A close up of a sign

Description automatically generated

**Third Party Vendor Due Diligence Checklist**

The purpose of the third-party resilience program checklist, it to allow the department or sponsor to perform an assessment of the prospective outsourced activity as part of the due diligence.

**Checklist #1** – This checklist lists a number of procedures to be considered while gathering information and documentation that will assist in the evaluation of the prospective vendor.

**Checklist #2** – To gather contract information at the first review and to capture changes to the contract as part of negotiation or contract renewals.

**Checklist #3** – To be used when there is any knowledge of third-party vendors that are subcontracted by the primary vendor provider.

**Description of possible values:**

* “Satisfactory”: When the agreement clearly outlines the procedures listed in the form.
* “Unsatisfactory”: When the procedure in the agreement is not appropriate. Enter an action plan and due date to remediate.
* “Not Applicable”: When the procedure in the agreement is not required. Explain the reason why is not applicable.

**Checklist #1** – This checklist lists a number of procedures to be considered while gathering information and documentation that will assist in the evaluation of the prospective vendor.

Name of the Service Provider: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Description of the Outsourced Activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Procedure** | | **Consideration** | **Evaluation** (Values could be "Satisfactory", "Unsatisfactory” or "Not Applicable") | **Comments** (Provide details for "Unsatisfactory" or "Not Applicable") | |
|
| **A. To determine suitability** | | |  |  |  |
| 1 | Legal requirements | Ensure if the service activity can be outsourced under applicable laws or local regulations. |  |  | |
| **B. To Exclude Vendors Lacking Needed Requirements** | | |  |  |  |
| 1 | Evaluate Public Trust | Determine if the vendor and any subcontracted provider(s) are involved in any criminal activities or organizations. |  |  | |
| 2 | Service Suitability | Determine if there is any possibility that the use of the vendor services may cause reputational risk. |  |  | |
| 3 | Qualifications | Determine vendor qualification requirements to perform outsourced activities. |  |  | |
| **C. Vendor Selection** | | |  |  |  |
| 1 | Dependability | Determine the vendor ability, capabilities, and past experience performing the service activities. |  |  | |
| 2 | Financial Stability | Determine vendor’s financial stability and indemnification for any potential loss resulting from the vendor’s negligence. |  |  | |
| 3 | Policies and Procedures | Determine the vendor’s policies and procedures for the outsourced activities to be followed by the personnel providing services to the firm. |  |  | |
| 4 | Performance Review | Determine if the vendor has been able to provide services to the firm without any major issues. |  |  | |
| 5 | Regulatory Reporting | Determine whether the vendor provides on behalf of the firm any regulatory reporting. |  |  | |
| 6 | Data Privacy | Determine the vendor qualifications to handle confidential information to comply with applicable laws. |  |  | |
| 7 | Data Protection | Determine the return or destruction of data by the vendor when contract ends. |  |  | |
| 8 | Clients Inquiries | Determine established procedures to handle complains, inquiries, and feedback by clients (if to be handled by the provider as per firm’s discretion). |  |  | |
| **D Assess Service Agreement** | | |  |  |  |
| 1 | Legal risk | Use Checklist #2 to determine compliance to the service agreement. |  |  | |
| 2 | The Arm's-Length Rule | Determine compliance to the Arm’s-Length Rule in the event services are to be provided by any of the firm’s branch / affiliate companies. |  |  | |
| **E. Additional Considerations** | | |  |  |  |
| 1 | Business Continuity Plan (BCP) | Determine the establishment of a Business Continuity and Disaster Recovery (BCDR) planning to ensure continuity of business to clients. Obtain and confirm regularly emergency contact information. |  |  | |
| 2 | Assess subcontracted provider(s) | Use Checklist #3 to list any subcontracted providers by the vendor and to verify the two items below: |  |  | |
| Verify the agreement provides a clause when you allow the vendor to outsource some or all activity to a subcontracted service provider(s). |  |  | |
| In the event the vendor outsources the activity, verify the controls in place by the vendor to monitor the subcontracted provider. |  |  | |
| **F. General Evaluation** | | |  |  |  |
| **General Evaluation** | | **Document any identified risks from the above procedures and describe mitigating controls.** |  |  | |

**Checklist #2** – To gather contract information at the first review and to capture changes to the contract as part of negotiation or contract renewals.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No** | | **Procedure** | **Action** | **Comment** | **Status** | **Action plan, if required** |
| **(values could be ‘Satisfactory’ ‘Unsatisfactory’ or ‘Not Applicable’** |
| **1** | Outline Activity being Outsourced | | Determine Service Level Agreements (SLAs) for activities to be performed, method utilized, procedure, and delivery and timeframe of any required material. | — |  |  |
| **2** | Amount for the Contracted Outsourced Activity | | Determine the expenses including any additional fees. | — |  |  |
| **3** | Payment Method, Periods | | Determine the timeframe and method payment. | — |  |  |
| **4** | Timeframe of the agreement | | Determine the agreement timeframe and any renewal clause. | — |  |  |
| **5** | Timeframe of delivered materials | | Determine timeframe for any required material and its delivery method. | — |  |  |
| **6** | Material Assessment | | Determine the procedures to assess any required materials and the criteria for acceptance. | — |  |  |
| **7** | Attribution of Rights (Patents, Copyrights, Licenses, etc.) | | Determine if any group should be awarded copyrights, patents, or user license, in relation to the outsourced activity. | — |  |  |
| **8** | Provider’s Financial Reports | | Determine the financial stability of the service provider and the frequency of the delivery and receipt of these type of reports for assessment. | -- |  |  |
| **9** | Coordination of requests from regulatory authorities | | Determine the procedures for submission of requested materials related to the outsourced activity by regulatory authorities. | -- |  |  |
| **10** | Business Continuity Planning | | Determine the provider’s contingency plan to ensure continuity of service. | — |  |  |
| **11** | Cancellation | | Determine how the agreement can be cancelled unilaterally by the outsourcing parties. | — |  |  |
| **12** | Compensation of Damages | | Determine compensation in advance in the event the outsourced activity cannot be performed. | \_\_ |  |  |
| **13** | Reporting on Outsourced Activities | | Determine the format, report content, and frequency of the reports required as part of the outsourced activity | \_\_\_ |  |  |
| **14** | On-site Inspections | | Determine the right to request to the service provider to allow on-site inspections, improve procedures, or submit materials related to the outsourced activity, including surveillance. | \_\_\_ |  |  |
| **15** | Confidentiality | | Determine if the agreement includes a confidentiality clause, and specify if client or undisclosed information will be part of the outsourced activity. | — |  |  |
| **15-(1)** | Prohibition of the use of outsourced information | | Determine the restriction on the use of the outsourced information by other firm entities/branch. | \_\_\_ |  |  |
| **15-(2)** | Return of outsourced information | | Determine the deletion and disposal of the outsourced information after the conclusion of the agreement. | — |  |  |
| **16** | Non-expiration Clause | | Include a clause that will leave the agreement in effect indefinitely after the agreement period has expired (such as for obligations of confidentiality). | ― |  |  |
| **17** | Security Controls | | Determine the controls in place and the incident response plan to data leaks, loss, and damage involving the outsourced activities that handle client or undisclosed information. | — |  |  |
| **18** | Employee supervision | | Determine the necessary supervision and controls in place to perform the outsourced activity. | — |  |  |
| **19** | Subcontracting | | Determine if the part or the whole outsourced activity would be allowed to be subcontracted by another service provider. Determine the procedures for this subcontracting. | \_\_\_ |  |  |
|  |  | | Determine if subcontracting the outsourced activity is allowed. For activities involving client information and undisclosed information determine that (a) the agreement between the original provider and the subsequent provider is the same as the agreement between the firm and the original service provider, (b) the original service provider is responsible for the proper selection of subsequent providers and to conduct necessary supervision, (c) further subcontracting by the subcontracted provider is prohibited or, if allowed, the agreement must be the same as the agreement between the firm and the original provider. | — |  |  |

**Checklist #3** – To be used when there is any knowledge of third-party vendors that are subcontracted by the primary vendor provider.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| In case the "Provider A" (original service provider) outsources the activity to another service provider(s),  use this form to list all subcontracted service providers which ultimately perform "your" job function. | | | | | | |
| **Provider’s**  **Tag** | **Name of the Subcontracted Service Provider** | **Description of the Activity being Outsourced** | **Category (I/III)** | **Classification of Outsourced Activities** | **Information Handling** |
| "Provider B" |  |  |  | **Possible values:**  Outsourcing processing,  Outsourcing of activities handling information assets other than processing | **Possible values:**  Nothing,  Client Information, Undisclosed Information,  Both of Client and Undisclosed Information |
| "Provider C" |  |  |  |  |  |
| "Provider D" |  |  |  |  |  |
| "Provider E" |  |  |  |  |  |
| "Provider F" |  |  |  |  |  |

**Level (I/III):**

1. The activity by the third-party is not allowed to be suspended without prior notice because such suspension would affect our business or our services to the clients enormously.
2. The activity by the third-party may not be allowed to be suspended without prior notice because such suspension could affect our business or our services to the clients slightly.
3. The activity by the third-party may be allowed to be suspended without prior notice because such suspension does not affect our business or our services to the clients.