CEI Vendor Exit Strategy

I. Reasons for Change

II. Risk Management

III. Criticality/Ease of Replacement

IV. Contract Issues

V. Knowledge Base

VI. Total Cost of Ownership

VII. Project Planning & Management

We gratefully acknowledge the feedback provided by our Certified Regulatory Vendor Program Managers (CRVPM's)® and our other valued clients who took the time to review this document.

This document has been provided at no cost and is intended to support the greater good of improving each individual company's vendor management program.

It is not to be distributed or resold in any media form nor used for any commercial sales purposes but may be adopted in whole or in part to augment a Vendor Exit Strategy Plan.

Requests for additional copies should be made to SUPPORT@COMPLIANCE-EDU.COM

CEI Vendor Exit Strategy

A crucial component of planning the initial outsource process for a high risk or critical service should include a detailed ***Exit Strategy*** so that when the time comes to part ways with the existing vendor, either prior to or at the end of the contractual term, operational and financial impact are minimized. The exit strategy could mean that the service is transitioned to another vendor or brought back in-house. Thus, there needs to be an **Exit Plan** within the overall outsourcing strategy before you even consider a vendor to outsource to. Examiners expect it.

This document is a combination of strategic and tactical issues that should be considered. While you might not be able to address the tactical issues prior to outsourcing, such as milestones for a project plan or early termination fees or availability of other providers or how in-sourcing might affect your staff as well as other projects that are under way, you should be *aware* of those issues that you'll need to plan for when the time comes to exit. Please note that this is different than *contingency planning* which is geared towards more immediate short-term solutions.

Reasons for Change: It is typical for a variety of conditions to change over the course of a relationship that might affect both you and your vendor which might necessitate an exit from the contract either prior to the end of term or at the end of it (non-renewal). Some of those conditions include:

- **Technology** – changes in technology can quickly render a vendor's service obsolete, no longer cost effective for you and/or the vendor, vulnerable to breaches or no longer competitive.
- **Economic Conditions** – changes in economic conditions could put a vendor out of business, could reduce your transaction volume where it is no longer cost-effective to outsource or could cause you to exit a particular line of business for which a vendor provides services.
- **Business Requirements** – chances are that today's needs will not be the same 7 or 5 or even 3 years from now. While long-term contracts of 5+ years might seem financially attractive, there is typically more of a downside than an upside unless your contract covers periodic renegotiation or adjustments.
- **Regulations** – new regulations are periodically issued by state and federal authorities and vendors need to be able to comply with those requirements as applicable or else the institution can be exposed to Compliance Risk and suffer financial and legal impact.
- **Vendor Direction** – vendors might eliminate unprofitable services or acquire/be acquired by other vendors which could change their go-forward strategy resulting in the termination of the service being outsourced thus requiring your company to transition it to another vendor or take it back in-house.
- **Company Direction** – a change in *your* business model, company acquisitions or a change in corporate strategy might eliminate the need for the vendor or cause your company to outgrow the capacity and capabilities of the vendor prior to the termination date of the contract.
- **Pricing** – price increases, new business models, unanticipated increases or decreases in transaction volume may change the ROI of outsourcing and render it no longer cost-effective.

Documentation: It is extremely important that any negative issues with a vendor's service are well documented. Capturing detail of the issue, notifying the vendor of the issue in a timely manner (in writing: email or hardcopy) and receiving the vendor's response in writing (when applicable) in a timely manner will help avoid finger-pointing and legal disputes down the road if an Exit is required.

The following should help you plan your Exit Strategy:

I. **Risk Management**: all risks should be identified with the service Exit Plan. There are several listed in other sections of this document but you should take into account the following:

A. **Operational Risk**: will the exit and transition cause business disruptions? It is important to identify possible points of failure and ensure that controls are in place to maximize resilience and minimize operational disruptions. Whether you bring the service in-house or transition to another vendor, infrastructure must be able to handle capacity, peak periods, backup and recovery to meet Return To Operational and Recovery Point Objective times.

B. **Reputational Risk**: transitioning the service in-house or to another vendor could cause disruptions to customers and effect quality and availability of service.

C. **Technology Risk**: it's important to ensure compatibility of systems and software when transitioning a service. Understanding the age of the infrastructure and software versions that are currently in place at either the new vendor or in-house is critical since technology refresh could be an issue and represent an unanticipated cost to you in addition to causing service disruptions. Older servers frequently perform poorly or crash frequently when nearing end-of-life or when pushed beyond their limit and used beyond end-of-life. Scalability is another factor and important as a service expands in volume so that you are not constrained by a dead-end infrastructure.

D. **Legal Risk:** when planning to outsource a service, issues pertaining to intellectual property (IP) such as proprietary processes, patents and copyright issues, data ownership, and data retention and destruction should be considered. An inventory of IP should be created prior to outsourcing. Those issues should then be incorporated into a contract. Upon planning an exit, legal review of a contract should take place immediately, especially if those issues hadn't been considered prior to contract, to ensure that there are no liability issues at stake.

E. **Compliance Risk:** regardless of whether the service is brought in-house or transitioned to another vendor, your company must ensure that all regulatory requirements can be met.

F. **Financial Risk:** a transition could cause loss of revenue, substantial early termination penalties could be incurred, hefty legal fees to extricate oneself from a contract could be incurred and, in the case where a vendor is also a customer, a potentially large revenue stream could be lost.

i. **Vendor As Customer:** when your vendor is also your customer, there are serious considerations that must be taken into account. While switching vendors is a normal course of business, there are some important relationships that you might not want to jeopardize and don't want your lines of business that might be affected to be caught off guard. Relationships between companies might exist at the Board level and

internal communication and planning is critical as is communication with the vendor-customer.

1. **Roles & responsibilities**: within your company, the Line of Business who outsources the service to be exited, Legal Dept. (if you have in-house counsel), executive management (if required), and possibly Procurement should contact the owner(s) of the vendor-customer business relationship before speaking with the vendor and discuss the reasons for the exit, timeline and other relevant issues in order to address any questions they might have. This will ensure that your position is well understood by all internally. Terminating the contract does not necessarily mean that you will lose the vendor-customer's business.

II. **Criticality/Ease of Replacement**: the criticality of the service must first be determined as evidenced by a business impact analysis (**BIA**). The BIA will help to understand requirements for Return To Operational (**RTO**) times and, equally important, Recovery Point Objectives (**RPO**). The RPO time dictates the backup schedule. While you might be able to wait 4 hours or even a full day to Return To Operational, your Recovery Point Objective might require backup of all transactions that occurred up to 1 hour prior to an outage. Losing a day's worth of transactions could be disastrous. The following need to be considered:

A. Is the service Mission Critical to the entire institution or Business Critical to a specific department?
B. Is sensitive data involved (process, store, destroy, manage, view/add/modify/delete, transport, transmit)?
C. Is your intellectual property a facet of the service? If so, Ownership needs to be addressed within a contract.
D. Is the technology complex and are there many system interdependencies?
E. If transferred to another vendor, will there be 4th parties/vendor interdependencies involved and, if so, how will those relationships be managed?
F. Are there many providers of the service, are there a limited number or is it a sole source? Although it might be a critical service, there might be numerous vendors that can provide it.
G. How long would it take to bring the service in-house or transferred to another vendor? Less than 3 months, 3-6 months, 6-12 months, more than 12 months?
H. What would be the impact to your staff if you bring it in-house?
I. What would be the impact to your customers (could cause Reputational Risk) if brought in-house or transitioned to another vendor?
J. What would be the impact to other Lines of Business?
K. What would be the impact to other projects? Will they be placed on hold? Is there enough staff to manage them?

III. **Contract Issues:** sometimes the vendors that you do business with are legacy vendors whose relationships were developed prior to all of the regulations that we currently must comply with. Finding a 20 year old contract along with all of the amendments, extensions and updates could be nearly impossible. Thus, ***a key activity is to find the contract along with all amendments*** if you plan to exit a relationship with a legacy vendor.

If you have not yet outsourced then before you even consider a vendor with whom to conduct business, you should know the causes for termination that you'd want to include in a contract.

If you have already outsourced and decide to terminate a contract prior to the termination date, it is highly recommended that Counsel review the contract prior to notifying the vendor in order to understand:

A. Legal cause
B. Penalties for early termination
C. Required Notice to the vendor and sufficient time for your institution to prepare for the transition to another vendor or to bring the service in-house.

The contract issues listed below should be considered when planning your Exit Strategy.

A. Does the contract provide for termination rights for Merger or acquisition? (Your vendor might be acquired by a vendor that you don't like or that has a different strategic direction)
B. Does the contract provide for termination rights for Convenience (typically not something you'll find in a contract for a critical service)?
C. Does the contract provide for termination rights for Substantial increase in cost?
D. Does the contract provide for termination rights for failure to meet service standards?
E. Does the contract provide for termination rights for failure to provide critical services?
F. Does the contract provide for dispute resolution prior to termination? If so, is there a cure period prior to termination?
G. Does the contract provide for termination rights for Failure to prevent violations of law or unfair, deceptive and abusive acts and practices (UDAAP)?
H. Does the contract provide for termination rights for Bankruptcy?
I. Does the contract provide for termination rights for Company closure?
J. Does the contract provide for termination rights for Insolvency?
K. Does the contract state termination and notification requirements with time frames?
L. Does the contract allow right to hire the vendor's employees? Critical skill sets might be required that would otherwise be difficult to find.
M. Does the contract specify how you will extract your data (can you do it yourself or is the vendor required to do it?)
N. Does the contract specify the File Format in which you will receive your data?

O. Does the contract specify the time expected to extract and transfer the data to you?

P. Does the contract specify the cost to extract the data?

Q. Does the contract specify the cost to customize anything beyond "standard"? This should be specified in a Rate Schedule.

R. Does the contract specify who owns data?

S. Does the contract specify who owns intellectual property?

T. Does the contract specify how the data will be archived, maintained or destroyed and any cost to do so?

U. Does the contract specify who owns assets (infrastructure and/or software licenses that sit at the vendor's location)?

V. Does the contract provide for continuation of services if the Exit/transition is not completed by the end of term or agreed upon period?

IV. **Knowledge Base:** once a service is outsourced, your staff will likely be allocated to other functions, possibly in other lines of business, and working knowledge of the outsourced function could be diminished or lost. Thus, it is important to maintain staff that has a level of proficiency and familiarity with the outsourced service should it need to be brought in-house or migrated to another vendor. Prior to outsourcing, create an inventory of the following:

A. **Processes**

B. **Procedures**

C. **Data Touchpoints** including systems, storage and cloud (where does the data go?)

D. **Skill Sets required** to perform the function including technical and business knowledge

E. **Technology requirements** including hardware, software, bandwidth requirements to handle peak period transaction volume, data encryption

F. **Backup requirements**, Return To Operational times and, just as important, *Recovery Point Objectives* since this will dictate the backup architecture and replication schedule

V. **Total Cost of Ownership (TCO) Model**: in order to plan for the service being brought in-house or transitioned to another vendor, a Total Cost of Ownership model should be built in advance in order to get a realistic idea of the hard and soft costs over a specific period of time. Factors to consider include:

A. **Cost-Benefit Model**: if it has not already been done when originally planning the outsource, a cost comparison should be prepared to determine cost to bring the service in-house vs outsourcing to another vendor.

B. **Technology Refresh:** how long will the existing technology support the service and what will be the cost of technology refresh to maintain the service in order to avoid disruption?

C. **Maintenance Fees:** hardware and software maintenance fees for all components

D. **Staff Costs**: fully loaded costs should be defined (salary + benefits) based upon the number of FTE's required to run the service and including any anticipated overtime costs.

E. **Disaster Recovery**: if the service is being brought back in-house then you'd likely want to have a Hot/Warm/Cold site available for contingency planning.

   i. The cost will vary based upon the availability contracted for (hot/warm/cold)

   ii. Your company might have to provide hardware and software or pay a fee towards it which will vary depending upon whether it is dedicated or multi-tenant infrastructure.

F. **Cost Centers**: if individual department cost centers are being billed then estimated network bandwidth can be projected in order to determine the cost allocated to each department along with any shared costs for hardware, software and staff.

G. **Controls**: if the service is being brought in-house, what is the cost to implement, test, maintain and monitor any physical, technical and administrative controls required to protect systems and data?

VI. **Project Planning and Management:** do you have enough resources with the proper skill sets to successfully manage exiting the relationship? Exiting a vendor relationship requires as much, if not more, project management as outsourcing the function in the first place. You might be managing parallel efforts away from one vendor while migrating to another, yet still maintaining current production in parallel with testing prior to final migration.

A. **Exit Team**: an Exit Team should first be assembled by anticipated Role Required.

   i. **Executive Team/Committee**: with most critical/high risk services that are brought back in-house or transitioned to another vendor, there must be Executive sponsorship. The Executive Team/Committee should be familiar with its strategic goals (better, faster, cheaper, more competitive, opportunity for new value creation opportunities, etc.) and help determine whether the Exit will keep it on track to meet those goals.

   ii. **Project Manager:** overall responsibility for the success of the Exit.

   iii. **Exit-Vendor Relationship Manager**: this person might be different than or the same as the Project Manager

   iv. **New-Vendor Relationship Manager**: this person might be different than or the same as the Project Manager or Existing-Vendor Relationship Manager

   v. **Resources and Supporting Roles**: make a list of staff required based upon role such as hardware engineer, DBA, software engineer, network engineer, information security specialist, business analyst, governance analyst, LOB interface.

   vi. **Staff Allocation**: a Project Schedule will help determine the number of resources required and at what point they need to be involved in the Exit

project. This will also help you determine the cost of the migration and where project bottlenecks could occur, thus impacting the schedule and total cost to exit.

vii. **Project Plan with Milestones**: this usually occurs once a decision has been made to exit and either bring the service in-house or transitioned to another vendor. While a detailed project plan is not typically a part of an initial Exit Strategy, listing it as a key component of the exit process should be a part of it.

viii. **Additional Stakeholders**: create a list who else should be involved in the Exit such as Risk, Finance, Compliance, Legal, Business Owner.

B. **Communication Plan:** open lines of communication are essential to a successful transition. The following should be planned:

i. **Who** needs to know specific pieces of information?

ii. **When** do they need to know (timeline)

iii. **What** information should be provided?

iv. **How** should information be communicated (email, conference call, in person, in writing)

C. **Transition Time:** What is the estimated time to exit/migrate? A project plan should be built that lists all of the tasks, milestones, interdependencies and staffing requirements.

D. **Requirements:**

i. **Business Requirements**: does the line of business have new requirements since originally outsourcing the function? A ***Business Impact Analysis*** (BIA) should be conducted prior to the exit to ensure that critical requirements are understood and current.

ii. **Technology Requirements**: would bringing the service in-house require an investment to upgrade existing and purchase new hardware, software or infrastructure?

iii. **Capacity Planning:** define the peak volumes to ensure that there is enough processing power and bandwidth to handle the peaks.

iv. **Controls:** based upon the type of data, what physical, technical and administrative controls are required to protect the data and what is the cost to implement, test, maintain and monitor those controls if it is being brought in-house? If the service is moving to a new vendor, what are the controls that the vendor must have in place and what types of audits, assessments, test reports will your company require that the vendor provide and who within your company will review those reports?

v. **Staffing Requirements**:

1. If the service is being brought back in-house, what skill sets are required to run it?

2. Do those skill sets exist in-house?
3. If the skill sets do not exist in-house, are they easily found and affordable?
4. Can your company acquire the staff from the job market and then cross train its existing staff to help run and support the service?

vi. **Resilience**: many of the factors already listed will help in determining the requirements to minimize disruptions but here is a list of things to consider.

1. **Concentration Risk**: Concentration Risk occurs when industry consolidation via mergers and acquisitions occur and there are fewer vendors available to service the same number of customers. Thus, how many vendors provide the service?
2. **Capacity**: if the service is transitioned to another vendor, will that vendor be able to restore service to all of its clients if a disruption occurs?
3. **Power Requirements**: if the service is brought in-house, will additional UPS devices or generators be required? If additional UPS devices are required, what is the minimum time that the UPS should last?
4. **Failover**: if the service is being brought in-house, is an alternate site required if the primary goes down? If so, will it be a hot site, warm, site, cold site?

vii. **Physical Space:** is there enough physical space available to accommodate equipment and staff if bringing the service in-house? If not, how much space would be required and what are the costs of construction/expansion inclusive of wiring/cabling, hvac, fire detection/suppression systems, offices, and office equipment and supplies.