IT Service Delivery And Support Week Seven: SLA

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Outsourcing & Vendor Management

* Outsourcing Drivers
* Outsourced IT Works
* Outsourced IT Activity Samples
* Top Three Outsourcing Risks
* Outsourcing Workflow
* Outsourcing Control Points
* Audit Report for Service Providers (SSAE16)
* References

Outsourcing & Vendor Management

Outsourcing Drivers

* Cost or internal headcount needs to be reduced
* Internal capacity is constrained by increasing market demand
* Internal manufacturing or service performance is insufficient or does not meet requirements

Outsourcing & Vendor Management

Outsourced IT Works

* Application development and maintenance
* Infrastructure management
* Help desk
* Independent testing and validation
* Data center management
* Systems integration
* R&D
* Managed security
* **Cloud computing**

Outsourcing & Vendor Management

Outsourced IT Activity Samples

* Outsourced information management and storage (all value stored, databases, customer files, key, parameters, etc.)
* Outsourced core knowledge systems and, development of new, or maintenance of existing, systems (corporate memory, key knowledge , elements, activity processes, executive preferences, etc.)
* Outsourced major computer installation and ancillary support services
* Outsourced networks or communications
* Provision of computer equipment, replacement of network PCs and servers, network devices

Outsourcing & Vendor Management

Top Three Outsource Risks

* Logical IS Security
* Total Dependence and Exit Barriers
* Legal Consequences

Outsourcing & Vendor Management

Other Outsource Risks

* On-time delivery performance and end-customer satisfaction levels may decline because of delays at third parties
* Product or service quality may also suffer in outsourcing, affecting customer satisfaction.
* The outsourcing transition phase may also fail if schedules and budgets are not achieved because of insufficient planning and/or resources.
* Providers may not be financially viable, thereby exposing the company to supply interruption risk.

Outsourcing & Vendor Management

Outsourcing Workflow

* Board and Senior Management Oversight
* Risk Assessment
* Due Diligence
* Contract Process
* Ongoing Oversight and Monitoring

Outsourcing & Vendor Management

Board and Senior Management Oversight

* Accountability
* Senior Management Involvement
* Resource Allocation
* Authority and Independent of the vendor management team
* Reporting
* Identify Program Weakness and Take Corrective Actions

Outsourcing & Vendor Management

* Risk Assessment
  * Risk Metrics and Tolerance (Inherent and Residual Risks Rating)
  * Core Risk Categories
    * Strategic Risk
    * Reputational Risk
    * Operational Risk
    * Transactional Risk
    * Credit Risk
    * Compliance Risk
  * Risk Escalation
  * Ongoing Risk Assessment & Update

Outsourcing & Vendor Management

Due Diligences Activities

* Questionnaire
* Management Interviews
* Industry-Related Surveillance
* On-site Visits
* Analysis and Follow-Up

Outsourcing & Vendor Management

Contract Procedures

* RFP Process
* Preliminary Discussion
* Relationship Risk Allocation and Input from Legal Counsel
* Contract Drafting and Negotiation
* Contract Terms and Provisions
* Contract Review, Approval and Execution (Legal to approval and Authorized officer to execute)
* Contract Boarding and Ongoing Monitoring

Outsourcing & Vendor Management

Ongoing Oversight & Monitoring

* Quality of Service
* Risk Management Practices
* Financial Condition
* Material Changes
* Compliance with Contract Provisions

Outsourcing & Vendor Management

Service Organization Control Report

* *SAS70 & SSAE16*
* *ISACA Journal* volume 2, 2013
  * Common Myths of Service Organisation Control (SOC) Reports

Outsourcing & Vendor Management

* Internal Audit Considerations - Strategic Fit and Sourcing Evaluation
  * Assess strategic context and whether benchmarking and other supporting market information is reliable and complete
  * Determine whether there are adequate IT governance processes in place to guide outsourcing considerations and alignment with business outsourcing goals
  * Confirm whether stakeholder involvement and process ownership are clear and aligned
  * Consider the service provider's client base, experience, and reputation for reliability

Outsourcing & Vendor Management

Internal Audit Considerations - Decision-making Process

* Assess whether information in the detailed analysis is reliable and considers all business risks and implementation risk.
* Ascertain whether governance and approval processes are transparent, documented, and completed.
* Determine whether appropriate parties and experts are included in the evaluation process
* Determine whether other major stakeholders are kept informed

Outsourcing & Vendor Management

Internal Audit Considerations - Decision-making Process (continue)

* Assess management's contingency plans if the outsourcing initiative fails at various stages
* Evaluate whether estimates of failure and the probable impacts/costs are considered in the business case or when comparing options among providers.
* Evaluate sensitivity of cost/benefits to assumptions.
* Identify key performance measures and data sources.

Outsourcing & Vendor Management

Internal Audit Considerations - Tender Process and Contracting

* Evaluate bid evaluation process, timing, criteria, completeness, and approval transparency.
* Review control assurance requirements of management such as a service auditor's report (e.g., Statement on Standards for Attestation Engagements (SSAE) No. 16: Reporting on Controls at a Service Organization, issued by The American Institute of Certified Public Accountants (AICPA) or International Standard on Assurance Engagements (ISAE) 3402, issued by the International Accounting and Assurance Standards Board (IAASB) of the International Federation of Accountants (IFAC)) or ongoing evaluations; ensure that the organization's right to audit clause is drafted effectively.

Outsourcing & Vendor Management

Internal Audit Considerations - Tender Process and Contracting (continue)

* Assess the project team's experience and capability as well as whether it is resourced appropriately to meet the need.
* Evaluate whether risk management, legal, human resources (HR), and finance functions are involved as needed.
* Perform due diligence reviews or assess management's review of provider operations.
* Consider ongoing or periodic evaluations conducted by other assurance providers for gaining comfort on performance capability control effectiveness. Review SLAs and OLAs to ensure that performance measures are defined and reliable. This should be done initially by management; however, internal audit can assess reliability with a focus on risk/control performance expectations and compliance with key provider standards or those specifically demanded by the customer or applicable regulations.

Outsourcing & Vendor Management

* Internal Audit Considerations - Implementation/Transition
  * Perform a pre-implementation review to ensure the project is following standard disciplines.
  * Review contingency plans if transition is not affected appropriately.
  * Determine whether risks and actions are identified, mitigated, and escalated to stakeholders appropriately and promptly during the implementation process.
  * Ascertain whether "go"/"no go" decisions are governed properly and based on reliable information.
  * Assess whether management has performed the appropriate testing before supporting the "go live" decision.
  * Determine whether appropriate stakeholders are involved and informed.
  * Determine whether reliable information for decision-making is available to the project management and senior management.

Outsourcing & Vendor Management

Internal Audit Considerations -Monitoring & Reporting

* Understand how provider performance and compliance with the contract will be assessed and reviewed routinely by management.
* Evaluate the reliability of metrics that are designed and used to manage risk regarding IT operations, changes, and security.
* Assess how concerns and areas for improvement will be communicated and leveraged to improve current and future operations/contracts.
* Ensure the outsourcing activity is part of the audit universe and risk-assessed routinely.
* Determine how internal audit is alerted to changes in relationships in the future.
* Assess performance against KPIs established during the planning phase.

Outsourcing & Vendor Management

Internal Audit Considerations – Renegotiation

* Understand the strategies and information needed to ensure optimal future negotiations.
* Understand reversibility and monitoring or performance results.
* Ensure that experts and process owners are driving renegotiation improvements.
* Ensure that relevant dates for audit involvement are considered in the annual risk assessment process.
* Ensure that adequate/accurate historical information and performance measures are available.

Outsourcing & Vendor Management

Internal Audit Considerations – Reversibility

* Assess the adequacy of contingency plans if the outsourcing arrangement does not work.
* Evaluate whether management has quantified the estimated costs and likelihood of failure.
* Determine whether failure has been considered in the business case and ROI needs.
* Ask whether management considered the use of other providers effectively to avoid unnecessary dependencies.
* Determine how management evaluated the provider's viability. Internal audit may need to confirm or evaluate the reliability of that evaluation.

Outsourcing & Vendor Management

Internal Audit Considerations – Reversibility (continue)

* Ascertain whether the trigger points to initiate or consider changes in the provider are understood and predefined.
* Consider other risks that might drive the need for bringing the process back in-house — including macroeconomic and political/geographical concerns — and determine whether these have been assessed.
* Determine whether the provider has sound, sustainable, business continuity planning (BCP) capabilities.
* Determine whether the contract has an appropriate exit clause.

Outsourcing & Vendor Management

Key Controls

* Contract
* Statement of Work (SLA)
* High Level Monitoring
* Connectivity and Network Security
* Data Security
* Project Monitoring and Governance
* Compliance with Regulatory Requirements
* Benefit Measurement
* Customer Satisfaction
* Impact on IT Strategy

Service Level Management

* SLM Objectives
* Related Issues
* Process Flow
* Key Players
* Service Level Agreement (SLA) Elements
* Three Pillars of Service Quality Measurement

SLM Objectives

* Measure Performance vs. Defined and Agreed Limits
* Prevention of SLA Breaches
* Identification and Monitoring of Key Performance
* Future Improvement

SLA Management Common Issues

Common Issues (Audit Concerns)

* Unrealistic
* Too complex
* Unclear measurements
* Lack of aggregate view (asset, people, process)
* Too many alerts/notifications (threshold setting)
* Resource allocation
* Micro management
* Out of control elements
* Multiple SLAs
* Use of SLA Metrics
* Process Fraud
* Priority Setting
* Escalation Process
* Excessive Admin. burden

SLA Process Flow

* Key Players
  * Service Users/Subscribers
  * Service Providers/Delivery Groups
  * Service Delivery Managers

Service Level Agreement

* Objectives
* Focus
* Reporting
* Validation Triggers
* Escalation Process

SLA Objectives

* Compliance with contracts
* Increase User Confidence
* Monitoring
* Identify improvement opportunities
* User expectation
* System/service reliability and stability
* Penalties for non-compliance
* Auditing
* Generating operational data for analysis purpose
* Reporting

SLA Focus and Reporting

* Define what's been monitored?
* How to monitor?
* When to report?
* Cross Reporting Threshold (service tickets as an example)
  * Before
  * During
  * After

SLA Focus and Reporting (cont.)

* Validation Triggers
  * SLA Initiation
  * On-going
  * SLA Termination

SLA Monitoring and Escalation

* Event Based Monitoring
* Periodical/Scheduled checks
* Escalation Thresholds
  * Time Based
  * Rule Based
* Escalation Actions
  * Notification
  * Prioritizing
  * Create new associated records
  * Associate to another record

The Three Pillars of Service Quality Measurement

* Responsiveness
* Availabilities
* Quality of Services (QoS)
  * Using Metrics
  * Additional

Dealing with Numbers

* Avoid Single Metric
* Avoid Manual Inputs
* Use Impartial Third Party to Collect Data
* No Pressure on Users
* Use Analytical Model