GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Information Technology Outsourcing

2nd Edition

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG®) 7
Information Technology Outsourcing
2nd Edition

June 2012

Executive Summary

The purpose of the Information Technology (IT) Outsourcing Global Technology Audit Guide is to help chief audit executives (CAEs) and their audit teams determine the extent of internal auditor involvement when IT is partly or fully outsourced in their entities. This guide provides information on the types of IT outsourcing (ITO) the life cycle of IT outsourcing, and how internal auditors can approach risk in connection with IT outsourcing delivery.

IT outsourcing is the contracting of IT functions, previously performed in-house, to an external service organization. Increasingly organizations are economically motivated to outsource portions of IT processes to focus on their core business. In some government environments the IT function is outsourced to a government shared services body that provides services, including IT services to numerous government departments. Some organizations use a single IT service provider and some use multisourcing, that is, the provisioning and blending of business and IT services toward an optimal mix of internal and external providers. Multisourcing can add complexity.

Key questions to ask when considering audits of IT outsourcing activities:

- How do IT control activities that have been outsourced relate to business processes?
- Are internal auditors appropriately involved during key stages of the outsourcing life cycle?
- Do internal auditors have sufficient IT knowledge and experience to consider risk and provide the right input?
- If IT control activities are transitioned to an IT service organization, does the service provider understand the roles and expectations of internal audit stakeholders? Are internal auditors able to see IT risk and present recommendations for processes that have been outsourced?
- What role do internal audit teams play during renegotiation, repatriation, and renewal of outsourcing contracts?

Introduction

Many reasons exist for outsourcing technology to service organizations, including expertise, cost restructuring, capacity management, and risk management; however, user entity management retains responsibility for the control activities and operational results.

Often, core financial and operational processes are dependent on technology that is outsourced. When IT processes — such as security, change management, and operations in support of key business processes — are outsourced, the internal auditor may be required to consider the effect on control activities. How will the service organization give the user entity visibility into ongoing operation of controls? Technology such as cloud computing facilitates the achievement of the user entity's strategy but can limit visibility into the effectiveness of control activities.

Depending on the nature of the outsourced process, the internal audit activity may need to evaluate the adequacy and effectiveness of IT controls conducted by a service provider, subject to performance Standard 2130. A1: Control. As a result, assurance is often required to determine whether there is sufficient internal control over processing performed by the service provider, because IT general controls are integral to assessing risk regarding information reliability, operations, and compliance objectives.

The complexity of the IT function, changes in technology, and proximity of expertise compel the user entity's CAE to assess risk to the business and the operating effectiveness of the control activities conducted by the service provider.

Internal auditor involvement varies depending on:

1. Management's capability and the governance structure in place to deal with business and IT risks.
2. Management's experience with outsourcing complex activities and managing large projects.
3. Involvement of other functions such as risk management, compliance groups, or other internal audit functions.
4. The nature of the control activities delivered by the IT service provider.
5. Expectations of key internal audit stakeholders.

This guide will:

- Outline the common IT outsourcing risks for the CAE to consider and mechanisms for providing assurance.

Performance Standards

2130 – Control: The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

- Walk the internal auditor through the most common types of IT outsourcing and discuss the seven life cycle stages often experienced when considering IT outsourcing:
    1. Strategic fit and sourcing evaluation.
    2. Decision-making process and business case.
    3. Tender process and contracting.
    4. Implementation and transition.
    5. Monitoring and reporting.
    6. Renegotiation.
    7. Reversibility.
- Provide the user entity guidance about risk and control considerations when deciding on outsourcing a function to an IT service provider.
- Provide the service provider guidance regarding risk and control considerations in connection with delivery of the outsourced IT process.

The appendix contains an audit program for the IT Outsourcing Life Cycle and IT Outsourcing Delivery.

This guidance is specific to IT outsourcing risk and processes. Where businesses are interdependent, and where "external" and "extended" business relationships exist, internal auditors may also find useful the Practice Guide, Auditing External Business Relationships.

1 – Types of IT Outsourcing

IT outsourcing has changed from traditional outsourced services, such as application development and IT help desk activities, to high-end services, such as product development, specialized research & development (R&D), and distributed computer support. Organizations continue to outsource IT services as new technologies emerge.

Outsourcing is sometimes confused with off-shoring. The difference between outsourcing and off-shoring is:

Outsourcing: Contracting the operation of specific business functions or knowledge-related work with an external service provider.
Off-shoring: Relocating activities that were previously managed in the domestic country.

The scope of this guide relates to IT outsourcing, no matter whether they are located domestically or in foreign locations. However, risk considerations should be given to domestic versus foreign providers in the business case to outsource. This guide does not apply to internal off-shoring activities, although many considerations may be similar.

The most common outsourced IT services include:

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

Service providers and user entities may use different names for the types of outsourced services. User entities also may outsource one or more of these services to multiple service providers.

Application Development & Maintenance

When development and specific functionalities or modules within a software application are outsourced, the user entity should give priority to third-party software development firms with technical skill and experiential knowledge to address client specifications. Coding should follow a rigorous software development life cycle (SDLC) methodology established as part of the service provider's standard quality process. In certain arrangements, SDLC steps may be specified, monitored, and managed directly by the user entity. The user requirements or work statement should be defined clearly from the beginning of the formal stages of the development phase. Consider involving internal auditors, as recommended in *GTAG 12 Auditing IT Projects:*

- To provide ongoing advice throughout strategic projects.
- To identify key risks or issues early.

In most cases, the SDLC process ends with the successful completion of the client's user acceptance testing, although the service provider may be responsible only until the unit testing's completion. The system, integration, and user-testing phases are essential elements that ensure the system satisfies the client's requirements. Testing can be conducted by the client team or jointly by the client and service provider. In either case, any problems or issues noted in the testing phase are referred back to the service provider for correction.

Ongoing maintenance of existing applications and application upgrades should respond to software development recommendations by the business process users and stakeholders. Recommendations may be minor changes, such as the creation of new fields or reports, or major changes, such as the creation of a new module.

Infrastructure Management

Services to manage and maintain the IT infrastructure can be classified as infrastructure management. These services include network management, maintaining overall infrastructure performance and availability, disaster recovery strategies and capabilities, troubleshooting errors, maintaining databases, and backing up and restoring services. More recent and value-added services under this category are the monitoring of IT infrastructure activities and capacity management, performing of downtime analyses, and reporting of critical system failures and their implications.

Help Desk

Any maintenance service, such as troubleshooting problems, production support, and infrastructure management, can be categorized as a help desk service. Under this arrangement, the service provider's personnel support the client through various IT problems either on site (i.e., at the client's premises) or off site (i.e., from the service provider's premises). Turn-around time (TAT) (i.e., responses and resolutions) is then defined for each level of service.

Critical compliance with service levels consists of meeting defined TATs and the quality of the service provided. In addition, management expectations are set for ongoing monitoring procedures that measure and compare actual performance to the expected service-level parameters. Finally, performance results, deficiencies, and remediation, should be used as core criteria for ongoing vendor evaluation.

Independent Testing and Validation

Many organizations outsource the testing and validation of software developed in-house or by a third party. Specialized testing of the developed system is used to monitor the system's performance and identify and track programming errors or problems to resolution.

Data Center Management

As more IT industry sectors, vendors, and service providers came into the market, there was a shift in the outsourcing mind-set. From simple cost savings, the objective of outsourcing changed to provide higher levels of operational efficiency, specialized products, and dynamic growth. Vendors started offering specialized services that could be leveraged across multiple clients, regardless of the industry sector. One such example is the use of data center operations.

Data centers today typically provide the following services:

- Physical hosting of mainframes and distributed servers and other IT assets.
- Hardware, software, and operating system planning, specification, procurement, installation, configuration, maintenance, upgrades, and management.
- Continuous monitoring of the server's performance and operational status.
- Server/mainframe capacity management, including capacity planning, load balancing, tuning, and reconfiguration.
- Server builds and application software installation and upgrades that meet release procedures agreed upon by the client and service provider.
- Backup and restoration.
- Recovery of server systems in the event of a disaster, which follow implemented TATs.

System Integration

In a decentralized environment, various functions are organized through disparate systems and applications that may not talk to each other. Decentralized environments require more human intervention to perform system and application updates, clear out-of-balance conditions, data sources, and detect erroneous results.
System integration services involve the development of scripts, modules, tools, or programs to integrate multiple applications and systems. This enables existing applications to communicate with one another seamlessly, resulting in one consolidated system. A key limitation of systems integration is its dependence on interoperability and the accuracy of data sources.

R&D

To adapt and innovate to meet market needs while continuing to build and maintain business intelligence databases, many organizations outsource the research and development of different technologies, solutions, processes, and systems. Outsourced research also includes the use of third-party vendors to perform market analyses that identify the trends and responsiveness of key industry sectors for certain products.

Managed Security

Many organizations outsource security services. This outsourcing area also is called managed security services (MSS) due to the service provider's management of an organization's third-party security requirements. MSS is defined as the service that oversees an organization's security over its entire IT infrastructure, data assets, and user management activities. Other terms used to identify this function include Internet security services, security outsourcing, intelligence services, security consulting services, network security services, security management services, security assessment services, security consulting, and IT security services.

Depending on the client's needs, contract terms may include the use of end-to-end security architecture design and support (e.g., design consultation, implementation, security administration, user provisioning, and technical support) or the management of specific security functions on a particular system (e.g., firewall monitoring, data transmission, content filtering, virus protection, intrusion detection and response, and network vulnerability assessments).

Cloud Computing

Cloud computing provides scalable and often virtualized computing resources to fill a business need on demand. Cloud computing provides servers, storage, and computer power as a service rather than a product. Resources, software, and other information are provided dynamically like a utility over a network, often the Internet. Types of delivery include private cloud, public cloud, hybrid cloud, or community cloud as well as one or more of the following services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), or platform-as-a-service (PaaS).

Cloud computing gives businesses the flexibility to adapt to their market and launch an initiative or program without buying and maintaining expensive IT capacity. Another consideration for cloud computing is being able to trade huge capital purchases for a pay-for-use model.

2 – IT Outsourcing Life Cycle: Risk and Control Considerations

For the User Entity

This chapter addresses the risk and stages followed by the user entity's management that outsources a task or function. The move to outsource can result from strategic or tactical business planning considerations. However, before making the commitment to outsource, management should establish clear ownership, business objectives, and alignment with strategic plans. The decision to outsource should be supported by a business case that assesses the return on investment and the underlying risks to realizing projected benefits, including the risk of implementing and transitioning operations. Too often, the risks of outsourcing are not considered fully and quantified transparently.

This section focuses on the outsourcing life cycle, the process supporting the decision to outsource, and the major activities performed in phases by management. Life cycle phases include:

- Considering strategic fit and sourcing evaluation.
- Decision-making process and business case.
- Tendering process and contracting.
- Implementation and transition.
- Monitoring and reporting.
- Renegotiation.
- Reversibility.

At the end of this chapter, please refer to Table 1, which details associated risks by stage and potential auditor involvement based on those risks.

Strategic Fit and Sourcing Evaluation

Understand the business context and drivers that determine the strategic fit for the service provider to play:

- Are organizational strategies the main drivers of IT outsourcing considerations? Or is outsourcing an IT strategy to promote innovation and enable the business to find breakthrough solutions leveraging IT capabilities in the market (i.e., not available through internal development alone)? The nature of the outsourcing strategy — organization-led or IT-led — may demand different governance considerations and impact how accountability is established and tracked.
- Understand the key drivers:
  – Cost reduction via economies of scale enabled by the service provider.
  – Improved effectiveness of process by leveraging the service provider's expertise and investment in solutions.
  – People/skill level challenges as IT expertise may be difficult to sustain and manage internally.
- What options are available in the market?
- What is the capability maturity level of the user entity as well as its actual past experiences with IT outsourcing?
- Is the organization ready to be a proof of concept or first to market, or is that too risky?
- Is the number of service providers, or "vendor survival" rate, adequate to avoid dependence on a sole provider?
- Is the process too strategically important to outsource? Certain IT activities may be a critical competitive advantage for some organizations.
- Have modeling and business process mapping needs been developed to build a baseline, define scope, and benchmark?
- Who should sponsor the analysis, own the relationship, and be involved in business case development?

Internal audit considerations:

- 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.

Decision-making Process – Business Case

The outsourcing option should make business sense in the long term and create value based on reliable information and projections (i.e., risks should be understood):

- Build a sound business case, addressing key benefits and risks. Outsourcing may be a solution to address business risks, or it may create new business risks, but evaluations also should include implementation risks and probable impacts if the outsourcing deal fails.
- Ensure the sponsor and major stakeholders are involved and considered in the final decision.
- Consider other options or variations. The optimal solution should be chosen; there is more to the decision than just whether or not to outsource.
- Respect internal governance mandates. The final risk level accepted should align with the entity's risk appetite.

- Consider management-of-change requirements. How does one create an environment inside an organization to enable an outsourcing environment (e.g., change of policies, operational procedures, and infrastructure support)?

Internal audit considerations:

- 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.
- 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.

Tender Process and Contracting

Conduct request for proposals, vendor selection, and structure a deal in line with the business case:

- Develop a detailed scope of work so providers can make informed bids and highlight other relevant matters.
- Evaluate bids based on relevant criteria as generally used in business cases or specific considerations needed.
- Detail any new risks arising or any significant deviations from the approved business case.
- Select provider based on criteria and bids/proposals submitted.
- Staff an experienced team to perform an operational due diligence review and ensure key performance indicators — service level agreements (SLAs) and operational level agreements (OLAs) — are addressed in the contract.
- Assess potential losses, breakdowns, and non-performance results. Determine tolerance thresholds and what will happen (recourse) when deviations occur.
- Obtain sign-off by sponsor and inform key stakeholders, highlighting any deviations or new risks. Include legal compliance reviews and necessary legal steps to finalize a binding agreement (including exit strategies and plans if terminated or not renewed).

Internal audit considerations:

- 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.
- 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.

Implementation/Transition

Develop a transition plan, secure necessary funding, and formalize program/project management sponsorship, support, and other resources:

- Formalize plans and set governance expectations for any outsourcing of a significant process or operation. Consider incorporating a schedule on governance in the contract, budget for it in the business case, and schedule/build contract compliance audits.
- Determine fundamental timing, funding, deliverable dates, testing, and ongoing monitoring.
- Address human resource issues and cultural adjustments as critical success factors before, during, and after transitions.
- Obtain service provider resource accreditation. How does one ensure operationally and contractually that service provider resources are qualified to perform the job?

- Manage expectations regarding deviations and non-delivery, on either side, to contain the cost of unplanned disruption to operations.
- Standardize processes before transition. This may take substantial effort and investment.
- Perform a post-implementation analysis and work relevant issues into the monitoring and reporting phase (or issues to be considered upon renegotiation). Attain assurance that the transition was executed in accordance with the agreement and business case.

Internal audit considerations:

- 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.

Monitoring & Reporting

After transition, monitor operations to ensure they are delivering business requirements as defined by business requirements, key performance indicators (KPIs), and SLAs. This phase ensures that operations and monitoring of performance are optimized and reinforces improvements in the process and the outsourced relationship:

- Establish and evolve key performance measures. It is better that these are considered and designed as part of the contract phase and SLAs; however, all may not be anticipated. Ideally, metrics should ensure delivery of requisite service and indicate general compliance or non-compliance.
- Receive other sources of ongoing assurance that operations are controlled and maintain integrity (e.g., SSAE 16, ISAE 3402, quality assurance or compliance reports on operations, or reports from independent or internal audits). Consider building in ongoing or periodic evaluations of contract compliance.
- Monitor the nature, cause, and response by providers to performance and contractual issues. Ensure that this knowledge is shared and leads to improved delivery or more demanding renegotiations. Manage the current and future relationships with improved knowledge.
- Look for innovation from the service provider to give visibility into risk and improve business enablement.

Internal audit considerations:

- 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.

Renegotiation

As the contracted term nears completion, understand the actual benefits and problems, changes in the market and benchmarks, and costs of taking back the process or going to another supplier as part of renegotiations. Ensure that problem and incident reporting is leveraged effectively.

- Compare steady state operations to the original business case and validate lessons learned.
- Benchmark with other service providers.
- Explore market alternatives and current benefits versus bringing the process back in-house.
- Perform a new risk, cost, and benefit analysis/assessment.
- Pursue more effective terms. To maintain leverage, the organization should have alternatives and understand its options (see also Reversibility in the next section).

Internal audit considerations:

- 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.

Reversibility

Understand the costs and disruptions that may result from moving operations either to another service provider or back in-house.

- Estimate the likelihood that the outsourcing arrangement will fail — many do historically.
- Determine the total cost and impact if operations had to come back in-house and determine a "probable cost" (likelihood times cost) of this happening either during or at the end of the term. Factor that into the return on investment (ROI) analysis in the business case, the original contract and upon renegotiation.
- Understand other options and partial reversibility scenarios.
- Anticipate contract elements that would prevent the organization from being locked into a relationship to the extent that the provider could increase charges without recourse. Build into the agreement information on how much can be charged based on market conditions and economic factors, such as inflation, to the extent possible.

Internal audit considerations:

- 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.
- 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.

Table 1: IT Outsourcing Life Cycle: Risks and Auditor Involvement by Stages

This table details risks to be considered during the outsourcing decision-making process. The roles and responsibilities are emphasized within the user entity to mitigate the risks and establish the related controls necessary. Associated risks with major activities and potential areas of focus are highlighted for the internal auditor — these vary substantially based on the maturity of the organization and management (their experience with outsourcing operations), as well as the involvement of risk management, project management offices, and other assurance functions. The CAE should understand board[1] and key stakeholder expectations, but he or she should not be viewed as part of the approval process to maintain ongoing independence from management's strategic/operational decisions.

Stages	Objectives	Key Activities	Manager Roles *[2]	Risks	Auditor Involvement[3]
A: Strategic Fit and Sourcing Evaluation	Identify sourcing options and baseline the scope.	■ Map business model processes. ■ Prioritize options based on benefits and risks. ■ Develop market analysis and benchmarks.	Process owner,* procurement experts (technical, risk, BCP, and corporate strategy), business unit management, and executive sponsor.	■ Not aligned to organizational strategies. ■ Bad decision. ■ Loss of assets or lower ROI.	Understand strategic context and whether supporting information is reliable and complete, as deemed necessary.

[1] As defined in the *Standards* glossary, "A board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report."

[2] The * indicates primary responsibility and typical owner of stage.

[3] Internal auditor involvement will vary depending on risks, stakeholders' and board's expectations, management's capabilities, and the involvement of other assurance functions and available expertise.

Stages	Objectives	Key Activities	Manager Roles *[2]	Risks	Auditor Involvement[3]
B: Decision-making Process – Business Case	Build a reliable business case.	■ Conduct detailed business risk and benefit analysis. ■ Factor in execution risks and failure impact. ■ Select best option and detail cost/benefits. ■ Identify relationship between strategy and governance.	Process owner,* executive sponsor,* finance, legal, IT, human resources, and other experts.	■ Optimal supplier not selected. ■ Loss of assets, ROI, or reputational damage as quality of services may be diminished. ■ Negative regulatory impact.	■ Assess whether information in detailed analysis is reliable and consider all business risks and implementation risk. ■ Determine whether governance and approval is transparent and reliable. ■ Determine whether the right parties and experts are assigned. Assess whether major stakeholders are kept informed.

Stages	Objectives	Key Activities	Manager Roles *	Risks	Auditor Involvement
C: Tender Process and Contracting	Select a provider and design a contract that promotes success.	■ Detail requirements, scope, and requests for proposals. ■ Select provider and perform due diligence. ■ Negotiate contract. ■ Develop exit plan.	Process owner,* procurement,* project team, executive sponsor, legal, and finance.	■ Deal is not optimized or organization is not protected from gaps in delivery of quality, availability, and integrity/privacy needs. ■ Loss of assets, ROI, and reputational damage. ■ Impact on regulatory needs.	■ Determine whether there is an appropriate approval and procurement process. ■ Review contract and control assurance needs from provider (e.g., need for SSAE 16 or other available Statement on Audit Standards (SAS) 70-type assurance reports from provider) and assess whether the organization has drafted its right to audit clause effectively. ■ Determine whether the project team has appropriate skills. Ask whether risk management, legal, HR, and finance are involved as needed. ■ Perform due diligence reviews, or assess management's review of the provider.

*Primary responsibility and typical owner of stage.

Stages	Objectives	Key Activities	Manager Roles *[2]	Risks	Auditor Involvement[3]
D: Implementation and Transition	Execute transition as planned. Initiate new operations	■ Roll out transition plan. ■ Transfer/manage resources. ■ Transform process.	Project team,* process owner,* executive sponsor, finance, HR, and risk.	■ Loss of assets and ROI due to inefficiency and unmanaged risks. ■ Interruption of service and customer impacts. ■ Operational quality is less than projected.	■ Conduct pre-implementation review to determine if project is following standard disciplines. ■ Review contingency plans if transition is not properly effected. ■ Determine whether risks and actions are identified, mitigated, and escalated appropriately to stakeholders as part of project governance and execution.

Stages	Objectives	Key Activities	Manager Roles *	Risks	Auditor Involvement
E: Monitoring and Reporting	Oversee and control the outsourced operation.	■ Manage relationship. ■ Assess results and performance. ■ Design ongoing reporting and process improvement model.	Process owner,* retained team, project sponsor, finance, HR, risk, and other experts.	■ Relationship and deliverables devolve with customer damage and loss of assets and ROI. ■ Process is not sustained and is not optimized as planned.	■ Determine how provider performance and compliance to the contract will be assessed and routinely reviewed by management. ■ Ask what metrics and other key performance indicators are used. ■ Ask how concerns and areas for improvement are communicated and leveraged to improve current and future operations/ contracts.

Stages	Objectives	Key Activities	Manager Roles *	Risks	Auditor Involvement
F: Renegotiation	Ensure the renewed relationship evolves and improves.	■ Gather all operational, cost, quality, and relationship issues. ■ Benchmark and review current market studies. ■ Establish new targets to improve contract.	Process owner* procurement,* executive sponsor, legal, finance, and other experts.	■ Optimization is reached with resulting loss in ROI and future operational quality. ■ Better alternatives are not found or cost increases are not justified.	■ Identify the strategies and information used and needed to ensure optimal future negotiations. ■ Understand reversibility and monitoring or performance results. Determine whether experts and process owners are driving renegotiation improvements.

*Primary responsibility and typical owner of stage.

Stages	Objectives	Key Activities	Manager Roles *[2]	Risks	Auditor Involvement[3]
G: Reversibility	Ensure that the arrangement can be unwound and considered in business case/ strategy.	■ Make decision to bring back in-house and identify the impact of doing so. ■ Determine how to change vendor. ■ Identify business case impact.	Process owner,* procurement, executive sponsor, risk, BCP, and other experts.	■ Inability to react to adverse situations or other opportunities. ■ Lack of leverage in future negotiations. ■ Loss of assets and interruption of services if brought back in-house or to another provider. ■ Unanticipated costs if outsourcing fails.	■ Determine the contingency plans if arrangement does not work; what are the estimated costs and likelihood. ■ Ask whether the costs and likelihood have been considered in the business case and ROI needs. ■ Ask whether other providers are able to be used effectively. Ask about the provider's viability. ■ Determine whether the trigger points to initiate or consider changes in provider are understood and pre-defined. ■ Find out whether other risks have been considered that might drive the need for bringing operations back in-house and whether these have been assessed, including macroeconomic and political/ geographic concerns. ■ Ask whether the provider has sound BCP capabilities. ■ Determine whether the vendor's BCP efforts are sustainable. ■ Assess how the contract addresses the need to exit.

*Primary responsibility and typical owner of stage.

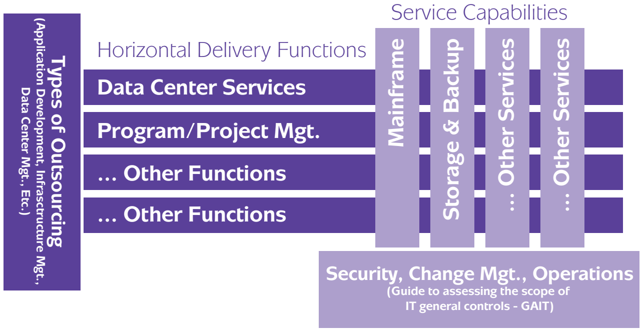
3 – IT Outsourcing Delivery: Risk and Control Considerations

For the Service Organization

This chapter addresses risk in connection with IT outsourcing (ITO) delivery performed by the service provider for other entities. In accordance with the SLA negotiated with the user entity, the service provider is expected to conduct IT control activities commensurate with IT risk. To develop a suitable audit approach, the CAE should start by gaining an understanding of the ITO delivery landscape and architecture. Then, the CAE should consider the service delivery risk and the controls designed to meet the risk, and determine a fitting ITO assurance method.

Understanding the ITO Delivery Landscape

Typically, services are organized and delivered by capability, or a group of capabilities, which is referred to as a function. A service capability is a defined set of competencies — a combination of skills, processes, tools, technologies, and experiences — required to deliver projects and services (e.g., mainframe services, midrange computing, and storage and backup services). Functions are horizontal processes, and operational functions that span across service capabilities provide integration of processes, tools, and outcomes across multiple service capabilities (e.g., data center services and program/project management).


Types of Outsourcing
(Application Development, Infrastructure Mgt., Data Center Mgt., Etc.)
Horizontal Delivery Functions
Service Capabilities
Data Center Services
Program/Project Mgt.
... Other Functions
... Other Functions
Mainframe
Storage & Backup
... Other Services
... Other Services
Security, Change Mgt., Operations
(Guide to assessing the scope of IT general controls - GAIT)

Given the foundational concepts identified above, it is important to understand the functions in the following framework. By relating service capabilities to the fundamental principles of security, change management, and operations, the internal auditor can better scope risk and assertions relevant to the business process. IIA Professional Guidance, Guide to the Assessment of IT General Controls for Business and IT Risk (GAIT–R), further identifies the critical IT aspects that are essential to managing and mitigating business risk.

As noted previously in chapter 2, horizontal delivery functions generally include:

- Application development and management.
- Infrastructure management.
- Help desk.
- Independent testing and validation services.
- Data center management.
- Systems integration.
- R&D.
- Managed security.
- Cloud computing (e.g., SaaS, IaaS, PaaS).

Organizations have numerous options when considering outsourcing capabilities and functions:

- Combining outsourcing services with internal IT functions (sometimes called in-sourcing or cosourcing).
- Completely outsourcing a capability or function while keeping others in house.
- Outsourcing everything to vendors that will manage the technology resources on-site (including machines, networks, and people).
- Outsourcing everything to vendors that will "rent" hardware, software, and communications to the organization through a "X-as-a-service" model.

Regardless of what technology is outsourced or which outsourcing model an organization chooses, there are common process areas, key risk areas, controls, and audit objectives that should be understood by the user entity and service provider. The IIA's GAIT document provides a suitable approach for organizing horizontal delivery functions by process category — security, change management, and operations — to assess the extent of risk and ensure key controls are tested across the various service capabilities.

Key ITO Architecture Domains

This section identifies and defines the IT layers or domains that constitute the ITO architecture. These are the IT technical areas and general oversight structures that provide the foundation on which the IT services functions and capabilities are built and managed.

1. **Organization:** An important element of successful delivery of services in an ITO arrangement is the service provider's organization and profile. The organization should be well-positioned to retain the right people with the right skills in the right roles. Consider the provider's customer satisfaction index. Do the provider's customers perceive it to be effective? When was the last time it conducted a skills-gap analysis? These types of questions are

important for the user entity to evaluate whether it has contracted the right service provider and for the provider to measure whether it is best positioned to meet customer expectations.

2. **Operating System:** An operating system (OS) is software that runs on computers, manages computer hardware resources, and provides common services for executing various application software programs. The OS acts as an intermediary between application programs and the computer hardware. Additionally, the OS provides:
   - System tools (programs) used to monitor computer performance, debug problems, or maintain parts of the system.
   - A set of libraries or functions that programs may use to perform specific tasks especially relating to interfacing with computer system components.

   Operating systems are often an avenue of attack, especially when critical patches or updates are missing. As a result, performance and availability issues could begin to surface, or the system could suffer unauthorized access and disclosure of sensitive or proprietary data.
3. **Network:** Outside the Internet and intranet, and the need for connectivity, the network is constantly adjusting to new business models and service offerings such as business-to-customer (B2C) and business-to-business (B2B) transaction processing, business-to-government (B2G) transactions, e-learning, collaborative customer service, and real-time, rich media-based teleconferencing. Increasing numbers of employees are working from home, from the road, or in virtual spaces where they are connected constantly. The pressure to provide reliable, secure, cost-effective communications is unprecedented and will continue to grow. The Web, which sits outside corporate firewalls, is emerging as a virtual operating system and is becoming the preferred platform for more and more organizations.
4. **Database:** Data lies at the heart of all business models. “Operational data,” especially if it is in different forms, often should get translated into a form where it can be used by many people in the organization. Safeguarding substantial amounts of sensitive and confidential data, personal information, intellectual property, and trade secrets from malicious attacks and accidental loss is one of the biggest challenges for IT management. Strategically, the trend has been to place more value on unstructured data and less emphasis on traditional hierarchical file systems, which were never designed to operate at today’s scale.
5. **Application:** Application architectures consist of integrated and interoperable back-office, front-office, virtual-office, desktop, laptop, personal digital assistants, and other thin-client applications that support the current and to-be business strategy. Applications should be standardized to support activities, processes, employees, customers, suppliers, and partners regardless of where they sit physically or how mobile they are. Most large and mid-sized organizations have large enterprise applications such as ERP and customer relationship management (CRM) systems. There also are proprietary applications and Internet or Web-facing applications that interface with customers, suppliers, and partners. Finally, there are applications that help organizations manage their applications and the computing and communications infrastructure (e.g., network and systems management applications).
6. **Metrics & Reporting:** The SLA is one of the primary metrics used to measure performance, and it can provide management with the evidence to support the evaluation of the customer/supplier relationship. An OLA supports the SLA and provides specific process goals to achieve the SLA. Organizations in IT outsourcing relationships should have an ongoing monitoring process to ensure the service provider’s performance is aligned with the outsourcing contract. KPIs and key risk indicators (KRIs) should be established to help the client and the service provider meet their business objectives.
7. **Program/Project Management:** In achieving its particular purpose, a project will have a discreet beginning and end, undertaken within defined constraints of scope, quality, and cost. Projects will vary in size and scope and could include building new infrastructure, new product development, and the implementation of new business processes or business transformations. In the evaluation of such projects at various stages, it is necessary to understand the key risks and to develop a set of key criteria.

Key ITO Service Delivery Risk Areas

This section outlines the common ITO risks related to the IT service delivery architecture. Fundamental to outsourcing is accepting that although service delivery (operational responsibility) is transferred to the service provider, the user entity retains responsibility for the management of and adherence to policies, procedures, and regulatory requirements. This is ITO risk. To manage this risk, the user entity should have an effective outsourcing oversight program with a framework for management to identify, measure, monitor, and control the process area risks associated with outsourcing. The risk associated with an outsourced IT service is subject to the process outsourced, the relationship with service provider, and the technology used by the service provider.

Failure by the service provider to implement appropriate controls, assurance, and ongoing monitoring related to the outsourced service may result in:

- Poor service quality with an unacceptable number of failures and errors.
- Service disruption and failure to meet the organization's client obligations.
- Privacy and confidentiality issues.
- Slow response, reduced system availability, questionable integrity of information, and compromised security and confidentiality.
- Service provider technology and system architecture issues related to scalability, capacity, and performance.
- Inability to maintain appropriate internal operational and IT controls and meet regulatory and industry requirements such as the European Union Data Protection Directive (EU DPD), the U.S. Graham-Leach-Bliley Act (GLBA), U.S. Health Insurance Portability and Accountability Act (HIPAA), International Financial Reporting Standards (IFRS), King III Report on Governance, and the U.S. Sarbanes-Oxley (SOX) Act of 2002, and Payment Card Industry (PCI).
- Poor disaster recovery and business continuity capabilities.
- User entity expenditure and effort to find an alternative service provider or to bring the outsourced service back in house.

ITO risks can be identified and prioritized from the user entity's and the service provider's perspective and grouped into three categories:

- Mixed ITO risks (specific to both the client and supplier).
- Client-specific ITO risks.
- Supplier-specific ITO risks.

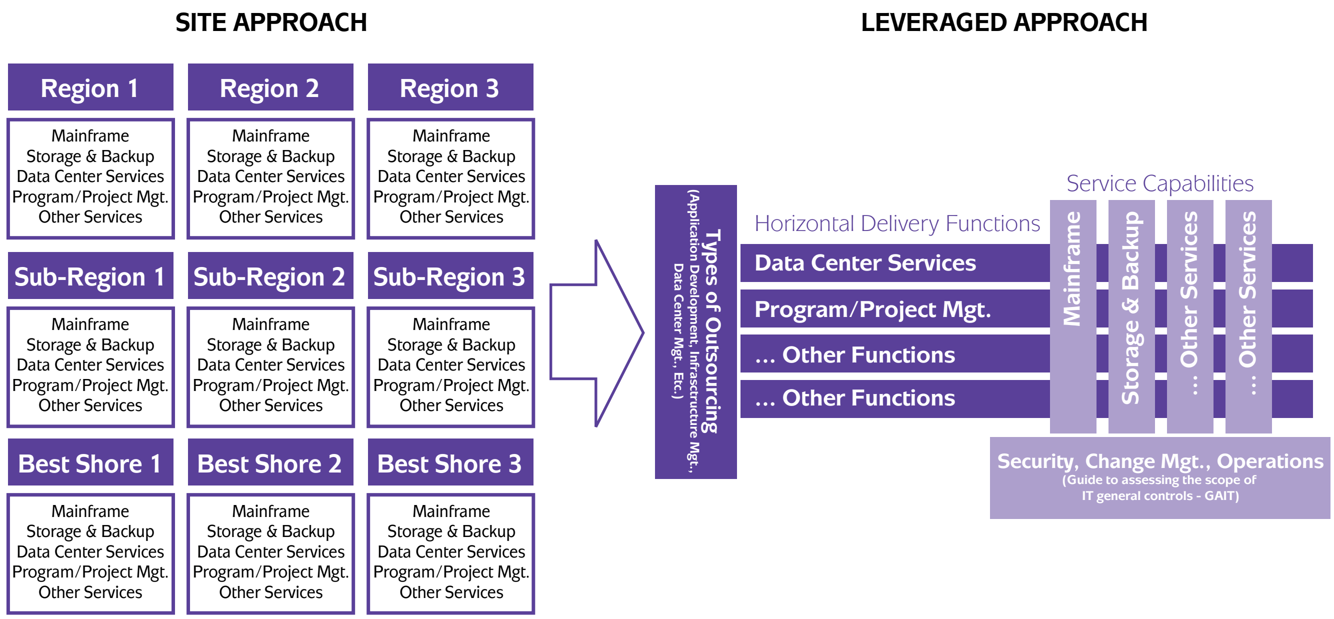
Areas of shared interest should rank high in an ITO audit risk assessment.

Table 2: ITO Risk Influence Matrix (example)

Risk Category	ITO Risks
Mixed	Conflict between the parties due to violation of contractual terms.
Client-specific	Provider's lack of compliance with the contract.
Client-specific	Unexpected increase in outsourcing costs.
Client-specific	Loss of data privacy.
Supplier-specific	Inadequate staffing.

Service Delivery Governance Risks (methodology, model, contract)

When assessing risk in the outsourcing environment, the user entity should consider the ITO governance model used by the service provider. In the old model (still used), a single capability is managed through a silo, usually by location, in which different teams use different processes and tools. In contrast, the new model focuses on fewer accountable leaders by capability, is globally integrated, is automated, and drives consistent processes across the service capabilities.



In either model, a well-defined, comprehensive contract will enable the management of risk for the user entity and the service provider. Non-technical risks to outsourcing success are best managed through a well-defined governance model and strong contract terms supporting a relationship built on the principles of service delivery excellence.

Table 3: Shared Governance Risks (example)

Risk	Definition and Mitigation
Service provider failing to meet the terms of the SLA.	Includes underperformance or poor quality of deliverables. The user entity can monitor performance of providers, escalate underperformance, and use penalty clauses in contracts, if necessary. The providers also can monitor SLAs and change delivery processes to meet them. Even after changing processes, if the SLAs are consistently difficult to meet, the providers can inform the user entity and, if required, renegotiate these SLAs.
Inadequate skill/knowledge level of the project resources of the IT service providers.	Skilled resources are key to the success of IT projects. User entities can mitigate this risk by clearly defining eligibility criteria for particular roles. Providers can mitigate this risk by maintaining sufficient expertise, ensuring retention of skilled resources, and maintaining resource pools for important clients.
Communication gaps between user entity and providers; unclear communication/escalation paths.	User entities and providers can mitigate this risk jointly by defining a clear management structure/communication path for outsourced projects, and including a communication plan in project plans. User entities and providers together can define response times for clarifications. Finally, both parties should align their objectives, processes, and time lines and regularly review status versus plan.

IT General Control Risks (GAIT: Security, Change Management, Operations)

In an ITO arrangement, IT general controls are critical to delivering quality service and protecting a client's business data. GAIT provides a risk-based approach to assessing the scope of IT general controls and ensuring that key controls are tested across the various infrastructure layers (e.g., application, database, operating system, and network infrastructure).

Security

Security is the foundation of the ITO model and is fundamental for protecting the user entity's assets (e.g., hardware, software, and data). The contract should explicitly identify which security policies and standards govern the ITO arrangement — the user entity's or the service provider's — and should address data access, applications access, network access, software, privacy, and BCP. Additionally, organizations should understand:

- Firewall technology.
- Antivirus technology.

- Certificate authority technology.
- Biometric technology.
- Data loss protection.
- Regulatory requirements (e.g., EU DPD, HIPAA, IFRS, King III, etc.).
- PCI standards.
- Encryption technology.
- Privacy-compliance technology.
- Authentication methods.
- Directory structures.
- Vulnerability and threat management.

Data Protection

It is difficult to protect confidential, personal, and other sensitive information when it is obtained and processed by service providers, which may not be bound by the same laws and regulations as their clients. Of all the aspects of outsourcing, information protection often is the most critical. It is especially crucial in government sectors such as law enforcement and defense, where secrecy is paramount, and in financial services and healthcare, which are often targets of malicious attacks.

Complications arise when different laws and regulations govern the user entity and service provider, particularly when they are located in different regions or countries, or in different jurisdictions within the same country. Organizations in heavily regulated sectors should make extraordinary efforts to ensure that their service providers comply on their behalf with relevant laws and regulations.

Security and data protection processes ensure that access to applications and data is authorized and assets are safeguarded appropriately. Addressing risk in connection with invalid assets, fictitious transactions, or unauthorized disclosure of sensitive information, security controls relate directly to management's assertion regarding the existence and occurrence of assets and transactions.

Change Control

In the ITO arrangement, changes will occur as part of the initial transition and transformation when a service relationship is initiated, or through other transformation projects conducted throughout the life of the contract (see the Project Management section of this chapter for details about related risks and recommended controls to be included in an ITO audit).

Change control processes are foundational to ensure the accuracy of the application software. To address risk that financial information is recorded incorrectly or in the wrong time period, the logic in the application system should be documented, tested, and authorized. Change controls therefore relate directly to management's assertion of valuation or measurement.

Operations

Operations management is defined as the process of operating or running applications and systems. This process typically includes controls to ensure applications run as intended, processing errors and exceptions are resolved in a timely manner, critical application data or system files are backed up, and physical security and other aspects of data center operations are performed.

The risk that the system is unavailable or insufficiently operational is met by operational controls. Operational problems can cause programs to run out of sequence, resulting in out-of-balance conditions. Operational processes ensure that information is complete and delivered timely to decision-makers. Control activities guard against unexpected interruptions or introducing errors while restoring service. Operations management relates directly to management's assertion of completeness — that actual transactions are not omitted, duplicated inadvertently, or accumulated incompletely.

Incident and Problem Management

Incident and problem management are best defined in relation to each other. Incident management is concerned with "firefighting" such as resolving service outages or other incidents quickly. Problem management is concerned with "fire prevention" by identifying problems and implementing solutions to eliminate their root causes. The primary focus of the incident management process should be to restore service as quickly as possible. Customer incidents should be prioritized, coordinated, and resolved through a service desk.

Data Quality

Data is good only if all links in the end-to-end transaction-processing chain are solid and strong. Transaction accuracy and completeness are critical to the business. Although the user entity will own the data, the service provider is accountable for providing or managing the IT environment where many control processes exist that may affect the quality of that data. Data quality is at risk at any link in the end-to-end data chain, whether it is at the point at which data is entered into a source system, during transfer from one system to another, or during the extract, transform, and load (ETL) processing.

Data Center Operations

Whether providing dedicated data center services or ITO services through a leveraged or centralized environment, data center (DC) operations are likely to have the highest inherent risk factor in the ITO arrangement. The risks span the portfolio of DC services and standard operational areas, which include:

- Managed mainframe services.
- Backup and storage services.
- Web hosting services.
- Server management services.
- Cloud services.
- DC modernization services.
- Physical security.
- Facility environmental controls.
- Security compliance monitoring.
- Asset management.

GAIT assists in the identification and assessment of inherent IT risk, which should be mapped to business risk — IT risk is a subset of business risk. The information-processing objectives relate to business-processing control activities referenced in The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Internal Control–Integrated Framework. By deliberately aligning GAIT control activities to information-processing objectives, the CAE can drive an integrated, optimized approach for assessing IT delivery risk.

Project Management Risks

Failed or challenged projects can have a significant impact on an organization, depending on the business need behind the project. Examples of possible impacts include:

- Disruption of service to customers.
- Loss of competitive advantage.
- Fines from failed regulatory compliance.
- Loss of revenue.
- Negative impact on reputation.
- Delays in deploying critical strategic initiatives, products, or processes.
- Loss of expected ROI.
- Facility closure or damage.

Ultimately, management is accountable for ensuring that the project and benefit outcomes are achieved, even though the service provider may be penalized for failures within the project. A review of project-related risks can contribute to the success of the project. The sooner a project is reviewed the better; reviews performed during the early phases of the project can be the most valuable because they can identify issues that can be fixed relatively inexpensively compared to issues found later in the project or post-implementation.

Key ITO Service Delivery Control Categories

The broad areas of IT service delivery are diverse and vary from organization to organization. These areas span service capabilities (e.g., midrange server environment and utility/cloud) and service delivery functions (e.g., DC operations and ITO support). Organizing controls into manageable categories will enable management to determine an assurance method and obtain a comprehensive view of risk.

As noted, GAIT does not identify specific key controls. It identifies the IT general control (ITGC) processes and related IT control objectives for which key controls need to be identified and should be leveraged during the risk assessment process. Other tools, such as the Control Objectives for Information and Related Technology (COBIT) or the Information Technology Infrastructure Library (ITIL), can be used to identify and then assess specific IT key controls.

ITIL, developed by the UK Office of Government Commerce, is one of the most widely accepted reference frameworks for IT service management, providing a cohesive set of best practices, drawn from the public and private sectors. Many organizations have already modeled their service delivery on this framework. A service delivery audit based on the ITIL approach can provide IT management with valuable inputs based on a well-thought-out global standard for improving IT service management and delivery.

Components of IT Service Management

Understanding the operational architectural environment related to IT service delivery is critical to the user entity and the service provider. Quality of service and the relationship between the user entity and the service provider should be the primary focus of any review.

Configuration and Change Management

Within configuration management, components of infrastructure and services are referred to as configuration items (CIs), which are maintained in a database referred to as the configuration management database (CMDB). This is more than just an asset register; it contains information that relates to the maintenance, movement, and problems experienced with the configuration items, along with any relationships between CIs and their associated supporting data elements (e.g., people and organizations). A CMDB can be a single physical database or comprise multiple physical databases.

A well-maintained CMDB should be able to:

- Provide accurate CI data (including dependencies and relationships) to other ITIL and operational processes in a central logical database.
- Account for all CIs and their controlled attributes.
- Verify that data supports an organization's IT, financial, legal, and security obligations.
- Validate actual CI data stored in the CMDB against the authorized (via change management) and discovered (via inventory/discovery tools) states through verification, compliance, and audit checks.

Change management is the practice of ensuring that all changes to configuration items are carried out in a planned and authorized manner. This includes ensuring that there is a business or technology reason behind each change, identifying the specific configuration items and IT services affected by the change, obtaining proper authorizations for the change from the appropriate business and technical experts, planning the change, testing the change, and having a back-out plan should the change result in an unexpected state of the configuration item. A change is any modification to the managed IT environment, including the addition, removal, or replacement of any component (CI) or service in that environment.

Capacity Management and Service Continuity

As the business grows, demands on IT systems increase, and the capacity of networks, storage, computing, and support should keep pace with the increasing demands. An ITO audit should validate that a process exists to ensure that the monitoring of capacities and planning for future capacities are done with participation of the business well in advance, and that plans are reviewed periodically. Good capacity management ensures that the quality of service is continued at all times.

Continuity management ensures critical business operations can continue in the event of a service interruption or disaster. The details of the continuity plan are documented in business continuity and disaster recovery plans and should ensure that the scope of the continuity plan contains clear and realistic recovery objectives and recovery time frames, is designed and developed to support recovery of critical business functions, and is reviewed, updated, and rehearsed regularly.

SLA Management

The SLA is the backbone of the service contract and should be clearly measurable. All statistics relating to SLAs should be system-generated and tamper-proof. The ITO audit should verify whether SLA reports are submitted to the appropriate levels of management and meaningful reviews are conducted. SLA management also includes the documentation, handling, monitoring, and management of customer complaints, compliments, and feedback.

Additionally, the following practices should be evaluated in the ITO audit. All service level targets should be:

- Clear and unambiguous.
- Agreed upon and approved by the client and the service provider.
- Measurable.

All targets within OLAs or underpinning contracts (UCs) should be aligned with the SLA.

Incident and Problem Management

Incident management processes should record impacts of all incidents in clearly quantifiable terms, including the number of users affected, staff hours lost, complexity, impact on business revenues, and impact on regulatory compliance. An audit should examine all incident reports and check whether they were resolved satisfactorily, the root cause analysis was performed, and preventive actions were taken to avoid recurrence of the problem.

The critical success factors for the incident management process are:

- Centralized incident management data.
- Access to CMDB information.
- Performance indicators.
- Clear case ownership.
- Management of case dispatches.
- Standard incident categorization.
- Access to SLAs.

The problem management process should contain the following procedures:

- Problem identification and classification.
- Problem investigation and diagnosis.
- Error assessment.
- Problem/error closure.
- Status/update communications.

Program/Project Management

A project review as part of an ITO audit should focus on five key areas (see GTAG *12: Auditing IT Projects*):

- Business and IT alignment.
- Project management.
- IT solution readiness.
- Change management.
- Post-implementation.

The project review should build controls around the following success factors:

1. **User Involvement –** Business and IT users are involved with decision-making and information-gathering processes.
2. **Executive Support –** Key executives provide alignment with business strategy and financial and conflict resolution support.
3. **Clear Business Objectives –** Stakeholders understand the core value of the project and how it aligns with business strategy.
4. **Agile Optimization –** Using iterative development and optimization processes to avoid unnecessary features and ensure critical features are included.
5. **Project Management Expertise –** Using project managers who understand the basic skills and practices, such as a certified Project Management Professional from the Project Management Institute.
6. **Financial Management –** The ability to manage financial resources, assess risk, and demonstrate the value of the project.
7. **Skilled Resources –** Acquire, manage, and control skilled project personnel to move forward in the face of turnover and other personnel hurdles.
8. **Formal Methodology –** The predefined set of process-based techniques that provide a road map for when, how, and what events should occur in what order.
9. **Tools and Infrastructure –** Building and managing the project infrastructure with tools that enable management of tasks, resources, requirements, changes, risks, vendors, and quality management.

Table 4: Project Control Considerations by Stage (example)

Project Stage	Control Considerations
Design and Development	■ A clear and robust business case. ■ Realistic and comprehensive assessments of costs and benefits. ■ Involvement of all key stakeholders at an early stage. ■ Thorough consideration of security and integrity controls.
Project Management	■ Proactive leadership and real-time reporting. ■ Involvement of all key stakeholders. ■ Issue identification and escalation. ■ Realistic time scales and clear targets. ■ Rigorous testing and piloting before going live.
Implementation	■ Management of change and training. ■ Regular and reliable tracking of benefits. ■ Ongoing customer satisfaction assessments.

ITO Service Delivery Assurance Methods

This section outlines the various methods management should use to gain assurance over the risks related to ITO. Managing ITO risk is something that should be done by the service provider and the user entity and will be much more successful when there is a strong relationship between the two. Service providers that do not value the need to obtain and give assurance through auditing and monitoring would be at a distinct competitive disadvantage to providers that understand the customer's need for assurance.

The Internal Auditor's Role in Service Delivery

An organization is unlikely to meet its objectives without effective service delivery mechanisms. Internal auditors have a unique insight and are well-placed to assess the policies, procedures, and operations in place to monitor the achievement of the organization's objectives and to identify and manage the risks to them.

The internal auditor may:

- Provide assurance by reviewing management's systems for identifying and effectively managing the risks to service delivery.
- Provide assurance by frequently carrying out comprehensive reviews of the management of service delivery.
- Provide assurance by reviewing performance reporting systems and the systems used to track and manage the attainment of targets.

- Gain assurance by relying on the other assurance providers.
- Play a more proactive advisory role across various aspects of the whole service delivery process — for example, by being involved early in the design of systems to ensure that the user entity's needs are identified, or by tracking management action.

The ITO Audit

The outsourcing process exposes clients and service providers to a series of risks that can seriously affect their activities. Managing these risks by improving the quality and efficiency of internal control has made the ITO audit a necessary component for all the organizations involved in this process. At the organizational level, the ITO audit can be included not only internally, but also in the external audit process. Moreover, the ITO audit can be extended from the user entity to the service provider through mutual collaboration. Alternative audit approaches, such as walk-throughs and continuous monitoring, can enhance the collaboration between service provider and client and elevate the level of assurance obtained through auditing.

ISAE 3402/SSAE 16

ISAE 3402 has become a widely recognized standard and indicates that a service provider has had its control objectives and activities examined by an independent accounting and audit firm. Third-party reports on internal controls in service organizations describe the control processes in services performed by a service provider. Such reports give users information to assess and address the risks associated with an outsourced service. If a service provider has an ISAE 3402 review conducted, it has greater credibility essential to meet the accounting and regulatory compliance needs of customers. Service-provider audits are necessary to a user entity's ability to assert that it has appropriate audit and control procedures to manage its business under Section 404(b) of Sarbanes-Oxley Act.

The Standards

International Standards: In December 2009, the IAASB adopted ISAE 3402 as an "attest" procedure for assessing service organizations' compliance with IT and process controls. An attestation involves an audit professional's assertion about subject matter other than the fairness of the presentation of financial statements. An attestation may be less rigorous than an audit. Service auditor reports might still survive by special request from enterprise customers.

U.S. Standards: In April 2010, the AICPA's Auditing Standards Board (ASB) issued SSAE 16. Like ISAE 3402, the SSAE 16 is an attest report.

AICPA Service Organization Controls Reports: In implementing SSAE 16, the AICPA has adopted three service organization controls (SOC) reports to expand the scope of issues examined by CPAs as service auditors. This helps organizations gain more trust in service delivery processes. Under the SOC label, there are three separate categories of service audits, designed to allow service providers to meet specific needs and refocus on niche risks:

- SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.
- SOC 2 Report – Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.
- SOC 3 Report – Trust Services Report for Service Organizations.

Service Auditor's Reliance on Internal Audit Function: The new attest standards will allow the service auditor to rely not only on management's description of the processes but also on the service provider's internal auditors.

The Problem with Over-reliance

In the past, SAS 70 Type II audits have been often used as the de facto standard for publicly traded companies to meet their Sarbanes-Oxley Section 404(b) "audit and control" disclosure requirements. This includes outsourcing contracts. However, the new "attest" reports will remove a layer of comfort for users, because the service auditors will not be exercising as much critical judgment as they would have under SAS 70 Type II. In short, the user entity will exercise its own judgment about the acceptability of the attest reports and may ask for a special attest report on user-defined "control objectives." User entities now will have to rely more on the service providers to perform the risk analysis, and the users will need to spot gaps in that analysis.

Under the new assurance standards, it is the service provider's responsibility to define the risks it faces and how it plans to monitor and mitigate those risks to ensure that the stated control objectives will be achieved.

Monitoring KRIs

Monitoring for emerging risk and responding with prompt action is the way forward. A KRI is a measure used in management to indicate how risky an activity is. Whereas a KPI measures how well something is being done, a KRI is an indicator of the possibility of future adverse impact. KRIs act as early warning signals by indicating changes in an organization's risk profile. As such, KRIs are a fundamental component of a full-featured risk and control framework and sound risk management practice. They are metrics capable of showing that the organization is subject to, or has a high probability of being subject to, a risk that exceeds the organization's risk threshold — that is, what is acceptable before action should be taken. Monitoring KRIs can be useful in helping the business reduce losses and prevent exposure by dealing proactively with a risk situation before an event actually occurs. The user entity and the service provider should develop customized KRIs as part of their risk management process.

Performing ongoing evaluations and continuous monitoring of IT risk indicators will provide assurance and more importantly raise issues in time for management to act and pre-empt risk.

Appendix A:

IT Outsourcing Life Cycle Audit Program

This is a baseline audit program for assessing the user entity's risk and process when deciding to outsource. The internal auditor's involvement with the outsourcing life cycle can vary significantly based on other assurance functions or outside experts' involvement, management's experience with outsourcing and project disciplines, or the amount of time given for audit to participate. This program lays out two examples of involvement: full scope review of all phases, or high-value areas where audit might focus given limited time or where an independent view might provide management more comfort. Numerous variations could be pursued based on consideration of audit stakeholder expectations and risk appetites or tolerances.

IT OUTSOURCING LIFE CYCLE		
Audit Step	**Full Scope Review**	**High Value Focus**
Strategic Fit and Sourcing Evaluation		
Audit objective: Identify sourcing options and identify the scope.		
Risks: Not aligned with organizational strategies; bad decision; loss of assets; lower return on investment (ROI).		
• Obtain an understanding of the strategic context and if supporting information is reliable and complete (as deemed necessary).	X	
o Is there a process mapping of the business model?	X	
o Are the options prioritized based on benefits and risks?	X	
o Has a market analysis and benchmarking study been performed?	X	
Summarize results and document conclusions.	X	
Decision-making Process – Business Case		
Audit objective: Assess whether the organization has built a reliable business case.		
Risks: Decision is not to use the optimal supplier; loss of assets, ROI, or reputational damage as quality of services may be diminished; potential regulatory impact.		
• Assess whether information in the detailed analysis is reliable and considers all business risks and implementation risk.	X	X
o Has the detailed business risk and benefit analysis factored in the execution risks and failure impact?		
o Is the best option selected based on a cost/benefit relationship?		
• Determine whether the governance and approval processes are transparent and reliable.	X	X
o Is there a relationship between the organizational business strategy and governance?		
• Assess whether appropriate parties and experts have been included in the process.	X	
• Assess whether major stakeholders are kept informed.	X	X
• Summarize results and document conclusions.	X	
Tender Process and Contracting		
Audit objective: Determine whether the selection of a provider is based on a contract that promotes success.		
Risks: Deal is not optimized or the organization is not protected from gaps in delivery of quality, availability, and integrity/privacy needs; loss of assets, ROI, and reputational damage; could have an impact on regulatory compliance needs.		
• Determine whether an appropriate approval and procurement process has been followed.	X	
• Review contract and control assurance needs from provider (e.g., need for SAS 70 type assurance or new SSAE No. 16 or ISAE 3402) and whether the organization's right to audit clause is drafted effectively and included in final agreement.	X	X
o Review detail requirements, scope, and RFPs.		
• Determine whether project team is built and resourced for implementation needs.	X	
o Review staffing levels and qualifications of project team.		
• Assess whether risk management, legal, HR and finance have been involved as needed.	X	X
• Review negotiation contracts, documents and exit planning documentation.	X	X

IT OUTSOURCING LIFE CYCLE		
Audit Step	Full Scope Review	High Value Focus
• Review due diligence documentation and results performed by operational management and the project team. Assess their adequacy and completeness.	X	X
• Perform additional steps considered necessary, with particular focus on the adequacy of control standards performed by the provider and compliance levels.		
• Summarize results and document conclusions.	X	
Implementation and Transition		
Audit objective: Determine whether the execution of transition occurred as planned to initiate new operations.		
Risks: Loss of assets or ROI due to inefficiency and unmanaged risks; interruption of service and customer impacts; operational quality is less than projected.		
• Perform pre-implementation review or have audit attend governance meetings to help ensure the project is following standard disciplines.	X	X
• Review due diligence reviews, or assess management's review of provider operations and ways of getting assurance on the provider's capability and history of providing high-quality services.	X	X
• Review contingency plans if transition is not accomplished appropriately.	X	
o Determine whether risks and actions are identified, mitigated, and escalated appropriately to stakeholders.		
• Summarize results and document conclusions.	X	
Monitoring and Reporting		
Audit objective: Assess oversight and control of outsourced operation.		
Risks: Relationship and deliverables devolve with customer damage and loss of assets and ROI; process is not sustained and is not optimized as planned.		
• Determine how the provider performance and compliance with the contract will be assessed and reviewed routinely by management.	X	X
• Review metrics that are used and other key performance indicators (KPIs).	X	
• Review how concerns and areas for improvement are communicated and leveraged to improve current and future operations/contracts.	X	
• Summarize results and document conclusions.	X	
Renegotiation		
Audit objective: Assess whether the renewed relationship evolves and improves.		
Risks: Optimization is reached with resulting loss in ROI and future operational quality; better alternatives are not found or cost increases are not justified.		
• Determine what the strategies and information needs are to ensure optimal future negotiations.	X	
• Review metrics and other KPIs that are used.	X	
o Review and compare performance to new benchmarks and new market studies.	X	
o Determine whether management establishes new targets based on performance.	X	
• Obtain an understanding of reversibility rights, monitoring activities, and actual performance results to ensure that experts and process owners are driving improvements before renegotiations commence.	X	
• Summarize results and document conclusions.	X	
Reversibility		
Audit objective: Assess whether the arrangement can be reversed and considered as part of a business case/strategy should the need arise.		
Risks: Inability to react to adverse situations or other opportunities; lack of leverage in future negotiations; loss of assets and interruption of services if brought back in house or contracted to another provider; unanticipated costs if outsourcing arrangement fails.		
• Obtain an understanding of the contingency plans in the event the arrangement does not work	X	
• Determine what the estimated costs and likelihood of failure are. Have these been considered in the business case and ROI needs?	X	X
o Can other providers be used effectively to fill any potential gaps?	X	
o What is the viability of the provider?	X	

IT OUTSOURCING LIFE CYCLE		
Audit Step	Full Scope Review	High Value Focus
o Are trigger points understood by management and pre-defined to initiate or consider changes in provider?	X	
o Has management considered other risks that might drive the need to bring services back in house, and have these risks been assessed, including macroeconomic, political, and geographic concerns?	X	
o Does the provider have sound business continuity plan (BCP) capabilities? Are the BCP efforts sustainable?	X	X
• Determine how the contract deals with the need to exit the business relationship.	X	X
• Summarize results and document conclusions.	X	

Appendix B:

IT Outsourcing Delivery Audit Program

This is a baseline audit program for assessing the service organization. Specific services provided or consumed should be identified and relevant controls added to the program. This program is designed to address risk areas in connection with a full scope audit or a control design walkthrough. A full scope audit is intended to provide assurance of the operating effectiveness of the control activities. A control design walkthrough is intended to give management an assessment of the design of the control activities. The walkthrough steps are prioritized in case the engagement is limited in resources, budget, or time.

IT OUTSOURCING DELIVERY AUDIT PROGRAM		
Audit Step	**Full Scope Audit**	**Control Design Walk-through**
Governance		
Audit objective: Determine whether the customer and service provider relationship (contract) has adequate governance and oversight.	X	X
Risks: Deterioration of the customer and service provider relationship.	X	X
• The contract should identify the division of responsibilities, which security policies and standards are to be followed, and clear service level objectives.	X	X
• Resource skill level should be adequate for the service being provided.	X	
• Communication between the service provider and consumer is formalized and sufficient to support the contract relationship.	X	X
Security		
Audit objective: Evaluate security posture at each IT infrastructure layer.	X	X
Risks: Customer systems may be accessed without authorization, or data may be lost, leaked, or disclosed without authorization.	X	X
• Security policies and procedures are in place and followed.	X	X
• Sensitive data is identified and protected.	X	
• Access at all layers is controlled (i.e., documented, authorized, reviewed, and revoked).	X	
• Regulatory or statutory requirements are identified and met.	X	
• Systems are patched.	X	
• There is a process to monitor for security proactively.	X	X
Data Quality		
Audit objective: Determine whether there are sufficient controls to ensure quality data.	X	X
Risks: Data is incomplete, inaccurate, or untimely.	X	X
• Interfaces should have data integrity controls built in, such as hash algorithms and record counts.	X	
• The jobs that process data are monitored for success or failure, and there is a process to address the failures.	X	X
• Data transfers past trusted boundaries should be protected appropriately (e.g., encrypted).	X	
Configuration Management		
Audit Objective: Evaluate existence, completeness, and accuracy of configuration database.	X	
Risks: Database does not support operational processes.	X	
• Provide accurate configuration item (CI) data (including dependencies and relationships) to other ITIL and operational processes in a central logical database.	X	
• Account for all CIs and their controlled attributes.	X	
• Verify that data supports an organization's IT, financial, legal, and security obligations.	X	
• Validate actual CI data stored in the capacity management database (CMDB) against the authorized (through change management) and discovered (using inventory/discovery tools) states through verification, compliancy and audit checks.	X	

IT OUTSOURCING DELIVERY AUDIT PROGRAM		
Audit Step	**Full Scope Audit**	**Control Design Walk-through**
Change Management		
Audit objective: Determine whether changes are carried out in a planned and authorized manner.	X	X
Risks: Unauthorized or unplanned changes result in system performance or functionality issues.	X	X
• Testing is performed to validate the functionality of the change before it is moved to the production environment.	X	
o Changes are approved and documented before moving to a production environment.	X	X
o Adequate segregation of duties are in place to prevent unauthorized program changes to the production environment.	X	
• The program libraries — both application libraries and database schemas (as applicable) — are reviewed to ensure changes are appropriate.	X	
Capacity Management		
Audit objective: Determine whether system capacity is monitored and managed to keep pace with business demands.	X	
Risks: System capacity does not meet business demands.	X	
• A process exists to ensure the monitoring of capacities and planning for future capacities.	X	
• The planning is done with participation by the business and well in advance of actual demand.	X	
• Capacity plans are reviewed periodically.	X	
• Capacity is monitored and results maintained and reviewed for trending.	X	
Service Continuity		
Audit objective: Assess whether the organization has an effective business continuity plan and disaster recovery plan.	X	X
Risks: Business-critical operations are unable to continue after a disaster or business interruption.	X	X
• There is a documented business continuity plan.	X	X
• There is a documented disaster recovery plan.	X	X
• The plans have been reviewed and approved, and have been reviewed periodically.	X	X
• The plans are tested/rehearsed regularly (at least annually).	X	X
• The plans have realistic recovery objectives and recovery time frames.	X	
• The plans are developed to support the recovery of critical business functions.	X	
Service Level Agreement (SLA) Management		
Audit objective: Assess whether the contract includes an SLA and whether the organization monitors and reports on SLA metrics.	X	X
Risks: Customer satisfaction is negatively impacted; penalties could be assessed; contract may not be renewed or may be cancelled.	X	X
• All service level targets are clear and unambiguous.	X	
• All service level targets are agreed to and approved by the user entity and the service provider.	X	
• All service level targets are measurable.	X	
• All targets within operational level agreements or underpinning contracts are aligned with the SLA.	X	
• The metrics are system-generated and tamperproof.	X	
• The SLA reports are submitted to management (and the customer) for review.	X	X
• There is a process to handle customer complaints.	X	
Incident Management		
Audit objective: Determine whether the organization has a process to handle incidents.	X	X
Risks: Business interruptions and performance issues.	X	X
• A process and tool exist to handle incidents.	X	X
• Incident management data is centralized and accessible.	X	

IT OUTSOURCING DELIVERY AUDIT PROGRAM		
Audit Step	Full Scope Audit	Control Design Walk-through
• Incident management (IM) operators have access to CMDB information.	X	
• Incidents are managed to clear performance indicators: time to own (TTO) and time to fix (TTF).	X	
• Metrics are reviewed by management and corrective actions are taken when needed.	X	X
• IM operators have been trained.	X	
• Incidents are categorized and prioritized in a way to support the business.	X	
Problem Management		
Audit objective: Determine whether the organization has a process to manage problems.	X	
Risks: Root causes of problems are not identified and incidents continue to cause business disruptions.	X	
• Problems are identified and classified.	X	
• Problems are investigated and diagnosed, with the root cause documented.	X	
• Problems are corrected and status/updates are communicated to management.	X	
Data Center Operations		
Audit Objective: Determine whether the data centers impacting service have adequate infrastructure to prevent outages or service interruptions (typically Tier III as defined by the Uptime Institute).	X	X
Risks: Provider is unable to provide or maintain service delivery.	X	X
• Physical and logical security is in place and managed appropriately.	X	X
• Temperature and humidity levels are monitored.	X	
• Power/universal power supply and grounding are installed to prevent single points of failure, outages, or service interruptions.	X	
• Smoke detection and fire prevention measures are installed and tested periodically.	X	
Program/Project Management		
Audit objective: Determine whether the organization follows a standard methodology to manage projects.	X	
Risks: Project does not meet business objectives; project overruns schedule and budget.	X	
Design and development — Determine whether the following criteria have been met:	X	
• A clear and robust business case for the project exists.	X	
• There are realistic and comprehensive assessments of costs and benefits.	X	
• All key stakeholders are involved at an early stage.	X	
• Thorough consideration of security and integrity controls exists.	X	
Project management — Determine whether there is:	X	
• Proactive leadership and real-time reporting.	X	
• Involvement of all key stakeholders.	X	
• Issue identification and escalation.	X	
• Realistic time scales and clear targets.	X	
• Rigorous testing and piloting before going live.	X	
Implementation — Determine whether there is:	X	
• Management of changes and training.	X	
• Regular and reliable tracking of benefits.	X	
• Ongoing customer satisfaction assessments.	X	

GTAG – Authors, Reviewers and Contributors

Authors

Bradley C. Ames, CPA, CISA
Frederick Brown, CISA, CRISC, ITIL-F
Jeanot Deboer
Dragon Tai, CIA, CCSA, CISA, CFE
Michael Lynn, CPA
Cesar L. Martinez, CIA, CGAP

Reviewers and Contributors

Steven Stein, CIA, CISA, CISSP, CFE, CGEIT
Steve Hunt, CIA, CRMA
Steve Jameson, CIA, CCSA, CFSA, CRMA

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

IIA®
The Institute of
Internal Auditors

www.globaliia.org