to Waze, Words with Friends. Any offering in Google Play, Apple App Store.
- Cloud: Examples include but are not limited to: Amazon Web Services (AWS), Rackspace, Google Cloud, Microsoft Azure, Salesforce.
- Software: Examples include but are not limited to: Adobe Acrobat, Solar Winds
- File Transfer Services: Examples include but are not limited to: Transmission of FICO scores from credit bureau to AXP|PAYBACK, Transmission of potential new customers from a lead management provider.
- Infrastructure Providers: Examples include but are not limited to: AT&T, Verizon, British Telecom, IBM, EMC.

8 **Q#L1 1.2.1 | What is the required Recovery Time Objective (RTO) of the application?**

Purpose: The purpose of this question is to identify the Recovery Time Objective (RTO) of the application before it causes significant impact to AXP|PAYBACK. Establishing the RTO sets criticality of the Third-Party to the BIA/Recovery Tier. RTO establishes when a business process and all it's components (applications and Third-Parties) need to return to full function. The BU defines this during the BIA process. The BIA Tier and RTO are linked. *For example, if the RTO = 0-4, then the BIA Tier is Tier 0.*

Response Guidance: The RTO should be answered in the number of hours allotted for the recovery time of the application based on the agreed parameters within the contract. RTO is one of the inputs into the BIA.

Response options:

- 0 to 4 hours (**Tier 0**)
- 5 to 24 hours (**Tier 1**)
- 25 to 48 hours (**Tier 2**)
- 49 to 72 hours (**Tier 3**)
- 73 to 743 hours (**Tier 4**)
- = 744 Hours/Out of Scope (**Tier 5**)

***Note**: If the service warrants a recovery time response between 0 to 48 hours (Tier 0 or 1 or 2) the RTO Service Level Agreement (SLA) must be mentioned within the contract.*

3. Privacy Pillars

9 **Q#L1 1.1.1a | Is the personally identifiable information (PII) processed during the service Aggregated or anonymized data?**

Purpose: to identify services provided that are processing Personal Data (data that could identify an individual or could be used in combination with other information to identify an individual). This question assesses the risk of the Third-Party / Fourth-Party (Subcontractor) re-identifying the data that AXP|PAYBACK provides. AXP|PAYBACK has developed standards around aggregated/anonymized data that should be reviewed to ensure it is in line with AXP|PAYBACK standards.

Response Guidance:

- Select **Yes** if the Third-Party captures, receives, processes, and/or shares complete, partial, aggregated, masked, or unmasked Personal Data/PII and Services involving de-identified, or aggregated data (these are evaluated for collection practices, source of data and consent for use and may require additional contractual safeguards restricting the Third-Party from re-identifying individuals).
- Select **No** if the PII processed is not aggregated or anonymized.

4. Resiliency Pillar

10 **Q#L1 2.0 | Please provide the BIA ID(s) this service will support.**

Purpose: Management must identify, analyze, and prioritize interdependencies among business processes and systems for alignment with resilience and recovery objectives. These interdependencies include Third-Parties.

Response Guidance: Please enter the BIA IDs of the business processes supported by the service. There is no option to enter N/A in this field. For the BIA Allocation – we should choose the most fitting one:

BIA-06925-Global Loyalty Coalition: PROCESSING OF PAYBACK POINTS (**Tier 3**)
BIA-06322-Global Loyalty Coalition: ACCURATE TARGETING OF MEMBER OFFERS (**Tier 5**)
BIA-06321-Global Loyalty Coalition: CUSTOMER EXPERIENCE AND PRODUCT DEVELOPMENT (**Tier 5**)
BIA-06320-Global Loyalty Coalition: DIGITAL MARKETING (**Tier 5**)
BIA-06323-Global Loyalty Coalition: OFFER MARKETING AND CAMPAIGNS (**Tier 5**)
BIA-06319-Global Loyalty Coalition: PARTNER MANAGEMENT AND BUSINESS DEVELOPMENT (**Tier 5**)

Recommendation: BC Coordinator Approval Validation will be required within Process Unity; it is recommended for audit purposes to upload the BC Coordinator's evidence of the BIA ID and BIA Tier.

11 **Q#L1 2.1 | How many Business Impact Analysis (BIA's) will this service support?**

Purpose: The purpose of this question is to gauge the extent of dependency that the enterprise has on the service. Taking a count of the business processes using this service allows a sense of concentration risk,

where the pervasiveness of a service through the enterprise may pose an aggregated risk greater than any one of the processes alone.

Response Guidance: TRM's should be working with the BC Coordinators to understand the business processes being supported by the service.

Response options:

- 1
- 2-9
- 10 or more

There should not be more than 1 BIA's allocated to a vendor (even though there are options to do so).

12 **Q#L1 2.2 | What is the highest Business Impact Analysis (BIA) criticality tier this service supports?**

Purpose: To identify Third-Parties that support business functions (activities and processes) critical to the continued operations of the enterprise. If a critical business function stops, AXP|PAYBACK could incur operational, regulatory, financial, brand, or other damages or penalties. TRM's should work with BC Coordinators to understand the highest Tier among the BIA to which the Third-Party is associated

Response Guidance: The BC Coordinator will report the function(s) supported has been assigned Tier 0, 1, 2, 3, 4 or 5 in its BIA.

Recommendation: BC Coordinator Approval Validation will be required within Process Unity; it is recommended for audit purposes to upload the BC Coordinator's evidence of the BIA IDs and the highest BIA Tier.

13 **Q#L1 2.3 | Please estimate the contribution of this outsourced service to enabling the business function(s) covered by the BIA(s)?**

Purpose: The purpose of this question is to estimate how much the Third-Party would contribute to enable the business function(s) covered by the BIA(s). The objective is to ensure that Third-Parties conduct sufficient business continuity management to ensure resilient service that meets the needs of the enterprise.

Response Guidance:

- **>50% or 100%** (service is significant, and process is reliant on the service). Mail handling and call centers in certain markets are fully supported by Third-Parties (90-95%). Statements and insurance claims are examples of business processes that can be greater than 50% supported by Third-Parties.
- **<50%** (Service is important, but workarounds required). Marketing and communications seem to be examples of business processes that can be less than 50% supported by Third-Parties.
- **N/A** (Service does not contribute to the process). Some fraud and authorizations BIA in certain markets depend 1% on their Third-Parties for contacting card members when a transaction has been identified as a potential Fraud concern (easily brought in-house). Another good example of low dependency on Third-Parties could be where consultants are brought in for reviews and advice but are never participants in the business process itself. For example, Legal might contract to use a repository of law journals that speeds research, but the task could also be accomplished on the Internet with a little more time and/or effort.

Response options:

- 100% - Process is entirely reliant on the service
- >50% - Service is very significant to process
- <50% - Service is important but there are workarounds
- N/A -Service does not materially contribute to the process

14 **Q#L1 2.4 | If the service is terminated or unable to be provided, what are the options to replace the product or service?**

Purpose: The purpose of this question is to identify if the service is terminated/cancelled, or if it cannot be provided, then who are other/alternative third-parties capable of providing this service.

Select appropriate option:

- AXP|PAYBACK currently has an in-house equivalent that is capable of providing the products or services today.
- There are several (>2) Third-Parties available in the marketplace that are capable of providing the products or services (within the next 3 months).
- There is a limited (1-2) number of Third-Parties available in the marketplace or AXP|PAYBACK would be required to develop an in-house equivalent or it would take more than 6 months to onboard a replacement service.
- Sole-source vendor – (e.g., unique specialized product/service tailored to AXP|PAYBACK).

5. Compliance Pillar

15 **Q#L1 3.1 | Will the service involve contact with any of the following?**

Purpose: The purpose of this question is to assess if the Third-Party service involve contact with any Individual Consumer/Cardmember, Small Business consumer, Commercial Clients, Merchant, Colleague or prospective colleague or the Third-Party service does not involve any contact with the consumer directly.

Select appropriate option (select all which apply):

- Individual consumer/Cardmember - potential or existing
- Small Business Consumer
- Commercial Clients
- Merchant
- Colleague or prospective colleague
- No direct contact with consumer

16 **Q#L1 3.2 | Will the service involve contact with any of the following?**

Purpose: To identify how the Third-Party service is being provided and the specific type of contact the Third-Party has with the customer. For example, how is the Third-Party going to interact with the customer, employee, merchant, or client?

Select appropriate option (select all which apply):

- In person
- Phone
- Contact center
- Mail
- Electronic
- Social Media
- Digital banners
- Print ads
- Billboards
- Radio
- None of the above

17 **Q#L1 3.3 | Does the service involve cash or cash equivalents?**

Purpose: This question determines if the Third-Party service involves any cash or cash equivalents, if it is receiving, processing, or issuing cash or cash equivalents. This is a common vehicle for Money Laundering.

Select appropriate option: YES | NO

18 **Q#L1 3.4 | Is the service subject to any of the following legal, regulatory or compliance requirements?**

Purpose: To determine if there are laws and/or regulations applicable to the service being outsourced and if the Business Unit is aware. This is not to identify every individual legal requirement but the area of Law that may be applicable.

Select appropriate option (select all that apply):

- Anti-Money Laundering (AML) OR Bank Secrecy Act (BSA)
- Data Privacy/Data Protection Laws/Regulations - i.e. GDPR, etc.
- Consumer Protection Laws
- E-Banking and E-Commerce
- Fair Lending
- Licensing - related to issuance/operation of AXP|PAYBACK products or services
- Employment-related requirements including Payroll and Benefits (Human Resources, General Counsel's Organization)
- Other banking Law and/or Regulation related to AXP's status as a Bank Holding Company
- Regulatory Reporting
- None of the above

6. Strategic Pillar

19 **Q#L1 3.5 | Is this a product or service which is not originated by AXP|PAYBACK or is rebranded as AXP|PAYBACK?** Could a customer reasonably perceive they are dealing with AXP|PAYBACK exclusively or could the brand experience in service delivery perceived as predominantly AXP|PAYBACK? i.e., white label

Purpose: To identify whether the engagement fits the white label conditions. For Example: gold card travel platform is hosted by Expedia; however, customers perceive they are dealing directly with AMEX.

Select appropriate option: YES | NO

20 **Q#L1 3.5.1 | Is this an insurance product, is the offering restricted to only AXP|PAYBACK products and is the insurance provider not replaceable?**

Response Guidance:

- Is the insurance offering exclusive to AXP|PAYBACK products and/or is the insurance provider not replaceable? If so, answer YES.
- Is the insurance product offered outside of AXP|PAYBACK and/or is the insurance provider replaceable? If so, answer NO.
- If none of the above apply, answer NA

Select appropriate option:

- **Yes**, both the offering is restricted to only AXP|PAYBACK products and the insurance provider is not replaceable i.e., this is white label insurance product
- **No**, either the offering is not restricted to only AXP|PAYBACK products or the insurance provider is replaceable
- NA - this is not an insurance product, but is still a white label product or service

21 **Q#L1 3.6 | Will this service be a co-brand relationship?**

Purpose: To assess if the Third-Party service is a co-brand Card relationship. Note: this is limited to card relationships and excludes events Global Network Services (GNS), and network card relationships.

Select appropriate option: YES | NO

7. Anti-Corruption Pillar

22 **Q#L1 3.7 | Will the service or activity outsourced by the business unit involve or potentially involve interaction with government entities in order to fulfill its contractual obligations, including subcontracting obligations?**

Purpose: This question identifies whether the third-party is acting as an Intermediary* for AXP|PAYBACK.

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

Response Guidance:

- Answer **Yes**, when the Third-Party is hired as an Intermediary to interact with government entities or government officials.
- Answer **No**, when the service requires no government interaction to fulfil the contractual obligation on AXP|PAYBACK's behalf.

8. SOX Pillar

*In 2002, the United States Congress passed the **Sarbanes-Oxley Act (SOX)** to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of corporate disclosures. The act sets deadlines for compliance and publishes rules on requirements. The SOX Risk Assessment will help identify SOX risk with services outsourced to third-parties and ensure that the Third-Party has SOX controls in place to mitigate legal and regulatory risk.*

23 **Q#L1 3.8 | Will the service process financial transactions or activities on behalf of AXP|PAYBACK, or does the service provide input into a financial model, calculation, accounting or reporting process.**

Purpose: To assess if the Third-Party service has any financial risk associated with it. For example, a payroll processing related services provided by a vendor, who does calculation of the Salaries and Benefits for AXP|PAYBACK, which is subsequently used by AXP|PAYBACK to authorize disbursement, will have a financial impact on AXP|PAYBACK Financial Statements.

Response Guidance:

- Answer **Yes**, when the Third-Party services will have a direct and/or indirect impact on AXP|PAYBACK financial statements, plays a role, or supports AXP|PAYBACK financial reporting, general ledger, or accounting systems which impact the financial information disclosed or published.
- Answer **No**, when financial reporting risk not to be assessed.

Note: Processing of financial transactions excludes remitting payment for services provided.

24 **Q#L1 3.8.1 | What is the expected annual volume of financial transactions to be processed or expected annual impact to financial statements as a result of the services provided?** Please consider all years over the contract term and respond with the highest expected annual impact.

Purpose: To assess whether there is any impact to the expected annual volume of financial transactions to be processed or expected annual impact as a result of the service provided by the Third-Party.

Example(s)of Direct /Indirect impacts (also known as **SOX Process):**

Direct: AXP|PAYBACK contracts a vendor to provide payroll processing services and inputs related to colleague information is shared by AXP|PAYBACK with the vendor, the vendor then provides the value of Salaries and Benefits to be booked in AXP|PAYBACK financial Statements.

Indirect: AXP|PAYBACK contracts a vendor to provide payroll taxation related services, where the AXP|PAYBACK team leverages the tax rates and other considerations provided by the vendor and does inhouse processing to arrive at the tax value.

Response Guidance:

- Any vendor service which may have an annual impact of $100M or greater on AXP|PAYBACK financial statements is categorized as a SOX impacting vendor.
- Financial impact refers to the dollar amount of transactions of the services provided by the Third-Party, for the period under review.

Select appropriate option:

- >$100,000,000
- $20,000,000 to $100,000,000
- < $20,000,000

25 **Q#L1 3.8.2 | Does the outsourced service impact an existing SOX process/control or SOX application?**

Purpose: The purpose of this question is to determine if the services provided by the Third-Party has an impact to any SOX process or SOX application.

Select appropriate option: YES | NO

26 **Q#L1 3.8.3 | Provide details of financial statement report lines (RL) impacted by the outsourced service.**

Purpose: To identify AXP|PAYBACK financial statement report lines (RL-1) either directly/indirectly impacted by the Third-Party. The risk ranking to identify high risk RL-1 can be located on the SOX Knowledge Center and then referring to the latest Financial Statement Risk Assessment (FSRA).

Response Guidance:

Answer **Yes**, if the service impacts a high-risk financial statement line item (RL-1) either directly / indirectly. Mention the name of the RL-1 line item in the comments box.

For example: While assessing the payroll processing services provided by a Payroll vendor, the Financial Statement Report Line (RL) impacted could be "Salaries and Employee Benefits", and the corresponding Report Line – 1 (RL-1) could be then assessed and mapped to that particular Third-Party (such as Incentive Bonus Provision/ Payroll Costs + Benefits/-Salaries) [Refer to the screen shot below] or, the Report Line can be Cash and Cash due from banks. and the corresponding Report Line-1 (RL-1) could be Depository Cash.

Select appropriate option: the response options are a combination of the RL Name Drop down and RL-1 Name Drop down.

Privacy Glossary

GLOSSARY	DEFINITION
Aggregate	Aggregate data means data or information from or pertaining to a group of people (generally, more than three people, at a minimum) that has been altered or manipulated so that there is no reasonable basis for the recipient of the information to discern the specific identity or response of any person from which the data was obtained or to whom it pertains. Aggregation is often done to produce high-level observations such as "demographics" or "trend analyses." Data, which has been anonymized but can later be un-anonymized. Anonymization is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
Application Programming Interface (APIs)	Application Programming Interface (API), is a software intermediary that allows two applications to talk to each other. Each time you use an app like Facebook, send an instant message, or check the weather on your phone, you're using an API. e.g. When you use an application on your mobile phone, the application connects to the Internet and sends data to a server. The server then retrieves that data, interprets it, performs the necessary actions and sends it back to your phone. The application then interprets that data and presents you with the information you wanted in a readable way. All of this happens via API.
Binding Corporate Rules	Binding Corporate Rules (BCR) are internal rules adopted by multinational group of companies, which define its global policy with regard to the international transfers of Personal Data within the same corporate/organizational group (intra-company transfers) to entities located in countries, which do not provide an adequate level of protection. BCRs only apply to cross border data transfer of European Union data.
Biometric Technology	Biometrics are body measurements and calculations related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric technologies generally refer to the use of technology to identify a person based on some aspect of their biology.
Choice	Privacy Choice is giving individuals the opportunity to determine what information we can collect, how we can use it, and with whom we can share it. Specifically, privacy choices about the use of data give a Data Subject/Individual the opportunity to determine how the Data Subject/Individual is contacted for marketing (by phone, mail, email etc.).
Data Harvesting	Data harvesting is a process where a small script, also known as a malicious bot, is used to automatically extract large amount of data from websites and use it for other purposes.
Data Subject/Individual	A data subject is any person whose Personal Data is being collected, held or processed. The terms 'Data Subject' and 'Individual' are used interchangeably.
De-identified:	De-identified data is data that has had enough Personal Information removed or obscured such that the remaining information does not identify an individual to a recipient and there is no reasonable basis to believe that the recipient of the information can use it to identify an individual. Generally, in place of Personal Data, a unique identifier is used (e.g., GUID, cookie, etc.) to create "de-identified Personal Data" which allows the recipient of the information to distinguish one individual from another for profiling or analytics purposes but would not allow the recipient to re-identify an individual.
Explicit Consent	When users are required to take an affirmative action (or proactive step) in order to provide their consent. This may include, for example, checking a tick box (which was not pre-checked), clicking "I accept" or any other positive action that maybe required by local law. Explicit Consent is also known as; **opt-in**, Affirmative, Express or Direct consent.
Facial Recognition	Facial recognition is a method of identifying or verifying the identity of an individual using their face. Face recognition systems can be used to identify people in photos, video, or in real-time.
Internet of Things (IoT):	The Internet of Things refers to uniquely identifiable objects and their virtual representations in an Internet-like structure. The concept is to equip all objects in daily life with identifiers so that they could be managed and inventoried by computers.
Joint Marketing	Activity where nonaffiliated companies market financial products or services together based upon a formal agreement between them.

Model Contracts/Standard Contractual Clauses	Legal tools to provide adequate safeguards for data transfers from the EU or the European Economic Area (EEA) to third countries. Additionally, other countries (i.e. Brazil) use Standard Contractual Clauses.
(Privacy) Notice	Clear and complete disclosure to individuals of how AXP|PAYBACK collects, uses, and shares Personal Data (online and/or offline). It is a promise to our customers of how we will treat their Personal Data. A Privacy Notice is a legally binding agreement. A Privacy Notice contains three key elements: 1. What Personal Data we want to collect; 2. How we intend to use it; 3. With whom we intend to share it
Online Behavioral Advertising	Websites or online advertising services that engage in the tracking or analysis of search terms, browser or user profiles, preferences, demographics, online activity, offline activity, location data, etc., and offer advertising based on that tracking.
Opt-In	A privacy choice in which an individual has affirmatively provided consent for AXP|PAYBACK to send the individual specific marketing or servicing messages. Data use or Data Subject/Individual contact is prohibited unless the individual expressly permits (or consents to) such use.
Opt-Out	A privacy choice in which an individual can specifically request to be excluded from or deleted from a direct marketing list (such as for telemarketing, direct mail, or e-mail). Data use or Data Subject/Individual contact is permitted unless the individual expressly prohibits or 'opts-out' of that use.
Permissible Purpose	Personal Data can be collected, used, or shared only for the purpose specified in the notice to the Data Subject/Individual. If the purpose has not been specified in the notice, you cannot collect, use, or share this data for that purpose.
Persistent Tracking (Cookies)	A small text file stored on a client machine that may later be retrieved by a web server from the machine. Persistent Cookies are stored on a user's device to help remember information, settings, preferences, or sign-on credentials that a user has previously saved. Cookies allow web servers to keep track of the end user's browser activities and connect individual web requests into a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session by recording that they have successfully supplied their username and password already.
Personal Data / Personally Identifiable Information (PII)	Personal Data / PII refers to information, in any form, that identifies, or can be used in combination with other information available to the organization to identify, an individual (i.e., current, former or potential customers or employees, or any other person) and includes any information that is associated with an identified individual. Please contact your local Market Compliance Officer (MCO) regarding relevant market data protection policies for market specific interpretations and requirements. Examples of PII include, but are not limited to, Card Number; Individual's name in whole or in part; Address; Email Address; Phone Number; Social Security Number in whole or in part; other government-issued ID number like Driver's License #, non-Driver's license #, Passport #, national ID #s of other countries; Date of Birth or Age; Bank Account or other account information; Mother's maiden name; User ID; IP Address; Location-based data; ID of mobile device/cell phone; Racial/Ethnic Origin; Political opinions; Religious or philosophical beliefs.
Precise Location Data	Data obtained from a device that provides information about the physical location of the device and that is sufficiently precise to locate a specific individual or device.
Privacy Choice	Privacy Choice is an option given by AXP|PAYBACK to a Data Subject/Individual* to determine what Personal Data AXP|PAYBACK processes - including what AXP|PAYBACK can collect, how AXP|PAYBACK can use it, and with whom it can be shared. Law, regulations, and rules set by self-regulatory bodies, which AXP|PAYBACK is a member of, or driven by AXP|PAYBACK's internal policy dictate privacy Choice requirements. *Data Subject/Individual: customer, prospect or employee. A corporation and merchant may also be considered a User for privacy choices, as required under applicable local law or regulation.
Privacy SME	Designated individuals who provide privacy leadership, guidance and are points of contact within their respective organizations for all matters related to Privacy. The SME works with leaders and colleagues to ensure that Personal Data is processed in accordance with applicable privacy requirements by: Developing privacy policies procedures and guidance / Identifying best practices and implement solutions around the collection, use and disclosure of customer and employee data developing privacy education/training.

Processing	Processing of Personal Data/PII refers to any action taken in relation to Personal Data/PII and includes collecting, storing, altering, accessing, using, transferring, receiving, sharing or destroying Personal Data/PII.
Profiling	The collection and analysis of consumer behavior over a period of time to draw inferences about their preferences or characteristics for the purpose of creating a record of information (or 'profile') based on those inferences. A 'profile' may include information about both declared and inferred consumer interests.
Real-time Geographic tracking	Real-time geographic tracking refers to the capture or tracking of an individual's current physical location, as opposed to use of geographical demographic information. For example, using the location data from the individual's mobile device to identify the nearest ATM/Cash point is use of real-time location information as the process involves capturing the individual's physical location at the time the location information is being used. Other location information differs from real-time location information because it does not capture or track the individual's location at that actual time. For example, use of a customer's billing post code for targeted marketing is use of geographical demographic information, but is not use of real-time location information as the post code does not necessarily identify their precise physical location.
Screen Scraping	Screen scraping is the act of copying information that shows on a digital display so it can be used for another purpose. Visual data can be collected as raw text from on-screen elements such as a text or images that appear on the desktop, in an application or on a website.
Sensitive Data Element	A data element that presents risk to the enterprise. Includes elements that, if used in a particular context, create PII risk and elements requiring controls for use both internally and externally.
Sharing	Sharing Personal Data' means disclosing, transferring or otherwise giving a copy of it to another party, as well as allowing another party to access to Personal Data, even if they access Personal Data held on AXP|PAYBACK systems or property.
Web Scraping	Web Scraping (also termed Screen Scraping, Web Data Extraction, Web Harvesting etc.) is a technique employed to extract large amounts of data from websites. It is a form of copying, in which specific data is gathered and copied from the web, typically into a central local database or spreadsheet, for later retrieval or analysis.