Vendor Management Using COBIT 5

William F Crowe, CISA, CRISC, CISM, CRMA, MBA
September 2013
All About Me

- 16 years’ experience in Information Security, Risk Management, Third Party Oversight and IT Audit
- Vice President Business IT Risk Management JPM Chase
- Bachelors of Science in Business Management and a Master’s in Business Administration.
- Adjunct Professor with ITT-Technical Training Institute
- President of the ISACA Jacksonville 2012 K. Wayne Snipes award winning chapter.
Introduction
Vendor Management
Threats and Risks Related to Vendor Management
Financial Impact of Inadequate Vendor Management
Mitigating the risks
3 Tier Framework
Binding Documents
Managing a Cloud Service Provider
Introduction

- **Background**
  - Vendors constitute an important part of an enterprise’s external environment

- **Purpose**
  - This publication on vendor management provides additional and more detailed practical guidance and facilitates the vendor management process for IT and business professionals.

- **Who should use**
  - The vendor management process involves many stakeholder functions within the enterprise.
Vendor Management

- **Vendor Management Defined**
  - Third party that supplies products or services to an enterprise.
  - Strategic process

- **Focus their vendor management efforts on third-party relationships that:**
  - Play a vital role in the enterprise’s daily operations.
  - Have a critical impact on the success of the enterprise’s strategic projects
  - Require long-term contracts
  - Have potential for significant financial implications
  - Are difficult to change overnight
  - Require frequent interaction and collaboration for disputes or have complex problem-resolution mechanisms
  - Access or manage substantial critical or sensitive data
Vendor Management (cont’d)

- **Life Cycle Phases**
  - **Setup**
    - Bidding Process
      - RFI
      - RFQ
      - RFP
  - **Contract**
    - Forms a common understanding of what needs to be achieved
    - Defines all deliverables, relevant service levels and metrics
    - Defines responsibilities and obligations
    - Defines the terms and conditions
    - Specifies how risk will be allocated between parties
    - Defines legal counsel and jurisdiction stipulations
Vendor Management (cont’d)

- Life Cycle Phases (cont’d)
  - Operations
    - Transition-in period
    - Contract Change Management
  - Transition-out
    - Vendor is no longer needed or willing to deliver product/services
    - Exit strategy
Common Threats in Vendor Management

Following are the most common vendor management threats and related risk components (financial, operational, legal/compliance and reputational)

**T1 Vendor Selection**

Description: Poor performance when ramp up is complete due to unforeseen inadequacies.

Risk: Exposes the enterprise to a financial risk in the form of the considerable costs associated with replacing the vendor, potential revenue loss and ineffectiveness of financial penalties.

Risk affected—Financial, operational, reputational and legal/compliance
Threats and Risks Related to Vendor Management (Cont’d)

T2 Contract Development
Description: An incomplete contract, not covering all the aspects of the relationship that need to be managed up front, is a major threat.
Risk: Neglecting to detail payment terms and price-setting mechanism requiring unrealistic or inadequate service levels from the vendors.
Risk affected—Financial, operational and legal/compliance.

T3 Requirements
Description: Inadequately setting up and detailing the requirements can have a huge impact on the proper execution of the service by the vendor.
Risk: Enterprises tend to focus on solutions instead of defining the requirements and giving freedom to the vendor to propose the optimal solution.
Risk affected—Financial, operational, reputational and legal/compliance.
Threats and Risks Related to Vendor Management (Cont’d)

**T4 Governance**
Description: A lack of governance during the contractual vendor relationship life cycle can be considered a major threat to proper vendor management.
Risk: Failure to define an adequate governance model between the enterprise and the vendor increases operational and compliance risk
*Risk affected*—*Financial, operational and legal/compliance*

**T5 Strategy**
Description—The enterprise vendor management strategy has considerable impact on the enterprise’s business activities.
Risk—Over reliance on a specific vendor, especially for business-critical tasks, increases operational risk (e.g., lack of in-house knowledge and demotivation of employees) and, consequently, financial risk (e.g., vendor can over price its service due to the enterprise’s dependence on the vendor).
*Risk affected*—*Financial, operational and legal/compliance*
Financial Impact of Inadequate Vendor Management

- During the setup phase, most activities related to vendor management are internal
  - Minimal impact financially
  - During this stage, enterprises are likely to cut corners to speed up the process
    - Can lead to financial impacts downstream
- In the contract phase, more internal and external stakeholders are involved and negotiations need to be more formal.
- Rectifying issues or correcting mistakes may require more effort and resources than during the setup phase.
- If it is discovered that requirements were not properly defined during setup, certain steps may need to be repeated
The amount of effort and resources required to correct issues or mistakes during the transition-in period and the operations phase is significantly higher.

Problems in the contract or deficiencies in products and services due to poor requirements definition should be addressed immediately to prevent additional impact on operations.
Mitigating the Risks

- Awareness about the importance of proper vendor management constitutes the first step to implementing an effective process.
- Enterprises have different approaches to managing vendor-related risk.
- **Managing vendors has many benefits**
  - Data loss reduction
  - Decrease in audit findings
  - Cost optimization
  - Increased availability
  - Liability reduction
  - Increased end-user satisfaction
  - Value creation
Mitigating the Risks (Cont’d)

- COBIT 5 Guidance on Mitigation Actions
  - 22 mitigation actions:
    - 1. Diversify sourcing strategy to avoid overreliance or vendor lock-in
    - 2. Establish policies and procedures for vendor management.
    - 3. Establish a vendor management governance model
    - 4. Set up a vendor management organization within the enterprise
    - 5. Foresee requirements regarding the skills and competencies of the vendor employees
    - 6. Use standard documents and templates
    - 7. Formulate clear requirements:
    - 8. Perform adequate vendor selection
    - 9. Cover all relevant life-cycle events during contract drafting
    - 10. Determine the adequate security and controls needed during the relationship
Mitigating the Risks (Cont’d)

- 22 mitigation actions continued
  - 11. Set up SLAs
  - 12. Set up operating level agreements (OLAs) and underpinning contracts
  - 13. Set up appropriate vendor performance/service level monitoring and reporting
  - 14. Establish a penalties and reward model with the vendor
  - 15. Conduct adequate vendor relationship management during the life cycle
  - 16. Review contracts and SLAs on a periodic basis
  - 17. Conduct vendor risk management
  - 18. Perform an evaluation of compliance with enterprise policies
  - 19. Perform an evaluation of vendor internal controls
  - 20. Plan and manage the end of the relationship
  - 21. Use a vendor management system
  - 22. Create data and hardware disposal stipulations
3 Tier Framework

- The 3 Tier Framework defines the key parameters affecting the product or service provisioning.
  - **Client Input**
    - The enterprise defines the key parameters affecting the product or service provisioning.
    - The enterprise provides input on the values of the key parameters.
  - **Delivery Model**
    - The vendor’s solution architects design a delivery model that takes into account the parameters from the client input.
    - The result of the model is a detailed overview of all the products and services that the vendor will deliver, the total cost, and transparent detail on the influence that parameters have on cost.
3 Tier Framework (cont’d)

- Cost Model
  - In the cost model, a detailed price per service activity or work unit is determined as it will be delivered and charged to the client.
Throughout the vendor relationship life cycle a number of information items should be prepared to support and document the steps in the process

- Requirements overviews
- **Call for Tender**
  - Sections
    - Enterprise Context
    - IT Governance and Management
    - Requested Services
    - Roles and Responsibilities
    - General Requirements
The call for tender should always make three elements clear to the vendor.

1. The enterprise context and more specific information on the enterprise IT governance and management
2. The requested services that the enterprise wants to acquire. It is vital to detail these service requirements as precisely as possible to enable the vendor to prepare an adequate offer
3. The expected roles and responsibilities for the service requirements.

Setting clear expectations in the call for tender phase provides a basis for negotiations, guarantees that a topic is not overlooked, and may help to avoid confusion or discussions in a later stage of the collaboration.
Vendor Contract

The enterprise should detail in the vendor contract, among other factors, the following items:

- Fees
- Roles and responsibilities
- Deliverables
- Workflows
- Fallback procedures
- Penalty and reward mechanisms
- Confidentiality of information
- Intellectual property
- Transition-out procedures
Different kinds of contracts exist regarding price structure.

- **Time and means (T&M) contracts**—The vendor provides resources per specifications, and payment is based on the performed work hours and used means.
- **Fixed-price contracts (FPC)**—The completion or performance of certain tasks per specifications is expected for payment of a fixed price
- **Hybrid contracts**—These contracts are a blend of FPC and T&M contracts

**Service Level Agreements**

- An SLA is an agreement, preferably documented, between a product or service provider and the enterprise that defines minimum performance targets for a deliverable and how they will be measured and reported.
  - SLA levels are often categorized into:
    - **Bronze**—Modest service level targets to guarantee basic availability and support for noncritical systems
Silver—Standard service levels in the industry and recommended for initial discussions with the business

Gold—Aggressive service levels to prevent any unscheduled downtime of critical systems that could impact customer operations or end users

Drafting an SLA

- Two critical parts should be included
  - The identification of services and performance metrics
  - Processes related to SLA governance and change management.

Operating Level Agreements and Underpinning Contracts

- Two or more (internal or external) groups collaborate for the delivery of these services, they usually define an OLA that applies to all parties involved
- Underpinning contract is an agreement between the vendor and a third party or subcontractor, whereby the third party provides services or goods to the vendor to support the vendor’s delivery of the service to the enterprise.
Managing a Cloud Service Provider

- Cloud computing has become more than just another IT buzzword.
- Cloud Service Providers (CSP) in many cases are strategic vendors.
- Concept of cloud computing constitutes an important part of the vendor management scope.
- These vendors have very specific cloud-related risk and challenges.
- Security and data privacy concerns are typically seen as critical barriers to the adoption of cloud services.
- The remaining discussion for managing a Cloud Service Providers will be from Chapter 6 of the Vendor management using COBIT 5 manual.
Questions?