Third Party Lifecycle Management 2.0.

Due Diligence Activities

Level 2

Sections:

1. Anti-Corruption

If the Anti-Corruption Domain Risk Rating = High or Moderate, then **DD AC1 – DD AC 12** will trigger.

Anti-Corruption Due Diligence (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.

1

Q#DD AC1 | Has there been any incident, investigation, or allegation of bribery, corruption, fraud, money laundering, misrepresentation, or similar conduct related to your business entity or any associated persons within the past 5 years?

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the required explanation in the comment box.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

2

Q#DD AC2 | Provide the information below for any director, officer, member of executive management, general manager, and employee with day-to-day management responsibilities involving the proposed or existing engagement with AXP|PAYBACK. Indicate whether any of these individuals is a Government Official.

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with accurate information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

3

Q#DD AC3 | Provide the information below for any owner who: (i) owns or exercises control over 25% or more of your business entity; or (ii) to the extent known, is a Government Entity (as defined at the end of this questionnaire) or Government Official.

SME Rating = MATERIAL

Note: LOBCO/MCO should approve or reject the relationship, confirm whether the third party is performing intermediary services, and escalate to GAC where applicable.

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with accurate information.

- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

4 **Q#DD AC4 | Will your business entity interact with any Government Entity or Government Official on AXP|PAYBACK's behalf as a part of the scope of services (or any amendment, schedule, or statement of work) being provided to AXP|PAYBACK?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the additional relevant information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

5 **Q#DD AC5 | Does the compensation for any individuals who will be involved in providing services to AXP|PAYBACK include any outcome-based compensation, such as an incentive, bonus, success fee, or commission, in connection with activity on behalf of AXP|PAYBACK?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

6 **Q#DD AC6 | Does any director, officer, member of executive management, general manager, or employee with day-to-day management responsibilities involving the proposed or existing engagement with AXP|PAYBACK hold director, officer, or other management positions, or own or control 25% or more of the equity or stock of any other companies or entities?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the additional relevant information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

7 **Q#DD AC7 | Will your business entity outsource any part of the AXP|PAYBACK engagement to any Third Parties who are or who will interact with a Government Entity or Government Official?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the additional relevant information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap.

8 **Q#DD AC8 | Will your business entity interact with any Government Entity or Government Official on AXP|PAYBACK's behalf as a part of the scope of services (or any amendment, schedule, or statement of work) being provided to AXP|PAYBACK, per question 4?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the additional relevant information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap.

9 **Q#DD AC9 | Does your business entity have an anti-corruption policy and related compliance program, including, but not limited to, meals, gifts and entertainment guidelines, Third Party/vendor oversight, established hiring protocols, and dedicated compliance personnel?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap.

10 **Q#DD AC10 | Does your business entity provide anti-corruption training?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap.

11 **Q#DD AC11 | Within the last 5 years, has your business entity been known by any other name?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option if the ACDD Questionnaire is received from the Third Party and is filled with appropriate response option along with the additional relevant information.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

12 **Q#DD AC12 | Please provide the Third Party's Signed Certification.**

SME Rating = MATERIAL

The TRM is required to attach the relevant document i.e. a copy of Third Party's signed certificate authorizing that the information filled out in the questionnaire is correct and complete.

Response options & guidance:

- **Yes:** Select this "Response Option if the Third Party has provided the certification statement showing that the information shared in the questionnaire is correct and complete.
- **No:** Select this "Response Option" if the Questionnaire is not received from the Third Party. Selecting this "Response Option" would result in a Material Pre-contract Gap.

13 **Q#DD AC13 | MCO/LOBCO approval has been obtained.**

SME Rating = MATERIAL

Note**:** The name of the LOBCO/MCO will need to be entered as well as the date of the approval from the LOBCO/MCO for the screening alert. The email evidence of the LOBCO/MCO's approval must be saved and uploaded. Approval includes the questionnaire responses, and the screening results escalated to the relevant LOBCO/MCO for approval, noting any red flags on the questionnaire and any screening matches that have been identified. LOBCO/MCO should approve or reject the relationship, confirm whether the third party is performing intermediary services, and escalate to GAC where applicable.

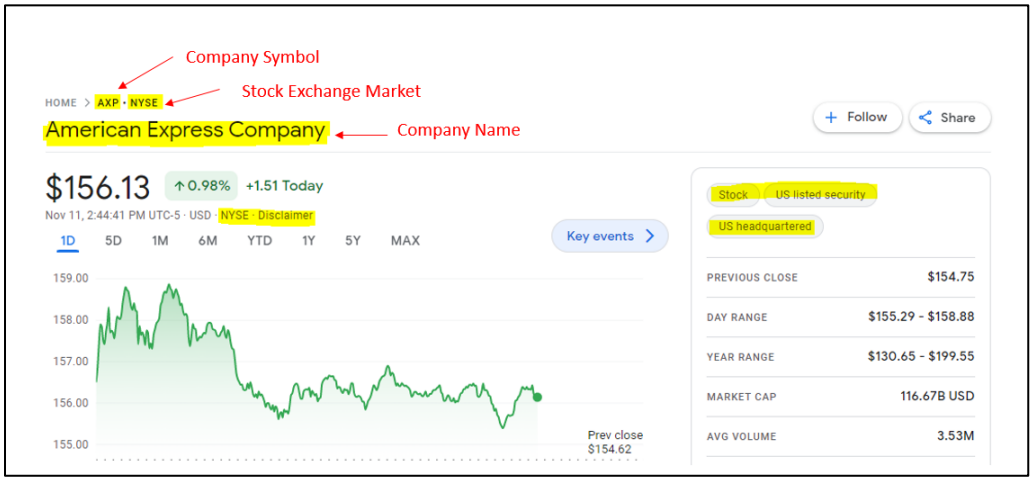
Response options & guidance:

- **Yes**: Select this "Response Option" if TLM analyst has obtained the MCO/LOBCO approval.
- **No**: Select this "Response Option" if TLM analyst has not obtained the MCO/LOBCO approval. Answer would result in a Material Pre-contract Gap.

14 **Q#DD AC14 | Provide a screenshot of the Third Party traded on the recognized stock exchange.**

SME Rating = MATERIAL

The TRM is required to capture evidence that the third party is publicly traded in the market exchange selected in question TRA 5.5. Acceptable evidence includes screenshots, or documents reflecting the third party's name, trading symbol, and stock market exchange selected in TRA 5.5.



Note: Google or yahoo finance searches are useful tools to validate stock and market traded

Response options & guidance (To upload evidence and complete the due diligence activity select):

- **Yes**: Select this "Response Option" if you upload evidence.
- **No**: Select this "Response Option" if TLM analyst has not obtained the evidence.

2. Anti-Trust

15 **Q#DD AT1 | Notification to Anti-Trust Team**

SME Rating = MODERATE

An escalation to the GCO Anti-Trust team for evaluation is required. GCO Antitrust SME antitrustlegalteam@aexp.com.

Response options:

- DD Attempted, **Evidence Received**
- DD Attempted**, Not Received**

Acceptable Evidence:

The TRM must provide evidence this has occurred - Notification proof, the Anti-Trust GGO SMEs must clear any anti-trust concerns and proof of this must be uploaded in ProcessUnity.

3. Compliance

When contacting for SME attestation or alternate artifact approval for compliance DD, please go to the LOBCO/MCO. Do not select "Not Applicable, SME Attested" response option just because a third-party is unwilling to provide documentation, nor should you be going to your LOBCO. Please select "Evidence Not Received" response option if the third party has not provided the required documentation.

16 **Q#DD C1 | Compliance Policy**

SME Rating = MATERIAL

Response options & guidance: select the appropriate option and attach the relevant document showing Third Party's Compliance Policy which should establish the framework for identifying, assessing, controlling, measuring, testing, monitoring, and reporting compliance risks, and potential compliance risks, as well as ensuring that there is a culture of compliance, employees are trained on compliance matters and there is regulatory oversight:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document showing Third Party's Compliance policy. Answer would result in a Pre-contract Gap.

- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document showing Third Party's Compliance Policy that covers the overall framework for a company's compliance risk program and includes the following elements:

- Leadership Engagement, Compliance Policy Training & Employee Communication, Effective training and regular communications regarding compliance matters, Regulatory Oversight (Board and Management), Monitor regulatory environment, Identification of rules and regulations, Risk Assessment and Mitigation
- Risk process helps ensure that resources are directed at the most significant and pressing compliance risks Compliance Monitoring
- On-going supervision to provide assurance that these adequately mitigate or minimize risk as intended, Compliance Testing
- Review methodologies such as inquiry, observation, validation, verification, and re-performance, Compliance Reporting & Analysis
- Provides adequate compliance oversight, addresses gaps and emerging trends, Escalation of Compliance Issues.

17 **Q#DD C2 | Legal Inventory**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing Third Party's Compliance policy. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence: Upload an evidence where the Third Party has provided a documented legal inventory and a description of a system, database or repository that houses the specific laws and regulations by jurisdiction, line of Business and category of law. The legal inventory policy provided by the Third Party should include:

- Documented process for identifying laws and regulations.
- Independent function that oversees compliance with laws and regulations.
- Process to ensure changes to laws or regulations are identified and implemented.

18 **Q#DD C3 | Compliance Monitoring and Testing or Audits**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing Third Party's Compliance Monitoring and Testing or Audits. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence: Upload an evidence where the Third Party has provided a documented compliance monitoring and testing process that includes the following elements:

- Risk-based approach to compliance, monitoring and testing
- Description of the Compliance monitoring program
- Compliance testing plan, methods and schedule (frequency)
- Staff for Compliance Monitoring role
- Description of risk assessment methodology
- Test program includes identifying the testing universe,
- Results reporting
- Issue follow-up and validation
- Escalation process
- Evidence of addressing gaps/deficiencies and corrective action reports

OR

- A documentation of internal Compliance audits, or external regulatory reviews related to the service being provided, performed within the last. The documentation must include: List of Internal/External Compliance Audits in the prior 12 months | Results from prior 12 months internal/external Compliance audits.

Note: SSAE 16, SOC1/2, reports are not acceptable to satisfy this activity on face value. The TLM Compliance analyst will need to review the entire report and determine if it clearly identifies Regulatory Compliance controls are tested and reviewed. If the report does not include the required information pertaining to Compliance, the Business Unit will need to engage their LoBCO/MCO to review/approve the artifact as alternate evidence based on the service being provided.

19 **Q#DD C4 | Third Party's Compliance Call Monitoring procedures**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document showing Third Party's Call Monitoring procedures/policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document showing third party's Call Monitoring procedures that includes the following elements:

- Documented call monitoring policy and procedures
- Key performance metrics evaluated and feedback process
- Evidence of call monitoring and/or a call monitoring schedule,
- Evidence of call monitoring testing and results
- Reporting and escalation process.

20 **Q#DD C5 | Third-Party's Complaint Handling procedures**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document showing Third Party's Complaint handling procedures. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document showing third party's Compliant Handling procedures that includes the following elements:

- How the Third-Party receives complaints –phone, paper, web, etc.
- Description of how complaints are registered/recorded
- A complaint documentation process, Instructions to employees on how to handle complaints
- Escalation process
- Evidence of complaints
- Details surrounding how regulatory complaints are handled, Complaint tracking, analysis, and reporting.

In some BU's the third-party is not authorized to have their own internal process and is required to follow AXP's policy. If the third-party is following AXP's Complaint handling/tracking process and/or forwarding Complaints to AXP, the BU can provide a statement outlining this along with their internal AXP Complaint Handling policy/process as supporting documentation. This will satisfy the due diligence activity and does not require SME approval.

21 **Q#DD C6 | Customer Fairness (Consumer Protection/Anti-Discrimination Program)**

SME Rating = MATERIAL

The Third Party must provide a documented **Customer Fairness Program** (in International Markets, it may be called something else) that outlines consumer protection and how all credit product decisions and services are provided to all current and future customers are engaged fairly and non-discriminatory. All staff have adequate training on that policy.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.

- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing Third Party's Compliance policy. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- A document that outlines the Third Party's Customer Fairness Program. An effective Customer Fairness Policy would be an established policy where all staff have adequate training and that there is a guarantee that all products and services available to all current and future customers are engaged fairly and non-discriminatory.
- Acceptable Alternate document = If the Third Party can demonstrate their employees have been trained on Customer Fairness in absence of a formal policy. Note: Alternative artifacts require alignment of the risk SMEs and must be attached.

22 **Q#DD C7 | Third Party's Record Retention policy and procedures**

SME Rating = LOW

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document showing Third Party's Record Retention policy and procedures. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document showing third party's Record Retention policy and procedures that includes the following elements:

- Schedule of record retention
- Classification of records.

23 **Q#DD C8 | Third-Party's incentive program description/documentation.**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence of the Third Party's incentive program description/documentation. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document showing Third Party's incentive program description/documentation, policy should include adherence of the Third-Party's incentive program to regulatory requirements. The Third-Party must provide a documented description of any Incentive Program(s) for representatives that includes the following elements:

- Description of incentive program for representatives
- Evidence of controls in place (call monitoring, sales verification, etc.) to support the Incentive Program
- Penalties for poor performance, including but not limited to Compliance issues.

24 **Q#DD C9 | Third-Party's Training Program and curriculum.**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the Third Party's training Program and curriculum. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document/evidence showing third party's Training Program, including:

- Description of the Compliance Training Program
- Training Schedule and Frequency
- Training Curriculum / List of Courses
- Method to deliver training and track and report training completion
- Description of the Third-Party's procedure or manual repository

Important Call out: This DD activity is only required if the third party is NOT taking AXP training and LOBCO does not have to be engaged to mark N/A for this specific DD activity.

25 **Q#DD C10 | Current Inventory of relevant Service Market License(s) required by staff members to provide the service (i.e. business, state, local, agent, etc.).**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the third party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the Third Party's current Inventory (i.e. list) of relevant Service Market License(s) required to perform the service for AXP|PAYBACK. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a document/evidence showing third party's documented current Inventory (i.e. list) of relevant Service Market License(s) required to perform the service for AXP. In addition, licenses allowing agents to perform collections, sales, insurance related activities or legal representation are required for review.

26 **Q#DD C11 | BU notification proof to AXP AML team.**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload a copy of the e-mail notification sent to the AML team or a confirmation from the AML team where they acknowledge review of the Third-Party service.

27 **Q#DD C12.1 | Is the Beneficial Owner a Government Official or Government Entity?**

Response options & guidance: Select ONE answer that best matches the beneficial owner relationship.

- **Government Official**
- **Government Entity**
- **Beneficial Owner is neither a Government Official or Entity**

Other components:

DD – C12.2: Is the Beneficial Owner a natural person or legal entity?

DD – C12.2.1: Beneficial Owner: Full Name of the natural person or Full Legal name of Business Entity

DD – C12.3: If Beneficial Owner is Natural Person provide: Nationality or if Beneficial Owner is Legal Entities provide: Country of Business Entity registration.

DD – C12.4: If Beneficial Owner is Natural Person provide: Date of Birth or TX ID Number or if Beneficial Owner is Legal Entities provide: TIN (if available).

DD – C12.5: If Beneficial Owner is Natural Person provide: Position or If Beneficial Owner is Legal Entities provide: Doing Business As (DBA) Name (if applicable).

DD – C12.6: If Natural Person - Populate Home Address of the natural person or of Legal Entity - Populate Physical Address of the entity

If there is more than one beneficial owner and/or a government official/entity, the fields in Process Unity with fresh number, for example, 13.1-15.5.

4. Financial Health Assessment (FHA)

Note: * Critical and high resiliency engagements **require full review;** i.e., collection of updated financials, when no credit rating is available or rating is outdated (TRM with TLM COE Support). Moderate, Low engagements or prepayment of $1M requires data input of current FHA rating, if available. **Critical and High resiliency engagements will trigger FHA 02 through FHA 05.**

28

Q#DD FHA1 | Automated CRU rating

SME Rating = HIGH

Confirm if a current rating exists in iCRUSE. CRU will analyze the risk associated with the Third Party services and assign a rating. Note: TRMs, BU TLM Leads, or TLM Analysts firstly can look on the current TLM FHA Report*, located on the TLM Square Page under Financial Health Assessment (FHA) Documents to determine if there is a current rating for the third party. Please follow the below steps:

- Open FHA Report from Financial Health Assessment (FHA) Documents
- Column A - "Third Party Level 3 (Unique)"-Select Third Party Name
- Column D – "Current Rating" – Leverage the rating available and update this in Process Unity
- Column E – "Current Rating Date" – Rating date available should be within 12 months
- Upload a screen shot of the rating shown within the TLM FHA Report into Process Unity

**If the FHA Score is B or lower see Additional Action Required below.*

If unable to locate a rating from the FHA report, then follow the below steps.

The Pre-Contract Analyst/TRM will send an email to the FHA team at Supplier.Health.Analysis@aexp.com to confirm in the Third-Party has a current FHA Rating in iCRUSE. The FHA team will provide the iCRUSE rating or there is not current rating on file and if any additional actions are required.

This DD activity will trigger when:

- TRA- Third Party Details TP.06 (Pre-payment of $1M) = **Yes**, OR
- Overall Risk (Final) = High AND Resiliency = Moderate or Low (in the Core Pillars/Overall/Residual Ratings)

Response options:

- Select the appropriate rating per email response from FHA team or from the TLM FHA Report. Attach either a screen shot from the TLM FHA Report or the email as evidence and enter the FHA Rating, CO ID, CRU#, and Rating Date in the comments OR
- Select No Fin Stmnt, attach the email from the FHA team and add to the comments: No rating found in iCRUSE

AAA	BB
AA+	BB-
AA	B+
AA-	B
A+	B-
A	C1
A-	C2
BBB+	C3
BBB	C4

BBB-	Default
BB+	No Fin Stmt

Acceptable Evidence:

- Upload a screen shot of the rating shown withing in the TLM FHA Report or an email from the Financial Health Assessment team providing the current FHA rating. OR an email from the Financial Health Assessment team confirming that there is no current FHA rating on file.

***Additional Action Required:**

Please be aware that an FHA Score of B or lower will have a downstream impact and will trigger an additional requirement.

1. Vendor will be reported on the TLM Watchlist
2. Exit & Replacement (E&R) Plan needs to be in place – Refer to Exit & Replacement Guidance
   a. E&R is not applicable for Co-brand services/products
   b. E&R Plan is due in 90 days from the TLM BU Lead meeting/TRMC, whichever is earlier.

When the vendor is reported on the Watchlist, there is a field that identifies if an E&R is in place. If there is already an E&R in place for this vendor, share it with the FHA team so it can be documented. Otherwise, please work with the TRM to create the E&R and share once it is complete.

29 **Q#DD FHA1.01 | Rated Company ID**

SME Rating = HIGH

Enter the iCruse and Company ID provided by the FHA Analyst.

Response Option & guidance: This is a freeform field where the TRM/Pre-Contract Analyst will receive the Company ID from the FHA Analyst.

30 **Q#DD FHA2 | Are the most recent 3 years audited financial statements for the contracted entity (TP L3) available?**

Note: If financial statements are not available for the contracted entity, a rating based on parent entity statements may be considered (See FHA3 and FHA4).

SME Rating = HIGH

Important: The TRM has 30 days to submit financial statements. If statements are not submitted by the due date, a gap may be opened in ProcessUnity, and the TRM has 30 days to close the gap with submission of financial statements.

TRM to obtain the last 3 years of financials for the Contracted Entity (TP L3).

This DD activity will trigger when:

- Critical Designation Final = **Yes**, OR
- Overall Risk (Final) = High, Moderate, Low AND Resiliency = High

Response Option & guidance:

- **DD Attempted, Evidence Received** select this "Response Option" if the financials for the contracted entity (TP L3) have been provided, attach the financials, and add comments.
- **DD Attempted, Not Received:** - select this "Response Option" if:

- no financials for the contracted entity have been received and add comments financials for contracted entity is not received OR
- the financials for the parent entity were provided, add comments that the financials for the parent entity were provided

If the financials are provided for either the contracted entity (TP L3 or the parent entity (TP L1, 1.5, or 2) mark either FHA 02 of FHA 03 response options appropriately and add in the comment sections "financials received for contracted entity or parent entity" e.g. if the Third Party provides the financials for a parent entity, then, for FHA 02, you would select DD Attempted, Not Received, and in the comments section, add "financials received for parent entity".

Acceptable Evidence:

- Upload a document showing 3 years of Audited Financials for the Contracted Entity (TP L3)

Note: If third party do not share their audited financial and if it is submitted without information it may result to lower rating, possible gap, and added to the Watchlist.

31 **Q#DD FHA3 | Are the most recent 3 years audited financial statements for the Parent entity of the contracted entity and the annual contracted spend available? If yes, attach statements.**

If no financial information is available for the contracted Third Party, the strength of the entity relationship may be leveraged. 1) TRM's requests three years audited financial statements on the contracted Third Party's parent entity. A minimum of two years of audited financial statements may be considered, and unaudited as a last resort. 2) TRM completes the additional questions that evidence implied parental support.

SME Rating = HIGH

TRM to obtain the last 3 years of financials for the Parent Entity (TP L1,1.5,2) and responses to the 10 parent/subsidiary questions. This DD Activity **will trigger when:**

- Critical Designation Final = **Yes**, OR
- Overall Risk (Final) = High, Moderate, Low AND Resiliency = High

Response Option & guidance:

- **DD Attempted, Evidence Received** select this "Response Option" if the financials for the Parent entity have been provided, attach the financials, and add comments.
- **DD Attempted, Not Received:** - select this "Response Option" if no financials for the Parent entity have been received and add comments financials received for Parent entity is not received.

Acceptable Evidence:

- Upload a document showing 3 years of Audited Financials for the Parent Entity (TP L1, 1.5, 2)
- Complete FHA4.0 – FHA4.10 based on TP responses to FHA Refresh- Financials Required email template

Note: If third party do not share their audited financials it may result in a lower rating, possible gap, and added to the Watchlist.

Note: Upload the completed template from the third-party showing the responses to the 10 parent/subsidiary questions.

If the financials are provided for either the Contracted Entity (TP L3 or the Parent Entity (TP L1, 1.5, or 2) mark either FHA 02 or FHA 03 response options appropriately and add in the comment sections "financials received for Contracted Entity or Parent Entity". For example, if the Third Party provides the financials for the Contracted Entity (TP L3), then, for FHA 03, you would select DD Attempted, Not Received, and in the comments section, add "financials received for Contracted Entity.

32 **Q#DD FHA4-FHA9 | Are the most recent 3 years audited financial statements for the Parent entity of the contracted entity and the annual contracted spend available? If yes, attach statements.**

Responses to the 10 parent/subsidiary questions are required when the name on the financials is different than the Contracted Entity (TP L3). **Q.DD – FHA 4** through **Q.DD – FHA 4.09** – complete using the responses received from the Third Party.

SME Rating = HIGH

This DD Activity will trigger when: DD FHA2 = DD Attempted, Not Received

Response Option & guidance:

- **Yes**
- **No**

Acceptable Evidence:

- Upload an email from the Third Party showing responses to the 10 parent/subsidiary questions.

33 **Q#DD FHA5 | Fundamental CRU-CRU Rating.**

SME Rating = HIGH

This DD Activity will trigger when:

- Critical Designation Final = **Yes**, OR
- Overall Risk (Final) = High AND Resiliency = High (in the Core Pillars/Overall/Residual Ratings)

Response Option & guidance:

AAA	BB
AA+	BB-
AA	B+
AA-	B
A+	B-
A	C1
A-	C2
BBB+	C3
BBB	C4
BBB-	Default
BB+	No Fin Stmt

Acceptable Evidence:

- Upload an email from the Financial Health Assessment team providing the current FHA rating. Provide the most recent 3 years audited financial statements for the contracted entity OR
- Provide the most recent 3 years audited financial statements for the parent entity with the 10 responses to the 10 additional questions from the FHA Team

ProcessUnity Instructions: Select appropriate rating, attach the email from the FHA team, and add to the comments: the CO ID, CRU#, Rating, Rating Date.

34 **Q#DD FHA5.01 | Rated Company ID**

SME Rating = HIGH

Enter the iCruse and Company ID provided by the FHA Analyst.

Response Option & guidance: This is a freeform field where the TRM/Pre-Contract Analyst will receive the Company ID from the FHA Analyst.

5. General Engagement

Note**:** The policy pack will still be an acceptable Alternate Artifact for the GE DD control activities. This is applicable for SS&BE managed contracts only.

35 **Q#DD GES1 | Third Party's Code of Conduct policy**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM Contact Privacy Request document for more details.

Acceptable Evidence: Upload the evidence showing third party's Code of conduct policy. The Third Party should provide a comprehensive Code of Conduct Policy that includes the following elements:

- Defined principles; values; and standards to be adhered by all employees
- Assurance that employees conduct business with all applicable laws
- Supports Customer Fairness-Forbids facilitating payments (anti-corruption)
- Addresses Conflicts of Interest
- Ensures Confidentiality of information
- Describes consequences of non-compliance with the Code of Conduct
- Demonstrates Employee Acknowledgement and Acceptance.

36 **Q#DD GES2 | Third Party's valid business license(s) or industry certification(s), relevant to the services provided to AXP|PAYBACK**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's valid business license(s) or industry certification(s). The Third Party must provide evidence of the license or permits that matches the business name; and license or permit that is current.

37 **Q#DD GES4 | Third Party's Incident Reporting and Media Management Policy**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: The Third Party must provide evidence of policy outlining how the Third Party communicates incidents to the public including parameters on who is responsible for communicating with the media or publicly discussing the company over the internet (blogs; social media; etc.) and how; similar to AXP' External Communications & Disclosure (AEMP18).

38 **Q#DD GES5 | Third Party's Background Check Policy**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's background check Policy. The evidence should include all the components that can describe how the Third Party's conduct their background checks

and what requirements are taken care of while conducting background checks of potential employees. (i.e.; citizenship or legal convictions), including the process to reject/terminate those who fail.

39 **Q#DD GES6 | Third Party's Criminal Background Check Policy Documentation**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's Criminal Background Check Policy. The evidence should include all the components that can describe how the Third Party's conduct their background checks and what requirements are taken care of while conducting background checks of potential employees. (i.e., citizenship or legal convictions).

40 **Q#DD GES8 | Better Business Bureau (BBB) Review**

BBB review is only applicable currently to third parties with U.S. based office. This verification is conducted by TLM COE through the. BBB website.

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's BBB review. The evidence should show that the Third Party has a positive public customer perception on the BBB and is accredited.

41 **Q#DD GES9 | World Check Report review**

This verification is conducted by TLM COE

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the third party's Code of Conduct policy. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's World Check review. The evidence should show that the Third Party has positive findings from the external background check and the media reports pulled, should describe that there are no negative results or finding in terms of bankruptcies, Liens and Judgements when the third party's external background and media report is being pulled through various tools such as Dow Jones, World Check etc. If the SME was consulted and reviewed the report due to a finding the SME response email must also be uploaded into ProcessUnity.

42 **Q#DD GES10 | Exit and Replacement Policy**

Complete an Exit and Replacement Plan.

SME Rating = MODERATE

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing Third Party's Exit and Replacement Plan. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Upload evidence where the TRM has provided a completed Exit and Replacement Strategy. Note: Completed implies that all sections within the form are filled-in, if any section(s) do not apply then appropriate commentary is included.

43 **Q#DD GES11 | Third Party's Supplier Management Policy or Program**

Provide a copy of the Third Party's Supplier Management Policy or Program.

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing Third Party's Supplier Management Policy and Program. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Upload evidence where the Third Party has provided an established / comprehensive Management Program that discusses the Third Party's framework to manage their suppliers inclusive of the following components: Pre-contract due diligence on suppliers inclusive of financial evaluation. Requirement of contract execution prior to commencement of actual work. Ongoing monitoring of supplier's activities, process to review, approve and monitor the Fourth-Party compensation when their incentive compensation is applicable. Such policy or procedure must be enterprise-wide and must be a published document.

44 **Q#DD GES11.1 | Does the Supplier/Third Party Management Policy/Program include pre-contract DD inclusive of financial health assessment, risk assessment, information security and compliance?**

SME Rating = MATERIAL

Note: When one of the approved AXP cloud providers have been identified as a material subcontractor of the third-party, DD GES 11.1 -11.4, and GES 12, are deemed "Not Applicable". Please refer to the TLM Programmatic DD Exception 5 Cloud Providers stored in ProcessUnity's Programmatic Exceptions document repository.

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- The Third Party must provide evidence of an established / comprehensive Management Program that discusses the Third Party's framework to manage their suppliers inclusive of the following components: Pre-contract DD on suppliers inclusive of financial evaluation.

45 **Q#DD GES11.2 | Does the Supplier/Third Party Management Policy/Program require executed contracts with suppliers?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence

- The Third Party must provide evidence of an established / comprehensive Management Program that discusses the Third Party's framework to manage their suppliers inclusive of the following components: Requirement of contract execution prior to commencement of actual work.

46 **Q#DD GES11.3 | Does the Supplier/Third Party Management Policy/Program include ongoing monitoring of the Third Party's suppliers?**

SME Rating = MATERIAL

Note: When one of the approved AXP cloud providers have been identified as a material subcontractor of the third-party, DD GES 11.1 -11.4, and GES 12, are deemed "Not Applicable". Please refer to the TLM Programmatic DD Exception 5 Cloud Providers stored in ProcessUnity's Programmatic Exceptions

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- The Third Party must provide evidence of an established / comprehensive Management Program that discusses the Third Party's framework to manage their suppliers inclusive of the following components: Ongoing monitoring of supplier's activities.

47 **Q#DD GES11.4 | If there is an incentive compensation arrangement with the Fourth Party, does the policy indicate a process to review, approve and monitor the Fourth Party compensation?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)
- **Not Applicable**, no Incentive compensation arrangement

Acceptable Evidence:

- The Third Party must provide evidence of an established / comprehensive Management Program that discusses the Third Party's framework to manage their suppliers inclusive of the following components: Process to review, approve and monitor the Fourth Party compensation when there is incentive compensation. Such policy or procedure must be enterprise-wide and must be a published document.

48 **Q#DD GES12 | Does the Third Party have an executed contract with each of the Fourth Parties/subcontractors?**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing that the Third Party has executed contract with each of the Fourth Parties/sub-contractors. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- The Third Party must provide documented evidence of the Third Party's executed contract with each of the Fourth Parties/subcontractors.

49 **Q# DD – GES13 | Please provide a documented description of the services that each of the Fourth Parties/Subcontractors provides to the Third Party, in support of the contractual obligation to AXP|PAYBACK.**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing description of the services that each of the Fourth-Parties/Subcontractors provides to the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Third Party must provide a documented description of services for each Fourth Party.

50 **Q#DD GES14 | Please attach the process flow depicting the workflows/dataflow (that includes all applicable Fourth Parties)?**

SME Rating = MATERIAL

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached showing the process flow which depicts the workflows/dataflow (that includes all applicable Fourth Parties) . Selecting this "Response Option" would result in a Pre-contract Gap.

- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence

- The Third Party must provide a documented process flow depicting the workflows/dataflow (that includes all applicable Fourth Parties).

51 **Q#DD GES15.01A-GES15.01J | Material Subcontractor Demographics**

TRM to work with Third Party to provide demographic information for Material sub-contractors.

Q#DD GES15.01A | What category of service will this material subcontractor provide?

SME Rating = MATERIAL

The AEMP10 chosen should be specific to the services provided by the subcontractor and can be different than the AEMP10 selected for the Third Party risk assessment. Select the response that most appropriately represents the service provided.

Response options: Freeform

- Fourth Party Name
- Fourth Party Address 1
- Fourth Party Address 2
- Fourth Party Address 3
- Fourth Party Country
- Fourth Party City
- Fourth Party State
- Fourth Party Postal Code
- Fourth Party URL

Acceptable Evidence

- TRM to work with Third-Party to provide demographic information for Material sub-contractors.

52 **Q#DD GES18 | India Data Localization Attestation**

This DD activity will trigger if the Third-Party services involves payment and/or settlement services (TRA3.2 = yes) and India is selected as services provided "to" is visual.

SME Rating = MATERIAL

Acceptable Evidence

- The Third-Party's email that includes the SIGNED Third-Party IDL Attestation letter. Note: It is necessary to upload both the third-party returned email and the IDL letter into ProcessUnity.

6. Information Security

A total point value of **41 or more**, indicating (moderate or high risk triggers DD activities for Anti-Corruption pillar.

53 **Q#DD IS/IT1 | Pre-Contract Physical Site Review with no open High-Risk Gap**

SME Rating = MATERIAL

The TRM must be able to provide evidence of a Pre-Physical review has been performed by the TSM team.

Response options & guidance:

- **Yes**: - Select this Response Option if Acceptable Evidence is attached
- **No**: - Select this Response Option if No Acceptable Evidence is attached. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

Acceptable Evidence:

- An uploaded screen print of the email publication of the Pre-P completed. In the comment text box, provide the document name, page, or section, or a screen print of the completed Pre-P in TSM ProcessUnity.
- An uploaded screen-print of the completed Pre-P shown within TSM ProcessUnity.
- In the event that the service is a renewal, or addition to a contract for an existing service that does not involve modification to IT infrastructure or the technology footprint of the service, a pre-Physical assessment may not be triggered. In these instances, a screen print of the publication of the most recent completed post-Physical assessment can be utilized as an alternative artifact for the DD activity. The Post-Physical assessment must have been completed in the past 3 years.

54 **Q#DD IS/IT2 | Pre-Contract Logical Review with no open High-Risk Gap**

SME Rating = MATERIAL

The TRM is required to attach the relevant screen-print of the email publication of the completed Pre-Logical assessment (Engagement Status Active) within ProcessUnity. In the comment text box, provide the document name, page, or section.

Response options & guidance:

- **Yes**: - Select this Response Option if Acceptable Evidence is attached
- **No**: - Select this Response Option if No Acceptable Evidence is attached. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

Acceptable Evidence:

- An uploaded screen print of the email publication of the Pre-P completed. In the comment text box, provide the document name, page, or section, or a screen print of the completed Pre-P in TSM ProcessUnity.
- An uploaded screen-print of the completed Pre-P shown within TSM ProcessUnity.
- In the event that the service is a renewal, or addition to a contract for an existing service that does not involve modification to IT infrastructure or the technology footprint of the service, a Pre-Logical assessment may not be triggered. In these instances, a screen print of the publication of the most recent completed Post-Logical

assessment can be utilized as an alternative artifact for the DD activity. The Post-Logical assessment must have been completed in the past 3 years.

55 **Q#DD IS/IT4 | Remediation of High-Risk Gaps**

SME Rating = MATERIAL

Note: In order to meet the DD criteria for acceptable proof, there are two options. The acceptable evidence, along with comments detailing the high-risk gap(s) closure, must be posted into Process Unity.

Response options & guidance:

In the Follow-up Comments, include the document name, and verification that shows all high-risk gaps are closed.

- **Yes**: if high risk gaps are closed – see Acceptable Evidence
- **No**: if high risk gaps are not closed – see Acceptable Evidence

Acceptable Evidence:

- Screenshot to show all high gaps have been closed within Process Unity OR
- An email request to Third-PartySecurityManagement@aexp.com asking them to provide you with the screenshot showing all high gaps have been closed within Process Unity.

Note: Multiple IS logic conditions are built between the SRA and TRA questionnaires that can cause this DD activity to trigger:

If SRA 1.1.1 (classification) contains Secret (Any)/Restricted (Any) **OR** *Compliance / Strategic SRA IRA 3.5 = Yes,* ***AND***

Compliance / Strategic SRA_IRA 3.5.1 = Yes or N/A ***AND*** *TRA 1.1 includes None Apply* ***AND*** *TRA 1.3 = any option other than "AXP issued laptop with AXP access credentials* ***AND*** *FRM Review = New.The TRM will engage the GI (Global Infrastructure) Hosting team to request approval to proceed with the onboarding Third Party services when the following conditions exist:*

- *Web based application (branded or otherwise)*
- *Mobile Platform application (branded or otherwise)*
- *Cloud solution or data center*
- *File transfer services or interfaces*

56 **Q#DD IS/IT5 | Central ID w/Status Validation**

SME Rating = MATERIAL

For R3 engagements, the Map Central ID entered during the DD phase satisfies this activity and IS/IT5a is showing auto-populated a screenshot no longer is required. Select Yes for the response option, and state in the comment section that a Central ID was mapped. For R4 engagements, this DD activity will trigger if IRA L1 1.2 = Internet Facing (web/mobile) application or Non internet Facing OR if TRA L2 1. 3 = API.

An existing Central ID is acceptable evidence.

Response options & guidance:

- **Pass**: when Central ID-Lifecycle status = "Development" or "Production" or "Maintain"
- **Fail**: when Central ID-Lifecycle status "Envision" or "Exit"

If the Central ID- Lifecycle Status changes to "Envision" or in "Exit" Status, the below treatment needs to be followed:

- After DD Review Complete: - if the Central ID Lifecycle status changes from "Development", "Production", or "Maintain" to "Envision" or "Exit", the assessment would automatically rescopes to DD submission stage. At this point an auto generated email will be sent to the Onboarding TRM and Onboarding BU TLM Lead of that particular engagement (TLM ID#) which will say: "Your Central ID has reverted to an unacceptable Central Lifecycle status. Please action appropriately."
- After COERA has been issued or assessment is closed: -if and when the Central ID Lifecycle status is either "Envision" or "Exit", an auto generated notification will be sent to the Onboarding and Ongoing TRM and the Onboarding and Ongoing BU TLM Lead of that particular engagement (TLM ID#) which will say: "Your Central ID has reverted to an unacceptable Central Lifecycle status. Please action appropriately. Please create a new central ID or action the existing one if the TLM assessment is to continue. You will have 30 days to action until this negatively affects your Business's Control and Compliance Ratings and escalates to RAF metric Reporting."

Note: This dd activity is required if IRA L2 1.3=API, OR L2 1.3=SFT, OR L2 1.3=HTTPS] OR IRA L1 1.2 = Internet Facing (web/mobile) application, OR IRA L1 1.2 = Non internet facing application] & New or Existing With Change.

57 **Q#DD IS/IT6 | Information Protection Contract Requirement (IPCR) validation**

TRM is required to attach the relevant document which shows that the contract with Third-Party includes Information Protection Contract Requirement (IPCR) addendum or equivalent (e.g., **PAYBACK Data Processing Agreements**).

Note: An IPCR is only required if the Third-Party service involves accessing AXP Systems and/or if AXP Restricted or AXP Secret Data is involved. Review the IPCR (or equivalent language) for language around data protection and review rights. If the IPCR language is present and you are unsure if it contains the appropriate language, you may engage the IPCRReguestMailbox@aexp.com.

An IPCR is required if:

- service involves accessing AXP Systems (SRA 1.0 = Yes) OR
- AXP classification contains AXP Restricted (any) or AXP Secret (any) data (SRA 1.1.1) OR
- Compliance SRA 3.5 = Yes AND SRA 3.5.1 = Yes or N/A OR
- TRA 1.0 = Yes AND New or Existing with Change AND Non-GSM Contract = Non- SSBE (Relevant Sourcing Group)

SME Rating = MATERIAL

Response options & guidance:

- **Yes**: Select this Response Option if Acceptable Evidence is attached.
- **No**: Select this Response Option if Acceptable Evidence is not received. Answer would result in a Material Pre-contract Gap.

Acceptable Evidence: Upload a copy of the renewal contract with the IPCR (Information Protection Contract Requirement) present or equivalent (e.g., Data Processing Agreements) which may be in draft and a screenshot.

58 **Q#DD IS/IT7 | Post review scheduling validation**

SME Rating = MATERIAL

Response options & guidance:

- **Yes**: Select this Response Option if Acceptable Evidence is attached.
- **No**: Select this Response Option if Acceptable Evidence is not received. Answer would result in a Material Post-contract Gap.

Acceptable Evidence: Upload a screen-print of the Post Logical & Physical assessment within ProcessUnity (assessment should have been completed for this existing Third-Party or is scheduled as appropriate).

59 **Q#DD IS/IT8 | SLA Verification within contract**

SME Rating = MATERIAL

SLAs are defined as the business units' expectations for the third-parties performance concerning the services being provided. SLAs should be measurable, attainable, achievable, and in most cases reportable (e.g., metric submission, SLQ, ISQ).

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no document showing SLA verification within the contract is attached. Answer would result in a Material Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: A screen-print of the inclusion of the SLA's in the contract. In the comment text box, provide the document name, page, or section. Reach out to the Contract Manager or refer to the contract drafted for a screen print of the SLA's documented.

60 **Q#DD IS/IT9 | RTO Verification within contract**

SME Rating = MATERIAL

This DD activity is required if SRA 1.2 = Internet Facing (web/mobile) application OR Non internet facing application AND SRA 2.2.1 Tier = 0, 1, or 3.

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no document showing Recovery Time Objective (RTO's) within the contract is attached. Answer would result in a Material Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: A screen-print of the inclusion of the Recovery Time Objective (RTO's) in the contract. In the comment text box, provide the document name, page, or section.

61 **Q#DD IS/IT10 | IS Descoping Question Validation**

SME Rating = MATERIAL

Descoping Validation (Q. L2 1.1- Is the Third Party one of the following, or is any of the following applicable?)

Response options & guidance:

- **Yes**: Select this Response Option if Acceptable Evidence is attached
- **No**: Select this Response Option if No Acceptable Evidence is attached. Selecting this "Response Option" would result in a Material Pre-contract Gap. (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Leadership Attestation or evidence that the service provided is within scope of the response from TRA L2 1.1. Attestation should include an email from BU leadership that L2 1.1 response is accurate. Attestation of questionnaire is not sufficient. An email from BU TRM leader, or evidence of scope should be uploaded.

7. Model Risk

62 **Q#DD M1 & M2 | Does the Business Unit have proof that approval was received for the Third Party to utilize their own Risk Models?**

Notify the AXP Model Risk team to confirm / review the Third-Party Model Risk requirements and attach the relevant documentation within ProcessUnity.

Response options & guidance:

- Select **Evidence Received** if acceptable evidence is attached
- Select **Evidence Not Received** if AXP Model Risk team was not notified, or confirmed reviewing the Third Party service (selecting this response results in a Material Pre-Contract Gap)
- Select **Not Applicable, SME Attested** if pillar SME has attested this dd activity does not apply.

Acceptable Evidence

- Provide proof of notification was sent to the AXP Model Risk team, or confirmation from the Model Risk ream where they acknowledge review of the Third-Party service and/ or proof of pillar SME attesting that this dd activity does not apply. Attach proof of evidence and acknowledge the name of the document provided within the comment section.

8. Privacy

Privacy Guidance aims at mitigating Privacy Risk by ensuring that the AXP|PAYBACK Data Protection and Privacy Principles are addressed. There are the 10 AXP|PAYBACK Data Protection and Privacy Principles with their meaning/purpose: Collection of Data, Notice and Processing, Choice, Data Quality, Security and Confidentiality, Data Sharing, Openness and Data Access, International Transfer, Responsibility and Accountability.

In some cases not all 10 Principles (i.e. Collection of Data, Notice and Processing, etc.) will apply to every Third Party. Therefore, DD activities must be completed based on the applicable Principles. If a particular principle is not applicable to a Third Party, then SME confirmation/attestation must be obtained as evidence.

63 **Q#DD P1 | Privacy Program-Policy –** Do you have a Privacy Program / Policy and/or processes or documents that ensures that AXP Data Protection and Privacy Principles are addressed, as relevant: collection, notice and processing, choice, data quality, security & confidentiality, data sharing, openness & data access, international transfer, responsibility and accountability?

SME Rating = HIGH

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no privacy program documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Privacy policy and/or procedures.
- Privacy Charter.
- Privacy Compliance Policy, Standard or Program Document.
- Privacy Standards, Privacy Frameworks.
- Privacy Risk Assessments.
- Information Security Management Program Policy and/or Procedure.

If, after reasonable attempts, a TRM is unable to obtain physical copies of the Privacy Program related documents (as outlined in the Acceptable Evidence section above) or the Third Party is unable to provide the related documents due to confidentiality reasons, viewing the documents via Webex can be considered to satisfy this DD requirement. Note: All components do not necessarily have to be within one document.

Alternative Acceptable Evidence:

If, after reasonable attempts for Acceptable Evidence a TRM is unable to obtain evidence of a Privacy Program or the company is unable to share the related documents due to confidentiality reasons, a Letter of Attestation from an individual responsible for managing the company's Privacy Program stating that they have a Privacy Program in place

covering the applicable Data Protection and Privacy Principles is acceptable alternative evidence. Letter of Attestation should include the following evidence:

- The Letter of Attestation should be on a company letter head
- The name and description of the Privacy Program document
- Title and name of the person attesting to the letter

64 **Q#DD P2 | Privacy Program – Training –** Do you have a Privacy Program / Policy and/or processes or documents that ensures that Third Parties handling AXP|PAYBACK Personal Data are either taking AXP|PAYBACK's Privacy training, or providing Privacy training to their employees?

Important Note: TRM's can refer to the GRL Vendor Program (AXP Privacy Training) via Global Regulatory Learning site on the square to learn more.

SME Rating = HIGH

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no training program documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. Applicable documentation consisting of actual policy, procedure, standard or charter showing that Privacy Training Program exists, and Privacy training is conducted or that the Third Party is taking AXP Privacy training. Documentation must outline / describe the framework for how the Third Party provides Privacy Training to their employees. The Training documents should include AXP Data Protection and Privacy Principles are addressed, as relevant. Some examples of acceptable documents include, but not limited to the following:

- Privacy training program content/materials.
- Information Security Management Training Program which includes privacy content.
- An attestation from the Third Party which states that they have a privacy training program in place and that all employees with access to Personal Data are required to complete the training, and that the training is tracked and monitored for completion by employees. The attestation would need to come from the Third Party's official email address or company letterhead, signed by an individual responsible for the Company's Privacy Program (e.g. Chief Privacy Officer, Privacy or Compliance Team) and include the individuals full title, work location, business email address and business phone number. This can be sent via email and should mention the privacy components (i.e. choice, notice & processing, collection, etc.) which are included in their training program (i.e. similar to Privacy Principles which are typically included in a Company's Data Protection & Privacy Principles).

65 **Q#DD P3 | Privacy Program Ongoing Monitoring** – Do you have a Privacy Program / Policy and/or processes or documents that ensures that compliance with existing and changes to Privacy laws and regulations, as necessary?

SME Rating = HIGH

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no On-going monitoring process documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. Applicable documentation consisting of actual policy, procedure, standard or charter which demonstrates that the On-going monitoring process or program is in compliance with the existing or changed Privacy regulations. Some examples of acceptable documents include, but not limited to the following. Privacy policy and/or procedures which address privacy oversight and monitoring:

- Privacy charter addressing ongoing monitoring.
- Privacy Monitoring Compliance Policy, Monitoring Standard or Privacy Monitoring Program Document.
- Privacy Monitoring Standards, Privacy Monitoring Frameworks.
- Privacy Risk Assessment program.
- Information Security Management Program Policy and/or Procedure which include data privacy components/content.
- An attestation from an individual responsible for managing the company's Privacy Program stating that they have an Ongoing Monitoring Privacy Program in place covering the above Data Protection and Privacy Principles.
- WebEx review of the policy, procedure or any other document by a Privacy SME which addresses that the Third Party has a Privacy Oversight and monitoring program in place covering the above Data Protection and Privacy Principles is acceptable.

Alternative Acceptable Evidence. Letter of Attestation: If, after reasonable attempts for Acceptable Evidence a TRM is unable to obtain evidence of an On-going monitoring process or program or the company is unable to share the related documents due to confidentiality reasons, a Letter of Attestation from an individual responsible for managing the company's Privacy Program stating that they have an On-going Monitoring program in place which address compliance with existing Privacy laws and regulations and covering the applicable Data Protection and Privacy Principles is acceptable alternative evidence. Letter of Attestation should include the following evidence:

- The Letter of Attestation should be on a company letter head
- The name and description of the On-Going Monitoring document
- Title and name of the person attesting to the letter

66 **Q#DD P4 | Privacy Program – Accountability:** Do you have a Privacy Program / Policy and/or processes or documents that ensures that the Third Party has designated appropriate resource(s) responsible for Data Protection/Privacy? Provide evidence (e.g. a letter from senior management stating the name of the individual that is responsible for Data Protection/Privacy at the Third Party).

SME Rating = HIGH

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no documentation available from the Third Party showing the appropriate resource(s) which are responsible for Protection/Privacy. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. Applicable documentation consisting of actual policy, procedure, standard or charter which demonstrates that the Third Party has designated appropriate resource(s) responsible for Data Protection/Privacy. Some of the examples of acceptable evidence includes: organizational charts, job descriptions, and/or a letter from senior management on company letterhead stating the name of the individual that is responsible for Data Protection/Privacy at the Third Party (e.g., Chief Privacy Officer (CPO).

67 **Q#DD P5 | Notice & Processing**

SME Rating = HIGH

DD Activity: Do you collect personal data offline/online?

- If **Offline**, provide a copy of the Privacy notice/disclosure/statement provided by the Third Party to Data Subjects/Individuals which advises/informs them that data may be shared.
- If **Online**, provide a copy of the Third Party's Online Privacy Statement (OPS) and ensure it discloses that the Third Party may share data. If applicable, obtain a copy of any other Privacy disclosure/ notice provided by the Third Party to the Data Subjects/Individuals noting how data is processed (collection, access, use, sharing, storing).
- If applicable, market specific notices or OPS should be provided.

Privacy Notice/Privacy Disclosure/Privacy Statement informs Data Subjects/Individuals about: a) what types of PII/Personal Data will be collected; b) why it is being collected; and c) how the data will be processed. If a Call Center is involved, ensure that the call scripts used by the service representatives contain language to deliver the appropriate notice to the Data Subjects/Individuals (as applicable). If explicit consent is being collected by the Third Party, obtain evidence that Data Subjects/Individuals have provided such consent to the collection and sharing of their information. (offline or online). The notice should be provided to individuals prior to collecting their personal information. If Third Party is providing Privacy Notice/Privacy Disclosure provided/issued by PAYBACK (PAYBACK application forms, Call scripts etc.), this can be used as an evidence to complete this DD.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no documentation available from the Third Party showing the appropriate resource(s) which are responsible for Protection/Privacy. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. A copy of the notice/disclosure or Third Party's Online Privacy Statement (OPS). Some examples of acceptable documents include, but not limited to the following:

- Privacy Notice/Privacy Disclosure.
- Privacy Statement (online version of the Privacy Statement may be sufficient).
- Notices may also be verbal when interfacing with the Data Subjects/Individuals via a phone (tele servicing) – support documentation such as a call script containing privacy statement/privacy notice content is required.
- A copy of the document where the Data Subject/Individual has given consent to share their PII/Personal Data.

68 **Q#DD P6 | Notice & Disclosure:** Do you collect personal data from your own customer or via other sources and shares it with AXP|PAYBACK? If Yes, provide evidence of any Notice / disclosure language provided to the customers that shows that the customers have provided consent for the sharing of their Personal Data.

SME Rating = HIGH

A **Privacy Notice/ Privacy Statement/Privacy Disclosure** is a statement made to a Data Subjects/Individuals which describes how the organization collects, corrects, uses, retains, discloses, and deletes personal information. The notice should be provided to individuals prior to collecting their personal information. If the collection of data is performed offline (i.e., via paper applications), the Third Party may provide to Data Subjects/Individuals a copy of their Privacy Notice/Privacy Disclosure in paper form or as part of a form/paper application. If the collection is performed online (i.e., via a web application), the Third Party should have an Online Privacy Statement, which Data Subjects/Individuals can go to/review in order to understand the Third Party's privacy practices and how their Personal Data will be processed. If explicit consent is required to be collected, this is often included within the Notice/Privacy. If TP is providing Privacy Notice/Privacy Disclosure provided/issued by Amex (Amex application forms, Call scripts etc.), this can be used as evidence to complete this DD.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.

- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Privacy Notice/Privacy Disclosure.
- Privacy Statement (online version of the Privacy Statement may be sufficient).
- Notices may also be verbal when interfacing with the Data Subjects/Individuals via a phone (tele servicing) – support documentation such as a call script containing privacy statement/privacy notice content is required.
- A copy of the document where the Data Subject/Individual has given consent to share their PII/Personal Data.

69 **Q#DD P7 | Resell | Repurpose Data.** Do you purchase or access personal data that it is reselling/ repurposing and providing it to AXP|PAYBACK?

SME Rating = HIGH

A **Privacy Notice** is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information (offline or online). The notice should be provided to individuals prior to collecting their personal information.

Response options & guidance: Provide evidence of documentation / contract between the Third Party and the data sources that allows the Third Party to resell / repurpose the data.

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence: The documentation should confirm that Third Party processes data fairly and for permitted purposes only.

- Privacy Notice/Privacy Disclosure.
- Privacy Statement (online version of the Privacy Statement may be sufficient).
- Notices may also be verbal when interfacing with the Data Subjects/Individuals via a phone (tele servicing) – support documentation such as a call script containing privacy statement/privacy notice content is required.
- A copy of the document where the Data Subject/Individual has given consent to share their PII/Personal Data.

70 **Q#DD P8 | Privacy Choice**

SME Rating = HIGH

TRM to confirm the following:

a) Privacy choice is relevant/provided

If choice will be captured by the Third Party, **TRM to also confirm**:

b) Whether Privacy Choices will be shared /communicated with AXP|PAYBACK
c) Whether there is a need to engage the EDA GPC team to ensure that privacy choices are captured, collected, honored and tracked appropriately.

Also, TRM to gather and provide process flows confirming the following with their Privacy SME and the AXP EDA team to determine whether Third Party system used to collect/capture and/or honor/manage privacy choice (IF CHOICE CAPTURED/HONORED BY THE THIRD PARTY, TRM TO ALSO CONFIRM) are compliant with AXP choice standards. BU TRM, Privacy SME, and EDA team to align on whether Third Parties capture/honoring of choice requires uplift in EPCC and requiring a Risk Change Management be submitted to the EDA team.

Privacy choice is an option given to a user to determine the way their Personal Data is processed (including collecting, storing, altering, accessing, using, transferring, receiving, sharing or destroying data). When AXP|PAYBACK engages with a Third Party, it is important to understand whether Privacy Choices are relevant. This includes managing customers' choices (opt-in/opt-out) to be included or removed from receiving communications/marketing offers as required by applicable law. If the Third Party is responsible for capturing or applying relevant privacy choices, a system or process should be in place that stores the captured choices and evidence that the captured choices are honored and tracked.

Response options & guidance: The Third Party's service should identify whether privacy choices are relevant, who is responsible for the tracking of those choices (either the Third Party or AXP|PAYBACK) and how the choices will be captured.

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence: Process flows and meet AXP|PAYBACK choice standard requirements.

71 **Q#DD P9 | Openness and Data Access:** Does the Third Party have a mechanism in place for customers to submit requests and receive information about how their Personal Data is processed and their rights and remedies including processes and system capabilities to fulfill data subject requests, including but not limited to, requests or access, erasure, rectification, data portability, to restrict processing and to object to automated individual decision-making?

SME Rating = MODERATE

AXP's Openness & Data Access privacy principle grants Data Subjects/Individuals the right to submit a request to receive information about how their Personal Data is processed and their rights and remedies. If the Data Subjects/Individuals can contact AXP|PAYBACK to update their information, then this DD would be N/A on the privacy checklist. If the Third Party is required to have a process in place, the Third Party must provide a description of how individuals (customers) have the ability to access, correct, and /or delete their PII data.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Document outlining the Third Party's process for how Individuals can update their Personal Data.
- Phone number for the Data Subjects/Individuals to call
- An address to for the Data Subjects/Individuals to write in about for changes
- Reference to a website or online form that allows the Data Subjects/Individuals to make updates

Note: This information/process is often disclosed in a Privacy Notice, Privacy Policy, or Privacy Statement/Online Privacy Statement.

72 **Q#DD P10 | International Transfer**

SME Rating = HIGH

For **international transfers**, collect information from third party about any transfer mechanisms used to address cross border transfers of Personal Data (e.g., Binding Corporate Rules, model contracts) and ensure that transfer mechanism is appropriate for each cross-border transfer. The Third Party must provide documentation as to which countries are involved in the services provided on behalf of AXP in order to determine applicable privacy requirements. The documentation provided must show adherence to international privacy requirements based on countries noted.

This does not apply when data transfer occurs between one EU country to another EU country.

Note: Cross-border data transfer regulatory requirements are not specific just to EU countries. However, Binding Corporate Rules (BCR) as a method of compliance for cross-border data transfers only apply to intra-organizational transfers for Personal Data across country borders in compliance with EU Data Protection Law. BCRs do not apply to external data transfers from one company/organization to another.

Response options & guidance: The Third Party must provide documentation as to which countries are involved in the services provided on behalf of AXP|PAYBACK in order to determine applicable privacy requirements. The documentation provided must show adherence to international privacy requirements based on countries noted.

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.

- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. Data flows of the data to/from each location to show what data is being shared, where is it going to/from, how is it being shared, what is source of record, what are record retention periods; evidence showing that standards or requirements are being followed to meet International Data Transfer regulations. Some examples of acceptable documents include, but not limited to the following – data flows of the data/to from each location.

- If transferring data across borders, the Third Party should provide evidence showing that standards or requirements are being followed to meet International Data Transfer regulations and laws such as a copy of a Model Contract Clauses (or Standard Contractual Clauses), (not limited to EU countries only) or Binding Corporate Rules (BCR) document. Also, Binding Corporate Rules (BCR) only apply EU countries and only address internal data transfers within the same organization/Third Party. BCRs do not cover external data transfers from one organization/Third Party to a different organization/Third Party. As such, AXP BCRs do not cover Third Party cross-border data transfers.
- Documents that specify which international countries (outside US) data is sent to and what process is in place to meet the international data transfer requirements.
- If the vendor does not transfer data internationally, a letter of affirmation stating that there is no international transfer of PII data within the service provided must be captured as evidence. Must be on Third Party company letter head/email containing the Third-Party email address and contain a signature from the Chief Privacy Officer or other individual within the Third-Party organization with responsibilities for Privacy. This does not apply when it's EU to EU.

73 **Q#DD P11 | Data Flow**

SME Rating = MATERIAL

Response options & guidance: Submit the data flows to show what data is being shared (i.e. data elements list/inventory), where data are going to/from, how data are being shared, what is source of record, and what the record retention periods are.

- DD Attempted, **Evidence Received**
- DD Attempted**, Not Received**

Acceptable Evidence. Provide mandatory data flows for, at a minimum, all high privacy risk services to show mapping of data flows, (what data are being shared, where data are going to/from, how are being shared, what is source of record, what the record retention periods are).

74 **Q#DD P12 | De-Identified/Aggregated Data**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no documentation available from the Third Party to justify de-identification/aggregation of data. Answer would result in a Pre-contract Gap.

- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: upload the appropriate document that shows the Third Party is following AXP|PAYBACK standards around de-identification/aggregation and that the Privacy SME has reviewed the contract to validate that there are proper contractual terms included.

75 **Q#DD P13 | DPIA: Record**

SME Rating = HIGH

DD Activity: link to or copy of a completed PRA-DPIA record (Privacy Risk Assessment – Data Protection Impact Assessment).

The TRM must provide documented evidence that a Contact Privacy (CP) inquiry has been submitted (i.e. screen shot of CP record) which shows that the Privacy SME has provided guidance stating that:

- **A DPIA is not required**: if the Privacy SME determines that a DPIA is not required confirmation must be provided as evidence – attached, and the follow comments must be updated to state "per Privacy SME, DPIA not required, and include CP record ID # ".

OR

- **A DPIA is required**: the TRM must provide the Privacy Risk Assessment (PRA) record ID and screen shot as evidence that a DPIA has been escalated to a Privacy SME and the comments must be updated to state "PRA/DPIA has been initiated" and the PRA record ID #" must be included. They do not have to wait for the full DPIA to be completed.

Response options: A DPIA is a deep-dive PRA focusing on compliance with European Union (EU) General Data Protection Regulation (GDPR). It is required when the processing of personal data related to EU customer, prospect or employee may result in high risk to individuals.

- DD Attempted, **Evidence Received**
- DD Attempted**, Not Received**

Acceptable Evidence. Provide a copy of the DPIA to show evidence this occurred.

Note: The DPIA is not necessary aimed at assessing the third-party, but more about the processing, which can differ from engagement to engagement, therefore a DPIA cannot be leveraged from another engagement for the same third-party. Through the Contract Privacy (CP) inquiry, the Privacy SME determines if a DPIA is required or not for each engagement.

76 **Q#DD P14 | Data Deletion**

SME Rating = HIGH

The TRM is required to attach the relevant documentation which consists of getting Third Party's Data Deletion Policy ensuring that requirements comply with the AXP|PAYBACK Data Protection and Privacy Principles.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Deletion Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence.

1. Data Deletion Policy that outlines the Third Party's policy on deleting PII on AXP|PAYBACK data, or if their Privacy policy or Data Deletion policy or any or document which includes information on how they document data deletion for their organization.
2. Description of the solution(s) employed by the Third Party to ensure PII that is no longer needed is deleted or anonymized
3. Data Deletion Schedule that details the retention periods that the Third Party uses to determine when to delete PII.

77 **Q#DD P15 | Data Breaches**

SME Rating = HIGH

The TRM is required to obtain documentation of data breach notification/incident response policy, program, or process from the Third Party.

A **data breach** generally happens to the unauthorized access and retrieval of information that may include corporate and/or personal data. The Third Party's data breach notification policy/process needs to confirm the process for identifying who will be notified (including relevant law enforcement agency), when and how data subjects will be notified, what actions can data subjects take and how data subjects can reach relevant contacts within the Third Party.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no "Third Party's Data Breach Policy" documentation available from the Third Party. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence. The Third Party's data breach notification policy program. If available, a copy of the Third Party's breach notification letter/template should be provided.

9. Resiliency

78 **Q#DD R1 | Crisis Management Planning**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- Evidence Not Received: if there is no Crisis Preparedness Program evidence or document available from the Third Party. Answer would result in a Pre-contract Gap.
- Not Applicable, SME Attested: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. *Please refer to TLM_Contact Privacy Request document for more details.

Acceptable Evidence: Upload the evidence showing Third Party's Crisis Preparedness Program. The purpose of this document is to ensure that the Third Party possesses the operational capabilities for an effective response to a significant business disruption or crisis.

79 **Q#DD R2 | Incident Response Planning**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the Third Party's Incident Response Plan. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. *Please refer to TLM_Contact Privacy Request document for more details.

Acceptable Evidence: Upload the evidence showing Third Party's Incident Response Plan. The evidence should include:

- evacuation procedures
- who is responsible for communicating with local government agencies (police, fire, fire)
- the response to various incidents (bomb threat, workplace disturbance, injuries, etc.)
- how the crisis will be managed until it is resolved

81 **Q#DD R3 | Business Continuity Planning and Exercises**

SME Rating = HIGH

Response options & guidance:

- **Evidence Received**: if you have received Acceptable Evidence from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received**: if there is no evidence or document attached of the Third Party's Recovery Plans. Answer would result in a Pre-contract Gap.
- **Not Applicable, SME Attested**: if DD activity is not applicable and the SME has attested* to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity. ***Please refer to TLM_Contact Privacy Request document for more details.**

Acceptable Evidence: Upload the evidence showing Third Party's Recovery Plans. Overview should include all types of recovery plans (Service Continuity, Business Continuity (BC), Disaster Recovery (DR), and Crisis Management (CM), Incident Response, etc.), what is covered in each type of plan, how often are they updated, how are they discarded, etc.). The evidence should include:

- Frequency of plan updates
- Description of exercises
- Exercise Results to include, if applicable, proof that the recovery time objectives of the application(s) were met
- How gaps identified during these exercises were resolved

10. SOX Risk

81 **Q#DD SOX2.01 | Extract of Contract**

SME Rating = MATERIAL

A SOC1 Type 2 report focuses on controls relevant to user entities internal control over financial reporting.

Response options & guidance:

- **Evidence Received:** Select this "Response Option" if you have received Acceptable Evidence* from the Third Party. In the comment text box, provide the document name, page, or section. The document needs to be attached in the ProcessUnity.
- **Evidence Not Received:** Select this "Response Option" if there is no evidence or document attached of the Third Party's Extract of Contract. Selecting this "Response Option" would result in a Pre-contract Gap.
- **Not Applicable, SME Attested:** Select this "Response Option" if DD activity is not applicable and the SME has attested to this alignment. A copy of SME attestation needs to be uploaded in the ProcessUnity.

Acceptable Evidence:

- Upload a document showing Third Party's Extract of Contract where the requirements to obtain SOC 1 Type II report or equivalent and right to audit clauses are included.

82 **Q#DD SOX2.02 | Control Environment Evidence**

SME Rating = MATERIAL

The business needs to obtain Control Environment Evidence covering the design and operating effectiveness of controls at the Third Party and any subservice organization (SSO = Fourth Party Subcontractor).

Response options & guidance:

- **Service auditor's report on control(s)** placed in operation covering design, and operating effectiveness, also known as a SOC 1 Type 2 Statement on Standards for Attestation Engagements 18 (SSAE 18). Attach report, if possible. In the comment text box, provide the document name, page, or section OR
- **Perform tests of control(s) at the SO.** Evidence of alignment with Third Party OR
- **A report on the application of agreed-upon procedures** (AUP) that describes relevant tests of controls. Evidence of alignment with Third Party OR
- **DD Attempted, Not Received** Select this "Response Option" if there is no Control Environment evidence attached, and/or any of the above is not available. Selecting this "Response Option" would result in a material Pre-contract Gap.

Acceptable Evidence:

- Upload a document or evidence which shows that SOC1 Type II report has been aligned and agreed with the Third Party as part of Contractual obligations and it also ensures adequacy of controls at the Third party including the controls coverage for sub service organization (SSO) used if any.

83 **Q#DD SOX2.02.01 | Will the SOC 1 Type II report be available by December of the relevant Financial year in which the services have been rendered with the Control objectives covering ITGC and Business application controls?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Upload a document that shows SOC 1 Type II report will be available by December of the relevant Financial year in which the services have been rendered with the Control objectives covering ITGC and Business application controls.

84 **Q#DD SOX2.02.02 | Will the SOC 1 Type II report period include at least 9 months of activity for calendar year and bridge letter for the remaining period?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached

- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Upload the appropriate SOC 1 Type II evidence or document. SOC 1 Type II Report and the bridge letter provided should be for an entire year. Since the report is furnished before the year end, as per best practices and recommendation from Auditors, AXP requires that the SOC 1 Type II report should ideally cover at least 9 months of activity in the current calendar year and a bridge letter for the remaining period. Create action plan for remediation that has been approved by the SOX team.

85 **Q#DD SOX2.02.03 | Will the SOC 1 Type II report cover the service being provided to AXP|PAYBACK?**

SME Rating = MATERIAL

Attach the relevant document showing the SOC1 report is covering the services which the Third Party is providing to AXP|PAYBACK for it to be relevant for AXP|PAYBACK. As SOC 1 report provides assurance over the control environment of the Third Party, it is essential that the control environment for AXP|PAYBACK services are covered in the "Scope" section of the SOC 1 Type II Report. Typically, under Section I (Report of Service Auditor's) of SOC1 report, subsection "Scope", it should be ensured that the services/ applications used for providing the services which are rendered to AXP|PAYBACK, are covered in Scope of the SOC 1 Type II report.

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

Acceptable Evidence:

- Provide evidence of agreement with Third Party on SOC1 Type II report for services to be rendered to AXP. The report should cover the controls objectives around ITGC, and Business applications controls along with tests of its operating effectiveness.

86 **Q#DD SOX2.02.04 | Will the SOC 1 Type II report cover ITGC and business application controls along with tests of operating effectiveness?**

SME Rating = MATERIAL

Attach the relevant document that provide evidence of alignment with the Third Party on scope of the report to cover the controls objectives around ITGC and business applications controls along with tests of its operating effectiveness.

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Upload a document that provide an evidence of SOC 1 Type II report covering the ITGC and business application controls along with tests of Operating effectiveness. Both ITGC and Business application controls are relevant for reasonable assurance on the control environment of the Third Party. In the section where the tests of operating effectiveness of the controls is provided, it needs to be ensured that the IT General Controls (such as ITGC Program Change Management, Program Development, Logical Access, Computer Operations etc.) are available with results of testing performed on such controls. Similarly, Business Application controls (such as Data transmission, Edit Checks, Validation of input/ output (system calculation) etc.) controls should be available with results of testing performed on such controls. The evidence may include a SOC1 Type II report issued for the previous calendar year.

87 **Q#DD SOX2.02.05 | Does the SOC 1 Type II report have a qualified opinion?**

SME Rating = MATERIAL

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)
- **No:** Select this "Response Option" if Acceptable Evidence is attached

Acceptable Evidence:

- Upload a document that provides an evidence of a non-Qualified opinion SOC 1 Type II report for the previous calendar year or a plan to identify compensating controls with due date (to be provided by Process Area outsourcing the service).

Note: Typically, in the SOC1 report provided under Section I (Report of Service Auditor's), opinion is provided by the Service Auditor on the SOC 1 Type II report. Evaluating all material aspects, Service Auditor opines on if the SOC 1 Type II report of the Third Party under the stated scope is qualified/ not qualified and the reason for qualification, if any.

88 **Q# DD – SOX2.03 | Complementary User Entity Control(s) (CUECs)**

SME Rating = MATERIAL

Attach the relevant document showing the Complementary User Entity Control(s) (CUECs) at AXP which monitor the activities at the Third Party to ensure that all applicable financial statement risks/assertions are adequately mitigated.

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Upload a plan with due date (to be provided by Process Area outsourcing the service) to document adequate CUECs as part of AXP PRSA to mitigate the residual risk out of Third Party services.

89 **Q#DD SOX2.04 | In absence of SOC1 report, please provide the plan documenting compensating controls at AXP|PAYBACK to mitigate the underlying risk from vendor services and test of operating effectiveness.**

SME Rating = MATERIAL

Attach the relevant document showing a plan that consists of the Compensating control(s) at AXP|PAYBACK to mitigate the underlying risk from vendor services and test of operating effectiveness in case of SOC 1 Type II report not being available with the Third Party.

Response options & guidance:

- **Yes:** Select this "Response Option" if Acceptable Evidence is attached
- **No:** Select this "Response Option" if Acceptable Evidence is not received. This answer would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed)

Acceptable Evidence:

- Upload a plan documenting compensating controls at AXP|PAYBACK to mitigate the underlying risk from vendor services and test of operating effectiveness.

Compensating control(s) are defined at AXP|PAYBACK in order to mitigate the risk of unavailability of SOC 1 Type II report by the vendor. They need to address the same risk of misstatement and operate at a level of precision that would prevent/ detect and correct on a timely basis any error/ misstatement from vendor services that could be material. Also, it is essential that operating effectiveness of compensating controls must be demonstrated to place reliance.

90 **Q#DD SOX2.05 | Subservice Organization SOC1 Type II**

SME Rating = MATERIAL

TRM is required to provide evidence showing alignment with the Third Party on the availability of SSO's SOC1 Type II report for AXP's review or coverage of Complementary Subservice organization controls (CSOCs) as part of Third party's SOC1 Type II report only including commenting on its operating effectiveness.

Response options & guidance:

- **DD Attempted, Evidence Received** select this "Response Option" if Acceptable Evidence is attached in ProcessUnity.
- **DD Attempted, Not Received** select this "Response Option" if Acceptable Evidence is not received. Selecting this "Response Option" would result in a Material Pre-contract Gap (In order to proceed with Contract a Risk Memo should be completed).

Acceptable Evidence:

- Upload a document that shows the availability of SSO's SOC1 Type II report for AXP's review or coverage of CSOCs as part of Third party's SOC1 Type II report only including comments on its operating effectiveness.

11. 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