Graphical user interface, text, application

Description automatically generated**Background pattern

Description automatically generated with low confidence**

**CLOUD VENDOR FRAMEWORK TEMPLATE**

This template provides summaries of Cloud-hosted products and the business goals to be achieved when reviewing products and vendors.

8 Pages (20-1093)

**CLOUD VENDOR FRAMEWORK TEMPLATE**

(ACTION) Overview: In the paragraph, provide a summary of the Cloud-hosted product and summarize the business goals to be achieved when reviewing products and vendors. Insert appropriate departments to approve in management signoff columns on right.

| **Stage** | **Risk Description** | **Considerations** | **Yes / No / N/A** | **Management’s Assessment and Commentary** | **Management Signoff:**  **Initials and Date** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IT** | **Business Process Owner** | | | **Legal** | **Accounting** |
| 1: Strategic Assessment | The Cloud Hosting objective is not aligned with [ORG]’s overall business strategy. | Cloud hosting solution consistent with [ORG]’s business and IT support model? |  |  |  |  | | |  |  |
| Have subject matter experts been involved with the solution and vendor selection? |  |  |  |  | | |  |  |
|  |  |  |  |  |  |  | | |  |  |
| 2. Business Case Development | The Cloud Hosting decision is based on incorrect assumptions around projected cost savings or investment needed to build governance, acceptance, and validation capabilities. | Is there a preliminary business process flow including the use of outsourced business process services and technologies? |  |  |  |  | | |  |  |
| Does the process incorporate how these outsourced activities will integrate with existing systems? |  |  |  |  | | |  |  |
| Is the solution heavily dependent on integration with other [ORG] systems and have the cost, operating, and risk considerations been adequately assessed? |  |  |  |  | | |  |  |
| Are there sufficient internal resources to effectively govern, assess and operate the solution on an ongoing basis, including performing retained elements of the business process?  *Note: Resources would include the following: Project Manager, IT support, Business Process Owner and ongoing business support, governance / compliance and Internal Audit.* |  |  |  |  | | |  |  |
| Have we identified one-time vs. ongoing costs, licensing fees, additional hardware requirements, and additional software requirements? *Consider the following: project management, communications and training, legal, finance and other costs related to the transition, as well as ongoing governance, third-party support and management costs* |  |  |  |  | | |  |  |
| Has the Process Automation Committee reviewed and approved the decision to proceed with the project? |  |  |  |  | | |  |  |
|  |  |  |  |  |  |  | | |  |  |
| 3. Solution Definition | Failure to identify a complete solution and related risks of the solution. | Have the business requirements including:   * Functionality of the software application * Functionality of the operating delivery services, i.e., non-software delivery services * Integration to existing [ORG] systems * Consideration on staffing impact, i.e., will new staff be required to support solution? |  |  |  |  | | |  |  |
|  |  |  |  |  | | |  |  |
| Has the IT team considered the following risks relative to the technical requirements of the proposed solution:   * Infrastructure / data security * Identity and Access Management * Data management * Data encryption * Service continuity / availability * Regulatory Compliance * Sub-service providers * Migration to the Cloud * IT Management * Audit rights * SOX controls (SOC or SSAE reports) * IT governance, including key performance indicators and other reporting tools available to monitor and assess performance   See **Appendix A: Technology Considerations** and list concerns or matters for follow-up. |  |  |  |  | | |  |  |
| Consider how to assess vendor viability as part of the Request for Proposal (RFP) process, including consideration of the following:   * Financial strength * Experience with this solution and overall maturity of the vendor and the solution * Suitability of the vendor support model and related baseline service level agreement provisions * Disaster recovery and other business continuation considerations * Existing client base * References * Site visits * Employee turnover |  |  |  |  | | |  |  |
|  |  |  |  |  |  |  | | |  |  |
| 4. Vendor Selection | Failure to develop vendor selection criteria that contemplate outsourcing objectives and risks, and failure to exercise thorough due diligence. | Assess available solutions and describe how you identified a list of vendors. |  |  |  |  | | |  |  |
| Was each vendor assessed relative to the business requirements established under **Stage 3: Solution Definition**? |  |  |  |  | | |  |  |
| Were vendors invited to provide product demonstrations and were all relevant departments invited to participate in the evaluation? |  |  |  |  | | |  |  |
| Did end users assess the solution based on appropriate criteria, including functionality and usability? |  |  |  |  | | |  |  |
| Has Internal Audit and / or Accounting performed vendor review confirming the business, technical, and governance requirements have been appropriately considered and matters requiring separate attention have been identified and resolved? |  |  |  |  | | |  |  |
| Has Internal Audit performed a preliminary assessment of the SOC 1 report including consideration of the User Entity Controls in comparison with the proposed business process map and, if applicable, sub-servicer reports? |  |  |  |  | | |  |  |
| Has Legal performed a review of the intended solution to identify risk exposures and developed a list of special considerations for the contracting process? |  |  |  |  | | |  |  |
| Did IT assess the solution based on technical requirements? See **Appendix A: Technology Considerations**. |  |  |  |  | | |  |  |
|  |  |  |  |  | | |  |  | | |
| Contracting | Contract provisions covering service levels, incentives, contingencies, vendor personnel, security, privacy, price protection, and termination are missing or faulty. Provisions for measuring key SLAs are not in place. | Was there a discussion between the Subject Matter Experts (IT, Internal Audit, Legal, Business Process Owner(s)) to discuss the overall assessment of the vendor’s contract, including consideration of:   * Scope of services * Service level agreement/criteria consistent with business requirements * Required customization and ownership of work product * Special intellectual property matters * Use of sub service providers * Vendor and sub service provider operations in foreign countries * Term, termination assistance and timing including sufficient notice provisions * Limitation of liability * Indemnities * Disaster recovery and testing and other business continuation matters * Audit rights * Ownership and use of data * Requirement for a SOC 1 Type 2 Service Auditor Report (and sub service provider reports) * Confidential and/or sensitive information * Mutual Non-Disclosure Agreements * Cyber risk and anti-virus protection * Special insurance or other risk management issues * Provider personnel provisions and related HR practices * Relationship management and escalation and reporting requirements * Potential penalties |  |  |  |  | | |  |  |
| Subject Matter Experts (Accounting)   * Embedded Lease Review |  |  |  |  | | |  |  |
| Based on the complexity of the contract, did Legal utilize outside legal counsel? (Please provide additional commentary if outside counsel was not utilized) |  |  |  |  | | |  |  |
|  |  |  |  |  | | |  |  |
|  |  |  |  |  |  |  | | |  |  |
| 6. Service Transition, Delivery & Post-transition Management | Lack of formal transition planning and governance oversight practices lead to low service levels, cost overruns, and other outcomes that erode value. | Consider the following requirements:   * Transition planning * Knowledge transfer * Documentation of policies and procedures / roles and responsibilities (for both [ORG] and the provider) and the software configuration * Training and other change management considerations * Key personnel retention * An appropriate post go-live support model |  |  |  |  | | |  |  |

**Appendix A: Technology Requirements**

1. **Infrastructure/data security:** Do Cloud providers have acceptable procedures in areas such as access badge management, exchange, storage and safeguarding? Flawed security could result in the exposure of infrastructure or data.
   1. Are there security vulnerabilities due to other customers sharing the same environment? How does the provider ensure other customers cannot see/access/change our data?
   2. Do conflicting customer priorities have the potential to compromise Cloud service security? To what level/degree are the IT services shared with other customers (facilities, network, hardware, software, support staff, etc.)
   3. Are security patches performed timely?
   4. How is code promotion to production handled? How will the provider ensure new the code functions as intended and doesn’t cause unexpected problems?
   5. How will the provider respond to denial of service attacks?
   6. Can we independently test security? If not, what are the implications?
   7. Has the vendor developed an encryption and key management process?
2. **Physical access security:** Do Cloud providers have physical security controls to restrict access to appropriate personnel and provide safeguards over [ORG]’s servers and data?
   1. Where is [ORG]’s data stored, processed and archived? Is the data center located in a jurisdiction in which we don’t operate, and if so, do we understand the requirements of that jurisdiction?
   2. What are the procedures for granting physical access to the data center or server room?
   3. Is the data center hosted or managed by a sub service organization? Does the sub service organization have an available SSAE 16 SOC 1 Service Auditor Report?
   4. Will we have access via on-site visits?
   5. Are there data redundancy procedures to support service failures at the data center?
3. **Identity and access management:** How does [ORG]’s authorization and access model integrate with new Cloud services? Is the Cloud provider using appropriate identity and authorization schemes to restrict access to our data?
   1. Can internal and Cloud based identity management components be securely integrated?
   2. What is the risk of unauthorized access to or inappropriate use of sensitive data, and how will this be handled? How will the Cloud vendor notify the organization of a violation?
   3. Has [ORG] conducted adequate due diligence prior to assigning Cloud management privileges?
   4. Are there proper access controls for Cloud management interfaces?
   5. Has the Cloud provider implemented segregation of duties for its staff?
   6. Do [ORG] and the vendor have adequate security over administrator accounts and password requirements?
   7. Is access to the Cloud based application integrated with internal systems (i.e. use internal logical access controls) or is it part of the Cloud service provider’s logical access controls?
4. **Data management:** Does [ORG] fully understand how data will be handled in the Cloud environment?
   1. Will the complexity of multiple Cloud data stores compromise data retention?
   2. How does change management by Cloud providers impact [ORG]? How are version updates and releases, patches and fixes communicated? What information is communicated and obtained (specs, testing documents, fixes)?
   3. How is data integrity assured? Will the organization be able to remove data from Cloud data stores? What are the data deletion/destruction policies after termination of the contract?
5. **Service continuity/availability:** How do Cloud providers ensure on-going access and availability of service (and underlying data)?
   1. How often is data backed up?
   2. Do Cloud providers and if applicable their sub service providers have suitable disaster recovery and business continuity plans in place? Are these plans tested periodically?
   3. Can data be obtained and recovered in a timely manner and has timely recovery of data been defined in the Service Level Agreement?
   4. Viability: if the provider goes out of business, how do we get our data back? Do we have a contingency plan to make a timely transition to an alternative solution in the event of bankruptcy or other extended service interruption?
6. **Regulatory compliance:** how is the entire Cloud system monitored in terms of compliance? What is the impact to Internal Controls over Financial Reporting and IT General Controls under SOX?
7. **Sub-service providers:** How are Cloud providers impacted by third party providers, e.g., one organization provides software application services and another provides hosting / infrastructure services?
   1. Can [ORG] maintain visibility regarding how the Cloud service organization manages third party providers?
   2. What level of assurances does the third party offer the primary Cloud service provider? Is it sufficient to achieve and maintain compliance?
   3. How are Cloud service providers prepared to address control failures at sub-service organizations?
   4. Are various contract provisions, specifications and [ORG] rights extended to the sub-servicer operations and agreements between the prime vendor and sub-service organization(s)?
8. **Migration to the Cloud:** how do we ensure the complete and accurate migration of data, i.e., no data is lost, placed in the wrong location, or altered in the course of the migration process?
9. **IT Management:** do IT personnel have the availability to manage the Cloud service model including sufficient support resources to address user, business and technical issues?