



GLOBAL TECHNOLOGY AUDIT GUIDE

# Information Technology Outsourcing



The Institute of  
Internal Auditors

## GTAG – Partners

---



**AICPA** – American Institute of  
Certified Public Accountants  
[www.aicpa.org](http://www.aicpa.org)



**CIS** – Center for Internet Security  
[www.cisecurity.org](http://www.cisecurity.org)



**CMU/SEI** – Carnegie-Mellon University  
Software Engineering Institute  
[www.cmu.edu](http://www.cmu.edu)



**ISSA** – Information Systems Security Association  
[www.issa.org](http://www.issa.org)



**ITPI** – IT Process Institute  
[www.itpi.org](http://www.itpi.org)



**NACD** – National Association of  
Corporate Directors  
[www.nacd.org](http://www.nacd.org)



**SANS Institute**  
[www.sans.org](http://www.sans.org)

# **Global Technology Audit Guide (GTAG) 7: Information Technology Outsourcing**

## **Authors**

Mayurakshi Ray

Parthasarathy Ramaswamy

## **Advisor**

Jaideep Ganguli

March 2007

Copyright © 2007 by The Institute of Internal Auditors (IIA), 247 Maitland Ave., Altamonte Springs, Fla. 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission from the publisher.

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

# GTAG – Table of Contents

---

1. Summary for the Chief Audit Executive (CAE).....	1
2. Introduction .....	2
3. Types of IT Outsourcing .....	4
4. Key Outsourcing Control Considerations – Client Operations .....	8
5. Key Outsourcing Control Considerations – Service Provider Operations.....	15
6. IT Outsourcing – A Few Applicable Control Frameworks and Guidelines.....	20
Compliance Standards .....	20
Other Available Frameworks and Guidelines.....	20
7. Recent Trends and the Future of Outsourcing .....	24
8. Glossary of Terms.....	25
9. Authors.....	27
10. Contributors and Reviewers.....	28
11. GTAG 8 Preview .....	29
12. Sponsor Bio .....	30

# GTAG – Summary for the Chief Audit Executive (CAE) – 1

Information technology (IT) outsourcing has grown in popularity as an efficient, cost-effective, and expert solution designed to meet the demands of systems implementation, maintenance, security, and operations. Access to skilled personnel, advanced technology infrastructures, flexibility, and cost savings are the driving forces behind IT outsourcing.

The benefits of IT outsourcing are accompanied by the need to manage the complexities, risk, and challenges that come with it. Internal auditors, therefore, can help organizations with a comprehensive review of its outsourcing operations, identify risks, provide recommendations to better manage the risks, and also include evaluation of the outsourcing activity's compliance with applicable laws and regulations. This guide is not intended to represent all considerations that may be necessary, but a recommended set of items that should be addressed. All decisions related to IT outsourcing should be thoroughly evaluated by each organization.

Key questions to ask during audits of IT outsourcing activities include:

- Are internal auditors appropriately involved during key stages of the outsourcing lifecycle?
- Do internal auditors have sufficient outsourcing knowledge and experience to provide the right input?
- Do internal auditors understand the roles and expectations of stakeholders within the context of the organization's outsourcing initiative?
- If IT audit plans are outsourced, are created plans based on a complete, top-down, and risk-based scope of work?
- Are internal auditors able to present outsourcing recommendations in a way that managers understand to facilitate their implementation?
- Are internal auditors able to communicate outsourced IT audit findings in a way that is understood and taken seriously by the organization's board of directors?

This guide considers the key considerations of the internal audit function within the context of IT outsourcing. The guide also provides information on the types of IT outsourcing activities that may be considered, the IT outsourcing lifecycle, and how outsourcing activities should be managed by implementing well-defined plans that are supported by a companywide risk, control, compliance, and governance framework.

Key issues include:

- How do you choose the right IT outsourcing vendor? The selection of the vendor will directly determine the success of the outsourcing arrangement. This guide will provide key considerations for vendor selection.
- What are the best ways to draft and manage outsourcing contract agreements? The concept of IT outsourcing is fairly mature, thus lending itself to well-established contracting practices. This guide

explores key contract components and structure.

- What practices need to be followed to ensure internal operations are transitioned as best as possible to the outsourcing party? Transition management can be a difficult process and needs precise planning and execution to succeed. This guide provides information on the transition process to help organizations have a smooth migration.
- How can organizations mitigate outsourcing risks? The impact of IT outsourcing on the organization can be dramatic. When business-critical functions are outsourced, they can have a significant impact on the organization's internal controls. This guide discusses main outsourcing risks and related recommendations.
- Which is the most effective framework for establishing outsourcing controls? When IT functions are outsourced, a number of critical controls shift to the vendor organization, both operationally and physically. However, the ultimate responsibility for achieving control objectives rests with the client. This guide discusses the frameworks available to help organizations design internal controls to better manage outsourcing activities effectively.

## Need of IT Outsourcing Guidance for Internal Auditors

Although IT outsourcing is an established practice and some large organizations are already experiencing the many benefits it has to offer, IT outsourcing is still evolving. However, before hiring an IT service provider, management is faced with some critical questions that must be answered to achieve its business objectives. This guide will provide some of the pros and cons of IT outsourcing, which, in turn, will enable organizations to make better outsourcing decisions.

It is important that internal auditors understand the outsourcing expectations of stakeholders regarding the outsourced activity and align their audit objectives to those of the organization. In the context of outsourced IT operations, evaluating the effectiveness of the organization's internal risk and controls framework and the chosen service provider is critical to mitigate internal control risks during the pre-transition stage and throughout the lifespan of the outsourcing agreement.

Another key issue is the internal auditor's role in ensuring adherence to the various security and compliance standards and to what extent they can rely on the work done by independent service auditors and other specialists. In essence, this guide will provide a roadmap to navigate through the complex fabric that is IT outsourcing and will point to some emerging trends in the area.

Please note that the terms vendor, service provider, service organization, and third party are used interchangeably throughout this guide.

### Definition of IT Outsourcing

During the past 15 years, outsourcing has moved from an imaginative, innovative, and high-risk attempt at reducing costs to a tried and tested strategic collaboration that helps organizations derive business value. A big contributor to this change has been the success of IT outsourcing. However, one of the key challenges for organizations is their ability to balance the benefits derived from outsourcing, such as reduction in operational costs, while maintaining a healthy risk appetite.

IT outsourcing is often defined as the use of service providers or vendors to create, maintain, or reengineer a company's IT architecture and systems. Although this definition is deceptively simple, it encompasses a wide range of outsourcing activities.

Over the years, IT outsourcing has evolved significantly in terms of its format and objectives. IT outsourcing has evolved from the outsourcing of low-end, non-core, labor intensive activities for cost reduction to the offshoring of functions such as:

- Network and IT infrastructure management.
- Application development and maintenance.
- Data center management.
- Systems integration.
- Research and development (R&D).
- Product development.
- Security management.

Other outsourced services include Web site hosting, development, and maintenance, as well as Internet security and monitoring services.

Two of the biggest contributors to the success of IT outsourcing have been the use of specialized IT skills across the globe and improvements in the technology sector that have resulted in the creation of faster, cheaper, and more effective systems and services. Countries such as India, China, and the Philippines have witnessed the emergence of large-scale, specialized vendors who have invested countless resources in the development of world-class IT infrastructures and processes. These vendors have evolved to support world-class, next-generation, end-to-end products at a lower cost and faster time.

A key driver of IT outsourcing has been the heterogeneity of IT services, platforms, and programs used by many large companies today. In many of these companies, chief information officers (CIOs) are no longer leading the IT service function. Instead, they are being asked to perform more strategic functions, such as improving service and efficiency levels, reducing costs, and adding significant business value. As a result, IT outsourcing is being used to:

- Reduce internal IT workload. This enables companies to focus on critical activities, such as IT strategy development and alignment of IT goals with business strategies.

- Achieve significant improvements in process efficiency levels. Outsourcing by definition includes process reengineering, thus resulting in a more efficient and proactive IT function.
- Provide a bandwidth of IT skills that otherwise may not be easy to retain within the organization. As a result, the vendor provides a range of IT competencies and skills that can be leveraged as the backbone of the IT function.

IT outsourcing's compelling business case as a strategic collaboration process that is capable of delivering substantial benefits and reducing long-term costs has made it a popular business. Unfortunately, anticipated cost savings sometimes leads to outsourcing contracts that are initiated for the wrong reasons or with inadequate planning. Outsourcing requires establishing and maintaining a partnership in which the vendor is an integral member of the CIO's team and the organization. Such relationships build long-term confidence and trust, remain focused on the company's objectives, and create the win-win scenarios necessary to make working relationships more productive.

The risks and impacts can have a material, strategic effect on the organization. Although processes in key areas may have been outsourced, the organization may still be vulnerable to IT risks. Thus, internal auditors can help management understand and better manage these outsourcing risks. Table 1 on the following page contains a list of common outsourcing risks and their potential impacts throughout the outsourcing lifecycle.

To establish the foundation for IT outsourcing success in terms of IT spending and performance optimization, the organization's management and internal control and operations functions must be coordinated. Components such as IT governance, IT investment portfolio management, and contract management are best addressed at the global headquarters. Other components such as cultural and communications management, local IT vendor selection, monitoring of vendor performance, and local regulatory and tax issues are best managed onsite at the local office. Regardless of where each function is managed, all of these elements must be in place and well coordinated to ensure the project's success.

In essence, the strategic outsourcing of non-core IT-assisted business functions can enable organizations to focus less on day-to-day technology management and more on its core competencies and activities. However, effective IT outsourcing requires an effectively managed collaboration with the IT service provider. This is essential to help the organization achieve benefits including:

- Reduced costs.
- Increased productivity.
- Improved customer and vendor relationships.
- Enhanced technology use.
- Increased controls.

- Proper business continuity.
- Competitive advantage.
- A renewed focus on innovation and excellence.

Internal auditors can help management oversee outsourcing activities by playing a proactive role in performance and compliance monitoring and by identifying areas of improvement and recommendations that can help vendors manage IT outsourcing activities.

Table 1: Examples of IT Outsourcing Risks and Impact

Risks	Impact
<p><b>Strategy:</b> Outsourcing strategy is not aligned with corporate objectives.</p>	<ul style="list-style-type: none"> <li>• The decision to outsource is the wrong one.</li> <li>• The contract is not set up and managed in line with corporate objectives.</li> </ul>
<p><b>Feasibility:</b> Assumptions (e.g., payback period, customer and supply-chain impacts, and cost savings) are wrong as the result of inadequate due diligence from suppliers and the organization’s failure to assess relevant risks.</p>	<ul style="list-style-type: none"> <li>• The potential for outsourcing is not explored in detail, resulting in the lack of fully derived benefits.</li> <li>• The contract is awarded to an inappropriate supplier.</li> <li>• Supplier issues are not managed efficiently and effectively because they were not anticipated properly.</li> </ul>
<p><b>Transaction:</b> Procurement policies are not met; proper service-level agreements are not implemented; operational, human resources (HR), and regulatory implications are not considered; and contingency arrangements are not planned.</p>	<ul style="list-style-type: none"> <li>• Absence of a well-drafted agreement could lead to a situation in which the client might be unable to fall back on a legally binding document to ensure compliance by the vendor to intended contractual terms.</li> <li>• Potential breaches of regulatory compliance exist that lead to financial penalties and negative repercussions on the company’s brand.</li> </ul>
<p><b>Transition:</b> There is a lack of formal transition planning, failure to plan for retention of appropriate skills, and an ineffective escalation and resolution of operational IT issues.</p>	<ul style="list-style-type: none"> <li>• There is a loss of key resources during the transition period.</li> <li>• Operational difficulties are present.</li> <li>• There is a loss of customer confidence in the outsource service.</li> </ul>
<p><b>Optimization and Transformation:</b> The outsourcing contract is not managed effectively. Therefore, outsourcing benefits and efficiencies are not realized.</p>	<ul style="list-style-type: none"> <li>• The return on investment is not what was expected or is minimal compared to the outsourcing costs.</li> <li>• The organization provides services that fall below established expectation levels.</li> <li>• There is a rise in unplanned costs.</li> </ul>
<p><b>Termination and Renegotiation:</b> There is an inadequate termination of outsourcing processes.</p>	<ul style="list-style-type: none"> <li>• The company is unable to take over the outsourced activity at a later date or to terminate or renegotiate the contract.</li> </ul>

# GTAG – Types of IT Outsourcing – 3

IT outsourcing has changed over the years. From traditional outsourced services, such as application development and IT help desk activities, to high-end services, such as product development, specialized R&D, and distributed computer support, companies continued to outsource IT services as the technology market kept maturing. The most regularly outsourced IT services today include:

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

Please note that service providers and clients may use different names for the types of outsourcing activities mentioned above. Clients also may outsource one or more of the above services to one or more service providers.

## APPLICATION MANAGEMENT

Application management can be in the form of application development, custom software development, software maintenance, and production support.

### Application Development

Development of software applications or specific functionalities or modules within an application should be outsourced to third-party software development firms that have the technical expertise and knowledge to develop applications based on the specifications provided by the client. Typically, such services start with the client's request for a technical or functional specification (e.g., requests for increased system functionality, new modules, structure or workflow activities, or system capacity work), system requirement specifications (SRSs), and functional requirement specifications (FRSs). However, in some cases the service provider may need to conduct a study of the business processes and user requirements, prepare the FRSs, and validate requirements with the client.

Coding should take place after the software development lifecycle (SDLC) methodology is created as part of the service provider's quality process. In certain arrangements, SDLC steps may be specified, monitored, and managed directly by the client. The contract or work statement should be defined clearly from the beginning, as well as the final stages of the development phase for which the service provider is responsible.

In most cases, the SDLC process ends with the successful completion of the client's user acceptance testing (UAT), however, the service provider may only be responsible until the unit testing is complete. 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.

Following are key aspects to consider during audits of SDLC activities:

1. The client and service provider need to agree on all SDLC activities, milestones, and deliverables. Service provider controls help to ensure that the development follows the guidelines defined by the client and service provider.
2. The client needs to sign off on technical and functional specification documents prior to the application's development. Alternatively, business requirements need to be received from users based on the functional specifications approved by the service provider and the client's project manager.
3. Software programming should follow a defined coding standard.
4. Independent reviews need to be designed at each stage of the SDLC process, and the review process needs to be documented.
5. Test plans, test cases, and test results must be documented and shared with the client, as well as specified in the contract.
6. Logs need to document problems noted during the unit or integration testing phase, as well as issues notified by the client after the user testing phase. Logs can be used as evidence when evaluating all defects or bugs.
7. Access control and segregation should be maintained during the development, testing, and migration of codes or programs as defined by the client's security standards.
8. Intellectual property rights are defined.
9. Access to source code in the event of financial insolvency of the outsourcer is specified.

### Custom Software Development

The purpose of custom software is to develop applications that meet specific user requirements or provide industry-specific solutions. Clients usually want a specific solution that meets a specific need or requirement. This can range from a simple standalone application to an integrated enterprise system that processes transactions from varied business cycles across the organization and updates the central database. Although audits of custom software applications are similar to those of standard development processes, the following distinct activities should be considered during internal audits of the SDLC process of custom applications:

1. Clients must sign off on all business requirement specification (BRS) documents (i.e., documents that state the functional and technical specifications of the proposed solution). Otherwise, the application

may not meet the customer's needs. Therefore, users need to be satisfied with and sign off on the proposed design.

2. Risk assessments and impact analyses need to evaluate the proposed solution and its capacity to meet established requirements.

### Software Maintenance

The custom software development recommendations should be implemented during the maintenance of existing applications and during any application upgrades whether these consist of minor changes, such as creation of new fields or reports, or major changes, such as the creation of a new module. In addition to the factors listed above, internal auditors should look at the following items during the software maintenance phase:

1. The turnaround time (TAT) defined by the client for all maintenance activities.
2. The time needed to complete the system's maintenance as recorded and monitored by the client.
3. Service provider controls are in place and adhere to the TATs. This is a crucial service-level expectation because failure to establish appropriate service provider controls could lead to a maintenance problem.
4. Integration and regression testing are completed successfully for the new module or functionality, while problems are rectified to ensure the seamless integration of existing applications.

### Production Support

Production support activities fix errors and interruptions in functioning systems (i.e., applications, mainframes, and databases) that are in production. The service provider needs to investigate the reasons for the error and interruption and fix the problem quickly. The turnaround time should be faster than that of a maintenance service because the affected systems are live and require a quick recovery so that the organization can resume regular operations.

Key audit considerations include identifying whether:

1. Service-level expectations such as expected TATs and the quality of the service provided are defined by the client in the contract. The TAT should relate to a response (e.g., the time taken to respond to the reported problem ticket) and resolution (e.g., the time taken to resolve the reported error or issue after it is logged in by the user or the time taken to submit a problem response).
2. A trail is maintained for each response and resolution. Also, auditors need to ensure there is adequate tracking and monitoring of SLA

compliance by the client. Specifically, internal auditors should look at the efficiency of the monitoring process and verify that the system's performance is measured.

### INFRASTRUCTURE MANAGEMENT

Services to manage and maintain the IT infrastructure can be classified as infrastructure management. These services include managing and maintaining infrastructure performance, 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, performing of downtime analyses, and reporting of critical system failures and their management implications.

Key audit considerations include determining whether:

1. Requests for outsourced maintenance, production support, and infrastructure management services are formally sent to the service provider. Although a workflow-based system where job tickets issued by the client to the service provider is the most effective way to send a service request, e-mails also can be used as an alternative. Verbal requests should be noted as a procedural or control weakness.
2. Approval from the client for implementation is noted in the same job ticket or separately through a written message.
3. Service-level expectations (i.e., TATs and expected quality of the resolution) are defined by the client in the contract.
4. TATs are measured and monitored adequately to ensure the availability of the infrastructure's backbone.

### HELP DESK SERVICES

Any of the maintenance services, 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 onsite (i.e., at the client's premises) or offsite (i.e., from the service provider's premises). TATs (i.e., responses and resolutions) are then defined for each level of service.

Critical compliance with service levels consist of meeting defined TATs and the quality of the service provided. In addition, the evaluation process needs to include an evaluation of procedures that measure and compare actual performance to the expected service-level parameters. Finally, performance results should be used as one of the core criteria for ongoing vendor evaluation. Audit reviews need to determine whether periodic status reports were submitted to the client and issues and improvement action items were documented.

# GTAG – Types of IT Outsourcing – 3

## INDEPENDENT TESTING AND VALIDATION

Many organizations outsource the testing and validation of software developed inhouse or by a third party. Specialized testing of the developed system is required to monitor the system's performance and identify and correct any programming errors or problems. During the testing and validation phase, internal auditors should review that:

1. Testing parameters (i.e., the system or application to be tested; actual test parameters; and the test's duration, level, and location) were defined by the client.
2. Test specifications developed by the service provider are based on the client's requirements and are signed off on by the client.
3. Test parameters include:
  - A validation of the system's design to determine whether user requirements are outlined in the system's function specification document.
  - The system is designed with adequate load-balancing capability (i.e., the system can handle the required number of simultaneous user transactions).
  - User inputs are accepted correctly, transactions are processed completely, and the desired output is obtained.
  - Application security parameters are built in to prevent common or known vulnerabilities specific to the product or platform.
4. Test cases designed to evaluate the parameters defined in point (b) above are validated by the client. Such cases also should be maintained as evidence and for future testing and reference.
5. Test results are maintained.
6. Errors, outages, and glitches (e.g., incorrect output and incomplete updates) are identified and reported in the test report.

## DATA CENTER MANAGEMENT

As more IT industry sectors, vendors, and service providers came into the market, there was a shift in the outsourcing mindset. The objective of outsourcing changed from simple cost savings to providing 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.

Outsourcing of data center operations originated from the need of organizations to decrease information management costs. As a result, data centers today typically provide the following services:

- 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 capacity management, including capacity planning, load balancing, tuning, and reconfiguration.
- Server application software installation and upgrades that meet release procedures agreed by the client and service provider.
- Ongoing installation and management of hardware and software.
- Security administration and data backup to ensure the security and integrity of systems and applications.
- Recovery of server systems in the event of a disaster that follows implemented TATs.

During reviews of outsourced data services, auditors need to determine whether:

1. The service provider has adequate capacity (i.e., infrastructure, financial, and technical capacity) to host outsourced services.
2. The service provider has segregated physically each client's data and systems to ensure their confidentiality and integrity.
3. The service provider has adequate back up capacity to ensure the client's infrastructure and network availability.

## SYSTEM INTEGRATION

In a decentralized environment, various functions are organized through disparate systems and applications that do not talk to each other. The risks of having a decentralized environment include the lack of seamless system and application updates, unreconciled account balances, and erroneous reporting or management of information systems.

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 in a seamless fashion, resulting in the presence of one consolidated system. A key limitation of systems integration is its dependency on the accuracy of existing data.

When reviewing system integration services, auditors need to determine whether:

1. Client internal assessments certify that the proposed system meets scalability, interoperability, security, and reliability requirements. Evaluation parameters should consider system interdependence, infrastructure load balancing capability, capacity planning for added infrastructure, and functional design.
2. Tools used for integration are tested separately for applicability and effectiveness.
3. Output reviews generated from the integrated system compare with desired outcomes and validate the integration's accuracy and completeness.

4. Test result reviews validate the integration's completeness and accuracy.
5. Back out procedures and conditions are defined adequately for system and integration failures.

### R&D SERVICES

To stay tuned to existing market needs while continuing to build and maintain their directories and databases, many companies outsource the research and development of different technologies, solutions, processes, and systems. Outsourced research work 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.

Audits of R&D activities need to determine whether:

1. R&D outsourced activities are classified by their necessary solutions, technologies, or specific work areas.
2. A task plan was created that identifies the sources, strategies, and types of research to be performed.
3. A database or data repository is maintained that stores information collected from various sources by category or the type of task identified. Information also needs to be collated and properly fed into the database or data repository.

### MANAGED SECURITY SERVICES

Recently, many organizations started outsourcing their security services. This outsourcing area also is known as managed security services (MSS) due to the activity's management of an organization's third-party security requirements. 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.

MSS is defined as the service that oversees an organization's security over its entire IT infrastructure, data assets, and user management activities. 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, and technical support) or include 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).

Due to the growth of information security requirements in regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996, the U.S. Gramm-Leach-Bliley Act (GLBA) of 1999, the European Union's (EU's) Directive on Data Protection of 1995, and the U.S. Sarbanes-Oxley Act of 2002, more organizations across the world are making security a top business priority.

To help organizations better manage their outsourced MSS, auditors need to examine the following:

1. Assessments of companywide security requirements. These requirements need to be based on the organization's type of work, country of operation, applicable security regulations, infrastructure set up, and user requirements (e.g., the system's level of access or system availability). The assessments should be conducted at least once per calendar year to validate the applicability and adequacy of established security requirements.
2. The outsourced function. The outsourced MSS needs to be commensurate to the assessment above.
3. The prototype design. This design needs to be validated before implementation and should be based on identified security requirements.
4. Post-implementation and MSS monitoring reports. These reports need to be presented to the user management team and include reports on vulnerability assessments, intrusion detection logs, and virus alerts.
5. Root-cause analyses of the reported vulnerabilities or incidents.
6. Designed mitigation procedures. These procedures should not be compromised at any point and ensure the security, confidentiality, and availability of data assets and systems.

Based on the types of activities described above, audit reviews need to further determine whether:

- The client follows a defined process to ascertain the access rights required by the service provider in the client systems.
- Access given to the service provider team is commensurate to the type of services rendered.
- Access is granted and revoked on a timely basis and is determined by the addition or removal of service provider staff, or by the expiration of time-based services.
- Periodic reviews of access rights take place to make sure rights established are valid based on the system's user requirements and lead to the removal of redundant access rights.
- The outsourcing team has adequate skills and expertise to determine the cause of errors and formulate plans to correct them.

# GTAG – Key Outsourcing Control Considerations – Client Operations – 4

A successful outsourcing initiative requires careful consideration of several aspects before the partnership is initiated and throughout its lifecycle. Each successful initiative begins with careful consideration of the business case, which specifies the investment schedule and the expected business benefits in terms of cost reduction and maximized work efficiency over a three- to five-year period. Thus, the business case helps to establish the expected payback period. A well-constructed business case also indicates how identified benefits are to be accomplished through a careful alignment of vendor selection, an established transition and process improvement approach, and the use of risk and security solutions.

The figure below depicts a typical outsourcing value chain. Some of the aspects are discussed in detail in the following paragraphs.

## 1. Governance Outsourcing Framework

When undertaking an IT outsourcing initiative, governance is arguably an area that organizations underestimate most frequently in terms of time and investment and the structural architecture necessary to manage accountability. Companies that commit to an IT outsourcing partnership without a strong governance capability do not have the means to properly manage the outsourced activity.

A robust governance framework requires skill and expertise so that the organization can deliver the strategic, operational, and project management guidance necessary for the outsourcing activity to be effective. Because the outsourcing activity spreads across two separate organizations, the need for a clear governance structure is critical when specifying the processes, roles, responsibilities, and incentives that will form the outsourcing arrangement. As a result, the governance structure should help the organization meet the following objectives:

- Align every IT outsourcing contract with the organization’s key business objectives and the needs of primary stakeholders.
- Set up a monitoring mechanism to ensure the IT services outsourced are performed according to the client’s specifications.
- Manage changes in IT projects and services across complex portfolios.
- Establish direct and visible accountability for IT performance.
- Define specific ownership of key contract terms.
- Define well-integrated IT management processes for the client and service provider.

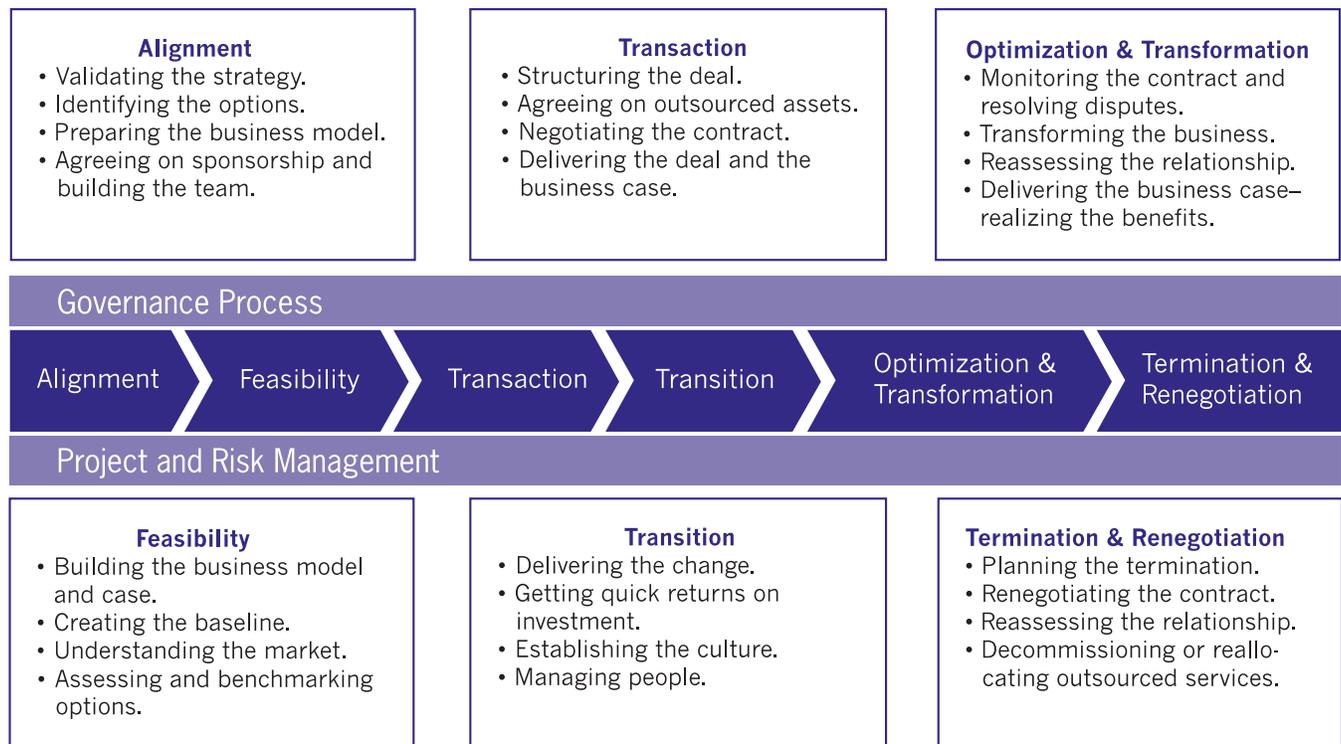


Figure 1: Typical outsourcing value chain.

Audits of governance effectiveness should evaluate risks in the client organization with regards to the objectives outlined above. Key questions auditors need to ask include:

- How transparent is the governance process?
- Do formal relationship management processes address outsourcing conflicts and build effective working relationships between contracting parties?
- Are roles, responsibilities, and delegation of authority activities defined clearly between contracting parties?
- Are communication channels established clearly?

## 2. Alignment and Feasibility

The alignment and feasibility phase deals with the formalization of the IT outsourcing strategy. During this phase, the client should prepare a business case that is based on various IT outsourcing models and an assessment of outsourcing options that is based on research and benchmarking. The outsourcing strategy chosen needs to detail the portfolio of services that will be assigned to one service provider, or to multiple service providers, and the location of these services (i.e., onsite or offsite). The different outsourcing models usually include build-operate-transfer activities, joint ventures with service providers, or a combination of both. Key audit considerations include:

- Is the client's IT outsourcing strategy aligned with the company's overall business strategy?
- Did the client properly consider all financial, operational, and legal considerations before embarking on the IT outsourcing partnership?
- Are outsourcing assumptions validated by research or data?

## 3. Transaction

**Vendor Selection** – Vendor selection requires a comprehensive evaluation of the service provider's technical competencies and constraints and is based on the organization's outsourcing service needs. Although there is no right or wrong approach, organizations should follow the steps below as part of any vendor selection program.

### Step 1: Plan and Prepare

- Establish a formal project management process that clarifies the roles and responsibilities of all the internal staff involved in the outsourcing partnership. The process also needs to be based on the type of services being outsourced and should define how authority is to be delegated.
- Create a core team to evaluate vendors and participate in negotiations. According to industry best practices, team members should represent different company segments, including IT, finance, legal, and

HR, as well as management from affected business units. The CIO typically leads this team.

- Identify the roles and responsibilities of team members throughout the lifecycle of the IT outsourcing initiative.
- Detail the scope of work (i.e., application, infrastructure, and type of service) that is expected to be outsourced. This includes the creation of a milestone-based plan that discusses how and when the organization should increase or extend the scope of outsourced work.
- Create a list of parameters to be considered for vendor selection that is in line with the organization's key outsourcing requirements. Parameter considerations could include the use of global delivery centers, necessary language skills, and minimum level of IT outsourcing experience in specific kinds of environments. List attributes may come from multiple formal and informal sources, such as referrals, market knowledge, competitor insight, and independent consultant recommendations.
- Understand legal outsourcing requirements, including compliance with different country-specific regulations, such as open market restrictions and open tendering.

### Step 2: Gather Vendor-specific Data

After plans and preparations are under way, the team needs to assess the vendor's capability and operations. Depending on the criticality, value, timeliness, and scope of the contract, the assessment should be conducted through a formal request for proposal (RFP) process or by holding informal discussions with identified vendors. Key actions to be completed when gathering vendor-specific information include:

- Gathering specific details, such as the vendor's size, stability, experience, location, infrastructure, level of process quality, and skill sets.
- Incorporating clear specification requirements into a document called the "statement of requirement" that highlights the scope of services to be outsourced, the contract's duration, expected control requirements and compliance, service-level requirements for all key processes and services, and the client's capacity requirements. The statement of requirement needs to be completed as part of the RFP process.
- Developing an exhaustive list of vendor information requirements with values attached to each parameter that can be used during the final selection round. Parameters to be used can include the vendor's:
  - Background and statement of experience.
  - Management and project management employee information. This is especially relevant for organizations that pay close attention to the vendor's technical skills.

# GTAG – Key Outsourcing Control Considerations – Client Operations – 4

- Operation and risk management frameworks, including any relevant certifications, methodologies, and business continuity measures; compliance with intellectual property rights; data and sub-contracting security measures; and legal and regulatory compliance activities.
- Project-specific approach and methodology, including the allocation of resources.
- Client references including, information on transitioning success.

The service provider's ability to manage the transition of client services is an essential aspect that needs to be evaluated during the vendor selection stage. Transition parameters encompass critical assessments of the robustness of the vendor's transitioning methodology for issues that include:

- All phases of the transitioning stage and incorporate best practices such as Six Sigma principles.
- Transitioning details on specific milestones, documentation, technology analysis, capacity planning, and costs.
- Available support to mitigate risk and manage productivity during the transition period.
- Onsite redundancy, reorganization, and retraining.
- Success in previous transitions, including number of transitions and whether they occurred on time and within budget.
- Robustness of support plans, such as risk, contingency, and business continuity plans.
- Quality of the transitioning team, including the team's profile and experience.

### Step 3: Conduct Due Diligence

When responses to RFPs have been received, the project team should begin to analyze the submitted information against the pre-defined evaluation framework. Action items to complete include:

- Client reference checks during the final due diligence stage. The project team must evaluate the vendor's project management competency, success rate, the quality and standard of work, adherence to contract terms, and communication process.
- Country-specific risks and information, including availability of skills, costs, political environment and stability, cultural compatibility, and accessibility.
- Site visits to evaluate the service provider's capabilities, operations, infrastructure, and local culture.

Based on each vendor's response, client reference checks, site visits, and final negotiations typically take place with a final group of two to three service providers.

### Step 4: Negotiate and Close

Negotiating and closing the deal are the final steps in

the vendor selection process. How to conduct this step is determined largely by the due diligence exercised in the previous steps. Below is a description of actions organizations can take.

- Simultaneously negotiate with at least two vendors. This enables the company to compare deal prices and legal terms. Large outsourcing contracts could involve negotiations with three to four vendors.
- Involve legal and senior management staff to discuss the contract's terms and conditions. Service providers usually come prepared with a standard contract containing the partnership's terms and conditions. Most organizations discuss the contract with their legal advisors before doing so with the service provider.
- Sign the contract. Most service providers are prepared to modify the contract as needed before signing takes place.

### Legal and Contractual Considerations When Contracting With Service Providers – IT outsourcing

arrangements involve different levels of complexity, risk, and a range of legal and contractual issues. Special concerns deal with the difficulties of terminating long-term engagements and in defining responsibilities in organizations that have not worked together before, especially in an environment shaped by changing business conditions.

Many senior managers will agree that part of the foundation for a successful initiative is based on the legal and contractual due diligence that takes place before the outsourcing engagement is formalized. Therefore, unless managerial outsourcing controls are supported by a well-written contract, management and operational activities may be under-supervised. This increases the likelihood that key processes, quality specifications, service delivery timing, and outcomes will be driven by or depend on the vendor.

Legal and contractual issues that should be addressed when drafting a well-written contract include:

1) **Service levels and incentives.** The organization must outline minimum performance benchmarks, standards, and metrics that are most appropriate for the outsourcing objective, such as measures that are directly tied to operational indicators (i.e., service quality, system availability, and response times). If possible, it is important to avoid exclusivity or preferred provider clauses to maintain competitive pressure on the vendor.

2) **Vendor personnel.** People represent a core performance driver. The client should be able to approve the selection of key vendor personnel and be in a position to define the criteria used to screen replacements. Because the loss of key personnel can affect the vendor's ability to deliver on contracted obligations, some clients insist on having approval rights over the

vendor's retention and compensation strategies. This will maximize the likelihood that personnel critical to solution delivery and knowledge transfer continue to work for the vendor throughout the agreement's duration.

**3) Data protection, privacy, and intellectual property.** Risk is always involved when third-party entities are given access to sensitive customer data, privileged business operation details, or intellectual property vulnerable to public or competitor disclosure. Key issues can range from requiring the vendor to maintain specified levels of security through employee awareness training and contractual obligations, such as signing a non-disclosure agreement by service delivery personnel and company indemnification by the vendor for any breaches.

**4) Price protections.** Establishing price changes is one of the most important contract areas in IT outsourcing because small differences in price can affect an outsourcer's options, choices, and business objectives. Contracts should cover pricing issues such as changes in service scope, agreed pricing parameters, maintenance of preferred or "most favored customer" pricing, and procedures to accelerate the resolution of pricing disagreements.

**5) Third-party assignments.** In situations where the vendor hires a third party (i.e., a sub-service provider) to deliver services, the client needs to include in the contract how service quality will be managed and any client performance risks.

**6) Ownership of assets used or created by the IT outsourcing partnership.** IT outsourcing vendors sometimes require use of the organization's resources or assets to meet contractual obligations. Rules and procedures should define and create ownership rights when new value is created from an outsourcing activity. Contract terms should specify any procedures needed to minimize confusion and disagreements that can arise whenever systems, resources, and assets are shared.

**7) Conflicts among different legal systems.** Contracts must be based on applicable national and local laws. Outsourcing contracts, especially those defining parameters for offshore initiatives, can become quite complex if different justice systems and legal resolution disputes are not considered at the beginning of the initiative. Key issues in this area include the use of language that clarifies potential ambiguities in contract interpretation and dispute settlements, as well as language that clearly defines procedures and processes

for problem identification, discussion, escalation, resolution, and management (e.g., dispute resolution, mediation, and arbitration).

**8) Contingency management and change planning.** One of the most important goals of the contract is to protect the client's ability to reshape the outsourcing contract, relationship, or operating framework so the client can adapt to changes in the business environment. Critical to any outsourcing partnership is the flexibility to accommodate unanticipated business changes, such as growth, extraordinary events, mergers, acquisitions, or sales. This flexibility needs to be stated in the contract.

**9) Notice of adverse material impacts.** A well-written contract must ensure the client's right to be informed of any event that could affect the vendor's ability to meet its obligations. Receiving timely notice on impending events enables the organization to keep down contingency planning costs while maintaining a high return on investment (ROI) when unforeseen events do occur.

**10) Right to audit.** Contracts need to include clauses that provide the client with well-defined rights to audit processes, controls, and results associated with the outsourced activity. This includes the use of Statement of Auditing Standard No. 70 (SAS 70) reports or a similar kind of review, as well as the audit of various regulatory compliance issues such as those associated with the U.S. Sarbanes-Oxley Act of 2002.

**11) Termination.** Even IT outsourcing contracts developed under the most auspicious principles of partnership and collaboration should stipulate the conditions leading to termination. These conditions range from termination for a specific reason to termination due to a convenience factor. Contract language should define the client's rights, as well as procedures that must take place for termination and the options to purchase or license assets.

Key internal audit considerations that need to be reviewed in this stage include:

- Determining whether the vendor selection process was conducted in a fair manner.
- Examining the contract's description of aspects the client will be exposed to once the outsourcing partnership begins.
- Identifying whether a checklist exists that consists of the legal and contractual factors agreed on by the client and service provider that help to determine the vendor's compliance with each of these factors.

# GTAG – Key Outsourcing Control Considerations – Client Operations – 4

## 4. Transition Management

Transitioning or migration involves the transfer and ownership of knowledge to an entity with no previous experience with a given system, process, corporate culture, or industry. Although transition plans are the responsibility of the client, they usually are delegated to vendors. Migration activities typically involve two stages, planning and knowledge transfer.

### Planning

The planning phase involves the development of a migration strategy. During the planning phase, the organization needs to include the costs and timelines for each significant milestone in the migration plan. As part of the transition strategy, the client and service provider jointly identify the most optimal migration mode (e.g., a complete transfer or all activities or a gradual rollout of functions based on a prioritization scheme). The strategy also needs to assign specific resources and budgets for each step of the migration phase.

### Knowledge Transfer

Executing an effective knowledge transfer plan is essential for the long-term success of the outsourcing partnership. This requires that the client and service provider identify and document all the necessary information (e.g., technical, business, process, and background information) so that the transfer process has the least impact possible on the service quality of the outsourced activity.

A high-quality service provider should have a well-established process for ongoing knowledge management that does not disrupt the client's quality of service. Comprehensive and detailed documentation needs to be available so that the company can bring the activity back in-house or transition to another service provider if necessary. This gives the client greater leverage to ensure services are delivered as stipulated in the contract. In addition, the client needs to have access to the relevant information documented during this phase. As a result, the company needs to perform periodic audits of the knowledge transfer process.

Finally, this stage may involve on-site visits by the service provider's senior project managers. Some organizations also prefer that their staff visit the service provider to set up the outsourcing process. Key personnel may include senior managers or product directors who can organize the outsourcing activity and senior engineers who can train the service provider team. The frequency and duration of visits should decrease as service operations mature and stabilize.

## 5. Change Management

The outsourcing project can disrupt the organization's operations during various stages of the outsourcing initiative. Organizations need to identify, plan for, and manage

these disruptions as best as possible to reach their desired outcome.

Transitioning is one stage in which the client and service provider could experience high levels of change. During this stage, the service provider has to ensure it has the necessary experience to deal with any disruptions caused by the transition process. The client and service provider can manage any changes that occur during the transition phase by:

- Defining key processes and control requirements. These processes and controls should cover security, business continuity planning, disaster recovery, compliance, and data protection activities.
- Identifying plan elements and their corresponding timelines.
- Describing client and service provider responsibilities during the transition phase.
- Establishing service-level requirements for all key processes and services, including service levels at various stages of the transition process.
- Specifying the different technology and connectivity adaptations needed during the transition period.
- Describing robust reporting tools, policies, and procedures to handle interfaces during and after the transitioning of reporting formats (i.e., status reports, key performance indicator (KPI) reports, hierarchy reports, and frequency reports) and escalating mechanisms to be used during the transition phase.

## Stabilization and Monitoring

The last stage of the change management process is the stabilization of operations. This refers to the live performance of the outsourced processes under the service provider's controls. During the transition phase, certain outsourced activities may resume their normal operations within a defined timeframe. Any delays should be closely monitored because they can have a negative impact on the realization of outsourcing benefits. This also helps the organization react and respond to any issues in a proactive manner.

During the monitoring phase, organizations need to ensure communication takes place between the on-site team and service provider. This is imperative for the partnership's success. Communication should address:

- Reports on KPIs and other performance measures.
- Analysis of KPI trends and performance.
- Documentation of any performance deviations and their analysis.
- Plans that identify any resolution issues including the timeframe for each resolution.
- Communicate through the appropriate channels. This may include telephone calls, Webex or Internet-based meetings, chat sessions, e-mails, and video conferences, or more formal channels, such as weekly and monthly updates or meetings.

- The responsibility of the vendor to upload any software product development information, project-related documentation, and work in progress reports to the appropriate intranet site, so that clients can obtain the necessary project status information.

## Internal Audit Considerations

Key questions internal auditors need to consider at this stage include:

- Does a formal transition management strategy exist?
- How effective is the knowledge transfer strategy in terms of its design and operating effectiveness?
- Has attrition affected the transfer phase or affected the operation of outsourced activities?
- How effective is the communication and review process?
- How effective is the change management process in terms of its design and operating effectiveness?
- Is there a process in place to ensure only approved changes are carried out by the service provider?
- Are review samples documented appropriately to demonstrate that all stages of the change management process were followed?
- Is there a formal management process? If so, did it monitor the project's progress and its benefits at the specified timelines?

## 6. Transformation and Optimization

A well-defined, yet flexible, contract is often the key to a successful IT outsourcing relationship. This contract defines the boundaries, rights, liability, and expectations of the outsourcing vendor and client and is often the only mechanism for regulating the outsourcing relationship. IT outsourcing contracts must be crafted to provide clients with tools that:

- Retain leverage and manage change.
- Manage in-scope and new services.
- Monitor and manage service quality.
- Deliver promised cost savings.
- Provide competitive price protection.
- Manage potential liability and risks without affecting the project's price.

One of the most critical outsourcing contract elements is the definition of service-level targets, which must be achieved as part of the outsourced service's delivery. It is important for the client to have a process in place that addresses how service-level parameters are to be changed, how formal reviews need to address compliance to agreed parameters, and how to evaluate any deviations.

The SLA should describe:

- The service's objectives and scope.
- Performance metrics and corresponding service levels against each metric, including:
  - Volume (i.e., the number of maintenance requests per month and lines of code).
  - Availability (i.e., availability of provided services for a specific period of time).
  - Quality (i.e., the number of production failures per month, number of missed deadlines, and number of deliverables rejected).
  - Responsiveness (i.e., the time needed to implement an enhancement or to resolve production problems).
  - Efficiency (i.e., the number of programs supported per person, rework rates, and client satisfaction surveys).
- Frequency definitions to measure performance (e.g., monthly, quarterly, etc.) and other informal contract performance reviews through regular progress meetings and reports.
- Payments based on SLA performance.
- Definition of clauses that stipulate the availability of the contract's renegotiation for nonachievement of SLAs.

As contract management increases in complexity, the role of contract manager may emerge, especially in organizations with a large number of outsourcing contracts. The contract manager can be an in-house or contracted employee and should work with the client's internal legal department to observe contract formalities. A full-time, experienced contract manager should track communications, as well as review and maintain manual and monitoring operation procedures for compliance with the contract's terms.

## Internal Audit Considerations

A key aspect internal auditors need to examine during this stage is the SLA conformance. Auditors also need to evaluate the strength of the client's review process. Key questions to ask include:

- Are key areas defined in the SLA aligned with the benefits or process improvement parameters identified in the business case?
- Are periodic reports from the service provider based on the key areas agreed in the SLA?
- Are service provider reports independently validated for accuracy and completeness?
- Is the review of service provider reports effective? Was adequate action taken when deviations occurred?
- Are SLA term changes approved appropriately?

# GTAG – Key Outsourcing Control Considerations – Client Operations – 4

## 7. Project and Risk Management

Given today's regulatory landscape, compliance risk management is emerging as a top priority for many organizations, especially those in the financial services and healthcare industries. To establish an effective compliance risk management process, clients and service providers need to:

- Determine the types of compliance risks the client organization is exposed to based on the type of outsourced service.
- Identify processes that can have a material impact on compliance risk.
- Establish manual and automated process controls to ensure that all risks are mitigated.
- Define SLAs with regard to potential compliance risk exposures, which processes will be reviewed, audit responsibilities and frequency, and correctional steps.
- Implement and monitor a robust governance model for overseeing regulatory compliance.

Outsourcing risks range from incorrect vendor selection, poor contract management, transition problems, risks of organizational backlash, and security vulnerabilities. As outsourcing activities mature, organizations become more aware of and are more sensitive to these risks. The challenge, then, is to identify hidden risks and define the appropriate strategies needed to minimize their impacts. For example, a possible control risk could arise after a service provider is made responsible for the outsourced activity's success or failure. As a result, the client organization must interact closely with the outsourced teams to track, guide, and plan outsourced operations based on organizational goals and expectations.

Project tracking that is based on predefined metrics, such as quality, timelines, and resource planning enables the seamless integration of client and service provider teams, cultures, and knowledge. This may be done through:

- Status reports and meetings. Many organizations maintain joint risk logs. This helps to ensure a better transparency and visibility of issues and action plans, thereby facilitating proactive decision making.
- Reports of project milestones.
- Daily communication among team members on operational issues through telephone calls, chat sessions, video conferencing, or e-mail.
- Delivery of interim artifacts, such as program designs, codes, documentation, and test plans.
- Project portals where all documents related to the project are stored. The project portals should be accessible only to team members assigned to the project.
- Service staff traveling onsite or development team members from client organizations visiting the vendor for reviews.

Sustaining and enhancing software development quality is one of the most important objectives of organizations that outsource IT operations. To ensure quality, outsourcing processes need to be well planned, managed, and monitored. Organizations also need to establish a special quality assurance (QA) team to ensure process quality, especially in organizations engaging in specialized processes such as software development.

In addition, contracts can be used to establish risk management expectations. Although a contract is a useful statement of the parties' responsibilities, it should not be a substitute for a strong governance model to monitor, communicate, and resolve vendor disputes. Client and vendor relationships are mutually beneficial when contract terms are clear and the parties have provided a robust mechanism to manage daily activities and a procedure for dispute resolution.

## Internal Audit Considerations

During their evaluations, internal auditors need to determine whether the service provider is in compliance with the outsourcing agreement and whether their activities are robust, transparent, and unbiased. To this end, internal auditors need to identify:

- The presence of a well-structured business case that clearly outlines desired business outcomes.
- A well-documented statement of requirements.
- A planned, structured, and transparent vendor short list, evaluation, and selection process, with pre-defined criteria and objective rankings.
- A formal migration strategy and knowledge transfer process.
- Mechanisms for the arrangement's stabilization and monitoring through defined KPIs and pre-agreed communication and status monitoring channels.
- Well-defined SLAs and comprehensive flexible contracts.
- Established processes for change and risk management, as well as process quality assurance.
- Well-documented frameworks for managing business continuity processes, as well as information, network, physical, and personnel security.

For the internal auditor to determine that the outsourced activity is executed in a well-planned and controlled environment, each of the above considerations must be met fully in terms of adequate documentation and evidence of operations.

# GTAG – Key Outsourcing Control Considerations – Service Provider Operations – 5

As part of the IT outsourcing venture, some of the client's controls may be transferred to the service provider totally or in part. In such cases, the audit's scope extends beyond the client's operations. This section discusses key control considerations that need to be evaluated to identify the effectiveness of the service provider's internal controls.

## 1. Control Environment

An important control consideration is the evaluation of the service provider's IT control environment. The control environment sets the organization's tone, impacts user behavior, and is the foundation for other internal control components. For instance, certain aspects of a service provider's control environment may affect the services provided to the client. Control environment prerequisites include the prevalence of strong documented policies, procedures, and guidelines, as well as a clear definition of the roles and responsibilities of information systems personnel.

Another objective of this evaluation is to gain reasonable assurance regarding the strength of the service provider's IT governance structure. As a result, this evaluation should analyze the service provider's:

- Team structure and composition (i.e., does the team have the skills, competency, and experience necessary for the services provided?).
- Delivery of services according to agreed SLAs.
- Security controls for all customer information.
- Endpoint security for all networks, extranets, and intranets, as well as security controls for all Internet activities and services, Internet service providers, and Web site activities directly linked to data centers.
- Feedback received from customers.
- Customer data backups.
- Disaster recovery and business continuity plans.
- System uptime and performance.

Service organizations also are required to perform periodic risk assessments that take into consideration various factors affecting the services provided to the client. Periodic, structured risk assessments of the IT infrastructure, systems, and applications are a good indicator of the service provider's attitudes toward the IT environment from a control perspective. Factors that should be considered while performing these risk assessments include:

- Changes in the operating environment.
- New or revamped information systems.
- Growth, including but not limited to, organizational growth and growth in services provided to clients.
- New technology.
- New business models, products, or activities.
- New accounting pronouncements.
- New personnel.

## Information Security Policies and Procedures

Service providers normally have documented policies and procedures related to various information security (IS) functions, including:

- IT administration (i.e., IT management, records management, document management, device naming conventions, transmission control protocol/Internet protocol implementation standards, network infrastructure standards, computer and Internet use policies, and e-mail policies).
- IT asset management (i.e., IT asset standards, IT vendor selection, asset assessment, asset installation satisfaction, and media storage procedures).
- IT training and support (i.e., system administration, IT support center, IT server and network support, IT troubleshooting, and IT user and staff training plans).

Organizations may have a separate IS team that has a clearly defined organizational structure and documented roles and responsibilities. The IS team establishes detailed security policies and procedures on IT security and disaster recovery activities, such as:

- IT threat and risk assessment.
- IT security planning.
- Media storage.
- IT disaster recovery.
- Presence of computer malware.
- User access control.
- E-mail security.
- Remote access controls.
- Network security management.
- Password policies.
- Data classification guidelines.
- IT security audits.
- IT incident handling.

Service organizations should ensure that policies and procedures are formulated, developed, and documented for all key IT activities. The policies and procedures developed should be communicated clearly to the appropriate process owners and business teams. A process should exist to review the policies and procedures periodically, while required modifications should be performed based on existing business conditions.

A policies and procedures compliance process is also vital. Once outsourcing procedures are formalized, they should be reviewed periodically to ensure their compliance with established policies. A defined process also needs to be implemented to address noncompliance with policies and procedures and remediate identified issues.

## 2. Security Considerations

To obtain the desired ROI, security risks need to be managed effectively. The primary types of security risks that need to be addressed in any IT outsourcing context include:

# GTAG – Key Outsourcing Control Considerations – Service Provider Operations – 5

- Information protection.
- Network security.
- Physical security.
- Personnel security.
- Logical access controls to applications.

## Data Protection Risks

Data is an essential business component and should be treated as an important corporate asset. Information is not restricted to papers and documents; it includes data residing in services and application software, employee information, research records, price lists, and contracts. To protect data assets, companies need to:

- Identify which security risks may affect the organization.
- Establish policies and procedures addressing key areas, such as acceptable use, information classification, third-party access, data transmission and remote data access, and password and user access policies.
- Support policies with necessary guidelines, procedures, and templates.
- Obtain senior management's commitment to the information security initiative. This demonstrates the presence of a strong operational team that understands the threats posed by security issues and the organization's ability to monitor and deal with security problems and vulnerabilities.

## Network Security

Organizations can take a number of measures to secure their networks, the place where information is stored and transmitted. To ensure the security of their networks, the following security elements need to be included as part of the organization's data protection efforts:

- Proper documentation, design, and implementation of the network.
- Configuration of firewalls to deny access to unauthorized traffic.
- Physical and logical separation of the client network from the service provider's local area network.
- Installation of antivirus software on all servers and systems.
- Use of regular virus signature updates.
- Measures to prevent unauthorized access to the company's network or data.
- Secure connection and encryption.
- Security of network software and operating systems.
- Policies for access control and authentication.
- Remote diagnostic port protection.
- Network connection control.
- Network routing control.
- Intrusion detection systems.

## Physical Security and Environmental Controls

Physical security refers to the means used to secure an object or location, such as company's building, work areas, systems and devices used, and documents. Depending on the type of activity outsourced, client organizations need to ensure that the service provider's documents, systems, and infrastructure are secured properly.

Many organizations are demanding higher security levels in outsourcing facilities, especially when the activity outsourced is critical for the success of the organization's operations. Key security measures include:

- Around-the-clock use of trained security guards provided by professional security agencies and use of physical entry controls such as:
  - Access authorization and identification mechanisms (e.g., identification cards and swipe cards).
  - Access restriction on a need-to basis to areas dedicated for client processing and service delivery. These areas should have their own dedicated workstations, computer network, and infrastructure (e.g., phone lines, file and print servers, and printers).
  - An entry and exit tracking system to ensure visitors are issued appropriate entry badges and their belongings are checked.
  - Additional restricted access to server rooms and data centers.
  - A dedicated floor space monitored by closed circuit television 24 hours a day, seven days a week to prevent and monitor suspicious activity on critical locations (e.g., the data center, network room, building entrance, and production floors).
  - Restricted movement of media (e.g., compact disks, floppy disks, and flash drives) and papers controlled through physical inspection and authorization at gate passes.
- Use of shredders located at various locations to dispose of data and documents. This helps to ensure that confidential documents and data are not stored or carried outside the building.
- Storing backup media containing critical data at on- and off-site fireproof cabinets.
- Use of fire suppression systems such as smoke detectors.

## Personnel Security

Personnel security refers to companywide procedures to ensure that all personnel who have access to sensitive information or a particular location have the required authority and clearances. The evaluation of personnel security should consist of the following:

- Detailed background checks of potential employees

# GTAG – Key Outsourcing Control Considerations – Service Provider Operations – 5

that identify previous employer reference checks, criminal record checks, and educational qualifications. The background check also could verify other aspects, such as a person's social background. Although most organizations prefer to conduct employee reference checks in-house, they may be outsourced to a specialized local agency.

- Mandatory confidentiality agreements for all employees. Most outsourcing partners have a standard non-disclosure agreement, which states the penalties for a breach of contract, including termination of services.
- Use of printers and photocopies on a need-to basis. Many service providers secure their photocopiers with staff and keep track of the employees, number of pages, and information printed or photocopied.
- Logs of each employee's work and access.
- Internet access controls. Some service providers have cybercafé facilities outside of the client processing area for employee use.
- Tools that scan all internal e-mails, forbid access to external e-mails, and scan e-mails for critical words and size limits.
- Password management, including confidentiality, regular change schedules, and single user sign-on where multiple accesses are required.
- Automatic terminal identification, terminal logon procedures, and user identification and authentication.

## Logical Access

Restricted access and application password controls are critical to prevent unauthorized access in locations where sensitive data is processed or stored. This may require restricting access to specific data elements based on a person's role and responsibilities, preventing access to other confidential data, or requiring the restriction of particular transactions to certain users.

Key logical access considerations include:

- Verifying that security requirements specified in the contract are implemented, such as regulatory specifications.
- Reporting security breaches regularly, such as invalid access attempts.
- Using independent tests to check that security levels cannot be breached, such as conducting penetration tests of IT networks and Web sites.
- Restricting access to sensitive data or particular transactions to key staff.
- Auditing the technology and processes used to prevent unauthorized access to the client's records in situations where a supplier provides IT operation services to several customers. This may require specialist assistance.

In addition, particular focus should be placed on logical access controls over critical applications, databases, and operating systems, such as:

- A formal process for account management (i.e., user and administrative controls for critical systems, such as operating systems, application systems, and databases).
- Audit trails to track the creation of user accounts and access authorization for user accounts.
- A formal review process for periodic user accounts on operating systems, databases, and applications that support a critical function to ensure logical access is provided to authorized users only.

Finally, the following security requirements should be considered when using Web services:

- Firewall protection with access rules and restrictions for internal network and applications accessible via the Internet by an Internet browser.
- Anti-spam software to prevent unauthorized Internet e-mail addresses or software downloads to the network.
- Installation of virus protection software to protect against and detect viruses on e-mails or Internet downloads.
- Regular updates of virus software to ensure that new viruses are detected.
- Authentication controls for applications residing outside the network (e.g., use of smart cards and digital certificates).

## Business Continuity

Business continuity management (BCM) is an enterprise-wide, risk-based approach to develop proactive measures that ensure the continuing availability of business support systems and mitigate disruptions risks. As stated in figure 2, BCM helps organizations to maximize the availability, reliability, and recoverability of business systems through the effective management of people, processes, and technology. It also enhances an organization's ability to recover from a disaster, minimize losses, and have the best level of preparedness to deal with business interruptions and restore operations. In the absence of such a plan, the organization could face long-term revenue losses and loose customer confidence.

Business continuity policies and guidelines are a critical component of the outsourcing contract and should be detailed clearly in SLAs addressing:

- BCM mechanisms.
- Response times based on the outsourced process type.
- Types of audits required, as well as the audit's location, frequency, cost, person in-charge of the audit, and the information that will be shared between the parties.

# GTAG – Key Outsourcing Control Considerations – Service Provider Operations – 5

- Penalties due to the inability of the service provider to resume business operations during and after a disaster as defined in the SLA.

The scope and operational aspects of the BCM typically differ based on the organization’s risk appetite, the criticality of activities and projects outsourced, and the overall dependence of operations on IT. Business continuity plans should identify:

- Potential sources of disruption.
- Critical processes and applications and acceptable levels of downtime via a business impact analysis.
- Acceptable response and recovery times.
- BCM mechanisms including:
  - Storage mechanisms and locations (e.g., tapes, off-site servers, and redundant arrays of independent disks).
  - Frequency of data backups.
  - Creation of alternate sites.
  - Infrastructure availability of equipment and networks.
  - Access points into several telecommunication carriers.
- Personnel responsibilities based on the extent of the disruption and the nature of the process impacted.
- The individuals accountable for the business continuity process.

- Business continuity plan tests and maintenance activities.

As a result, the following aspects become critical during the BCM process:

- Reviews of the service provider’s BCM and disaster recovery plans to ensure that disruptions in their premises, staff, or systems will not affect the client’s systems adversely.
- Reviews of the service provider’s BCM and disaster recovery test plans and test reports.
- An understanding of the role BCM and disaster recovery testing plays in ensuring the service provider’s plans are effective for the client systems.

### 3. SDLC Controls

SDLC controls should be applied to all new applications developed or acquired by the service provider or during major enhancements and maintenance activities to existing applications. To reduce acquisition and implementation risks, organizations may use a specific system development or quality assurance process or methodology that is supported by standard software tools and IT architecture components. This process provides a structure for identifying:

- Automated solutions.
- System design and implementation activities.

Business Continuity Management			
Issues Addressed	Availability	Reliability	Recoverability
Solution	Enterprise High Availability	Service Level Management	Enterprise High Availability
Objective	Achieve and maintain the chosen availability level of the enterprise’s IT infrastructure.	Effectively manage and control the IT infrastructure to improve the overall operational reliability.	Provides an effective plan to minimize downtime of key processes in the event of a major disruption.
Emphasis	Technology	Processes	People
Focus	Proactive and Preventive		Response and Recovery

Figure 2: Description of the BCM process.

- Documentation requirements.
- Testing, approvals, project management and oversight requirements.
- Project risk assessments.

Ideally, service organizations are expected to maintain evidence that demonstrates the procedures below are followed for all new developments and acquisitions, as they may have a direct impact on the delivery of client services. Key methodology components include:

- IT project definition and project management.
- Systems analysis.
- Software design, programming, documentation, testing, releases, and updates.
- Infrastructure planning.
- Design changes during development.
- IS clearance procedures.
- Code reviews.
- Data migration procedures.
- End-user training.

## 4. Change Management Control Considerations

Application maintenance addresses ongoing change management activities and the implementation of new software releases. Appropriate system controls should exist to make sure all changes are made properly. Controls may involve the use of authorizations of change requests, reviews, approvals, documentation, and testing, as well as assessments of changes on other IT components and implementation protocols.

The change management process also needs to be integrated with other IT processes, including incident management, problem management, availability management, and infrastructure change control. From an audit standpoint, the service provider must be able to provide evidence that changes are based on authorized requests only.

## 5. Human Resource Policies and Procedures

Successful outsourcing depends on technology and people. Therefore, an evaluation of the vendor's HR policies and procedures is important in the successful implementation and operating effectiveness of designed controls. Key review considerations in this area include:

- Adoption and promotion of the company's integrity management culture, including the organization's ethics, business practices, and HR evaluations.
- Reviews of employee incentives to ensure employees are not pressured to use unethical or unfair practices to meet unrealistic performance targets, particularly for short-term results.
- Use of adequate hiring practices, such as specification of job requirements, job posting procedures, handling of employment applications, interviews, background checks, job offers, and new employee orientations.

- Capturing, analyzing, and reviewing employee turn-over patterns for potential fraud or collusion.

## 6. Internal Audit Considerations

In the beginning, many organizations were reluctant to outsource their services due to fears of losing control. Because of this, a strong outsourcing control environment is especially important on the service provider side. The control aspects discussed in this chapter need to be understood and evaluated in all third-party processes based on the kind of services being outsourced and their complexity.

The internal auditor plays a critical role in evaluating the service provider's control environment. As a result, auditors need to assess the strength of the control framework and control activities affecting the outsourced processes, as well as inform management on the effectiveness of outsourcing operations from a compliance and operations standpoint. To do so, auditors should evaluate and test the service provider's policies, procedures, guidelines, risk assessments, and SDLC control monitoring activities, as well as obtain independent information through the established communication channels. Auditors also can rely on the international standards adopted by the service provider for compliance, such as the use of SAS 70 reports, and evaluate the service provider's documentation to identify whether controls were customized to fit the client's unique environment.

# GTAG – IT Outsourcing – A Few Applicable Control Frameworks and Guidelines – 6

When outsourcing an IT solution, companies face the risk that sensitive customer data may end up in the service provider's custody. Loss of data confidentiality and integrity, as well as unauthorized use and tampering of customer data, could lead to penalties and reputation loss. Data breaches also could result in security and privacy violations as indicated by regulations such as HIPAA, GLBA, and the EU's Data Protection Act, depending on the company's type of work and country of operations.

Although different frameworks can be adopted to oversee the effectiveness of outsourced activities, the contract remains the most important framework in reviewing a service provider's work and compliance. Below is a description of the main regulations service providers and organizations alike need to keep in mind or comply with throughout the duration of the outsourcing partnership.

## Compliance Standards

### a) HIPAA

HIPAA applies to U.S. organizations working in the health-care industry. Compliance with HIPAA is mandatory for all electronic health transactions, such as claims, enrollment forms, payments, and coordination of benefits. The standard also addresses the security and privacy of electronic health information systems and data, including policies and procedures for:

- Securing the privacy of electronic information.
- Preventing unauthorized access to and disclosure of health-care information.
- Maintaining audit trails in computerized record systems.

Service providers that provide IT services to organizations in the health-care industry must comply with HIPAA. To comply with the regulation, the service provider should ensure that:

- Standard training contents are designed to incorporate key compliance requirements. In many cases, training content is made available by the client directly.
- Service employees working on the account are trained on the relevant sections of the standard.
- The work area and network used for processing health-care information is held in a separate location to prevent unauthorized access to the client's data.
- Network security and controls are implemented for securing data transmissions, including the use of separate tunneled networks, firewalls, and proxy settings that:
  - Define access and traffic rules.
  - Enable encryption.
  - Control access based on defined rules.
  - Maintain logs, reviews, and incident management procedures for reported violations.

### b) GLBA

This act applies to financial institutions that provide financial products and services to consumers, such as:

- Lending, brokering, or servicing any type of consumer loan.
- Transferring or safeguarding money.
- Preparing individual tax returns.
- Providing financial advice or credit counseling.
- Offering real estate settlement services.
- Collecting consumer debts.

If any IT services are outsourced by a financial institution, the service provider must comply with the act's requirements. In addition to getting the proper training and education on the act's requirements, the service provider should ensure that:

- The work area and network used for processing the financial information is held in a separate location to prevent unauthorized access.
- Data processing and storage security measures are implemented. This includes restricting the use of mobile devices (e.g., mobile phones, cameras, and personal digital assistants), external storage devices (e.g., compact disks and flash drives), and output devices (e.g., printers and fax machines) to prevent unauthorized transmission of data and records.
- Network security and controls are implemented for securing data transmissions, including the use of separate tunneled networks, firewalls, and proxy settings that:
  - Define access and traffic rules.
  - Enable encryption.
  - Control access based on defined rules.
  - Maintain logs, reviews, and incident management procedures for reported violations.

### c) Additional Regulations

To ensure the protection of data, the most accepted standards are the UK's Data Protection Act 1998 and the related EU Directive on Data Protection (95/46/EC). The UK's Data Protection Act lays down provisions that discuss how to process personally identifiable information, such as obtaining, holding, using, or disclosing such information. The security requirements to be practiced by the service provider for compliance are the same as those described above for HIPAA and GLBA.

## Other Available Frameworks and Guidelines

Organizations that outsource services to a third party need assurance that the service provider's governance structure and controls framework can ensure the confidentiality, integrity, and availability of their data and systems, which can be accessed by the service provider's personnel. One measure

to ascertain the efficiency of the processes used is to examine whether they are certified by a recognized international standard, such as the International Standards Organization (ISO), International Electrotechnical Commission (IEC) 2700 Standard, Six Sigma, the Customer Operations Performance Center Inc., British Standard (BS) 7799, and the Capability Maturity Model from Carnegie Mellon University's Software Engineering Institute (SEI).

Periodic reviews and monitoring of the service provider's policies and procedures and internal controls framework can be performed by a specialized team from the outsourcing company, such as an internal audit group. However, due to the impact of Sarbanes-Oxley and similar legislation, many organizations are starting to use the services of external auditors and other third parties to conduct assessments of the service provider's work and efficiency of internal controls. These independent reviewers also provide independent assessments that can be used by the service provider and its audit team.

When an organization uses a service organization, transactions affecting the client's financial statements are subject to controls that may be physically or operationally separated from the client. The significance of the service provider's controls to those of the client depend on the nature of the outsourced services, the nature and materiality of the transactions processed, and the degree of interaction between the client's activities and those of the service provider. Controls placed in operation by the client organization and the service provider need to be assessed to identify potential misstatements and to design control tests.

Like their clients, many service providers are getting certified in different frameworks and are complying with different standards to gain acceptance in the international arena. Compliance displays a commitment to providing high-quality services, which also helps to distinguish service providers during the vendor selection process. Because certification has to be maintained once achieved, certified organizations demonstrate their commitment to maintaining high-service standards that are in line with the framework's compliance requirements. Following are some of the most acceptable frameworks and guidelines available for testing and assessing the effectiveness of controls.

## a) SAS 70

SAS 70 is an audit standard developed by the American Institute of Certified Public Accountants (AICPA). The standard allows service providers to obtain independent assurance on their control objectives and control processes. SAS 70 is generally used by auditors reviewing the financial statements of an organization that obtains services from another organization.

SAS 70 does not include a pre-determined set of control objectives or activities for service organizations to achieve. Rather, affected parties must negotiate the control objectives to be included in the SAS 70 report. Please note that as the service provider grows in size, the more difficult it becomes for the service organization to tailor its pre-existing SAS 70 report to meet the needs of the client organization.

## SAS 70 Reports

The SAS 70 report is best known for the Service Auditor's Report that is issued to the service organization at the conclusion of the SAS 70 by an independent auditor, which provides a description of the service provider's controls. The Service Auditor's Report is also one of the most effective ways a service organization can communicate information about its controls. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service provider's controls at a specific point in time (e.g., as of June 30, 2006). A Type II report describes the service provider's controls and includes detailed testing information of the third party's controls over a minimum six-month period (e.g., from July 1, 2006 to December 31, 2006). Under Sarbanes-Oxley, a Type II report has become the de facto requirement, given the need to evaluate both the design and operational effectiveness of internal controls under Auditing Standard No. 2.

In 2006, the Institute of Chartered Accountants in England and Wales released AAF 01/06: Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties. AAF 01/06 is similar to SAS 70 and guides accountants responsible for providing assurance on a service organization's internal controls.

## b) SysTrust®

The SysTrust® assurance service was developed by the AICPA and the Canadian Institute of Chartered Accountants. Its focus is to increase the confidence of management, customers, and business partners in systems that support an organization or a particular activity.

The SysTrust® service outlines different criteria that can help organizations provide assurance on the service reliability of their systems. These criteria include:

- Availability (i.e., a system must be available for operation and use at times set forth in service-level agreements).
- Security (i.e., a system needs to be protected against unauthorized physical and logical access).
- Processing integrity (i.e., system processing must be complete, accurate, timely, and authorized).
- Maintainability (i.e., systems can be updated when required in a manner that continues to provide for availability, security, and integrity).

# GTAG – IT Outsourcing – A Few Applicable Control Frameworks and Guidelines – 6

Each of the principles and related criteria are organized into four review areas:

- Policy (i.e., the organization needs to define and document policies relevant to the particular principle).
- Communications (i.e., the organization needs to communicate defined policies to authorized users).
- Procedures (i.e., the organization needs to use procedures to achieve its objectives in accordance with its defined policies).
- Monitoring (i.e., the organization needs to monitor the system and take action to maintain compliance with defined policies).

The objective of SysTrust® is to help independent auditors assess management's administration of controls that relate to SysTrust® services. The auditor's role is to determine whether system controls exist and perform tests to determine whether these controls are operating effectively during the period covered by the report.

## c) BS 7799 and ISO/IEC 27001

BS 7799 was first issued in 1995 to provide a comprehensive set of controls comprised of information security best practices. The standard's objectives are to protect the confidentiality, integrity, and availability of information, the essence of information security.

While similar to BS 7799, ISO/IEC 17799: 2000 Information Security Management was developed by a group of information security practitioners from different industries. The standard provides information security best practices that should be considered and implemented where appropriate by all organizations regardless of size. Certification of BS 7799 is issued in two parts:

- Part 1: Code of Practice for Information Security Management.
- Part 2: Specification for Information Security Management Systems.

BS 7799-1:1999, or Part 1, has been ratified as the international security standard used in ISO/IEC 17799. It focuses on the protection of an organization's information and the mechanisms for creating, editing, transmitting, and storing information. The standard has two stated objectives:

- To provide an objective means of measuring and comparing best practices in information security management.
- To promote confidence in electronic inter-company trading.

BS 7799-2: 2002 Specification for Information Security Management Systems, or Part 2, was developed later to help organizations prepare themselves properly for accredited certification against BS 7799. Both Part 1 and Part 2 are considered to be a comprehensive collection of information security

best practices that provide organizations with a measuring stick by which to evaluate their security and controls environments.

The certification body, known as the United Kingdom Accreditation Service or UKAS, issued a transition statement from BS 7799-2: 2002 to ISO/IEC 27001. Accredited organizations should consider transitioning to ISO/IEC 27001 by July 2007.

In 2005, ISO and IEC issued Standard 27001: 2005, which replaced BS 7799-2: 2002. The new standard is an expanded and adapted version of BS 7799-2 and specifies the requirements for IS management system certification. Among its distinctive features, the new standard introduced a new domain for security, known as information security incident management and a total of 17 new controls.

## d) Control Objectives for Information and Related Technology (CobIT)®

IT Governance Institute (ITGI) CobIT framework lays down a set of control objectives for effective IT governance. CobIT also helps organizations implement the necessary requirements to ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information. CobIT IT processes are defined under four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

Control objectives and processes are defined for each of the four domains, which can be adopted as best practices for designing an effective framework. Specifically, CobIT provides maturity models for control over IT processes so that management can map its current control maturity levels, where it stands in relation to best-in-class organizations, and where the organization wants to be. Maturity models describe:

- i. Critical success factors that define important management-oriented implementation guidelines to achieve control over and within its IT processes.
- ii. Key goal indicators, which define measures that enable management to identify whether an IT process has achieved its business requirements.
- iii. KPIs that serve as lead indicators on how well the IT process is enabling goals to be reached.

## e) The UK Office of Government Commerce's (OGC's) IT Infrastructure Library (ITIL)

Another global framework on IT governance and management is ITIL, an IT operations and services best practice framework that helps organizations align their business and IT activities. The OGC developed ITIL in the mid-1980s for companies seeking to manage their IT environments more efficiently. One of the main reasons ITIL is used by many organizations is due to its freedom. ITIL does not mandate organizations to implement all framework specifications.

ITIL's Service Support book helps organizations define their core IT service functions. According to the book, the role of an IT service function is to offer uninterrupted and best possible services to users. The book also defines five processes: incident management, problem management, configuration management, change management, and release management, which describe how to manage software, hardware, and HR services efficiently and ensure continued and uninterrupted business activities.

## Internal Audit Considerations

As outsourcing continues to evolve into a more global service delivery model, it is important for internal auditors to keep abreast of the control frameworks used worldwide. This allows auditors to make informed decisions on which frameworks are best suited to meet the needs of client organizations based on their type of work, the activities being outsourced, and the different kinds and levels of risks. Internal auditors also are playing a key role in the recommendation and evaluation of different IT control frameworks and the options available for deployment.

As a result, internal auditors need to assess the efficiency of the certifying organization's review processes and design an audit program that caters to the specific framework under evaluation. Audit results will help client organizations determine how much they can rely on the service provider's activities based on the certification obtained.

Factors that need to be considered when evaluating the effectiveness of the review process and certification include:

1. The reputation and competency of the organization that conducted the review and provided the certification.
2. The review's period of coverage (i.e., the review period should be current and within the client's financial period).
3. The control framework defined (i.e., the control, objectives, and control processes should cover the IT processes and operations outsourced, as well as include the controls desired by the client and mandated by regulatory requirements).
4. Review results (i.e., the efficiency of the control design in meeting the objectives and operating effectiveness of the controls over the period under review). Review results need to note any exceptions, the risk rating of exceptions based on their impact, management's response, and the time committed by management for implementing remedial measures. For high-risk exceptions, audit reports need to document the remediation measures implemented to ensure program effectiveness.

## Top 10 Questions CAEs Should Ask

1. Are the services outsourced significant to the client?
2. Does the client have a well-defined outsourcing strategy?
3. What is the governance structure relating to outsourced operations? Are roles and responsibilities clearly defined?
4. Was a detailed risk analysis performed at the time of outsourcing, and is a regular risk analysis being done?
5. Do formal contracts or SLAs exist for the outsourced activities?
6. Does the SLA clearly define KPIs for monitoring vendor performance?
7. How is compliance with the contract or SLA monitored?
8. What is the mechanism used to address non-compliance with the SLA?
9. Are the responsibilities of the ownership of data system, communication system, operating system, utility software, and application software clearly defined and agreed upon with the service provider?
10. What is the process for gaining assurance on the operating effectiveness of the internal controls on the service provider's end?

## GTAG – Recent Trends and the Future of Outsourcing – 7

Although IT outsourcing is an established management practice, ongoing and rapid industry changes have established the presence of trends. Below are some of the most noteworthy trends in the IT outsourcing arena.

- Application development continues to be one of the most outsourced IT activities followed by application maintenance and support. This trend is expected to continue in the near future. Service providers are continuing to build their skills and capacity in this area and hold high expectations for growth in the managed services category, particularly in the areas of database management and network management.
- Mega deals in excess of US \$1 billion represent a significant share of the total outsourcing contract value, which averaged US \$25.3 billion per year between 2003 and 2005. However, mega deals are set to decline in the near future and will be replaced by an increase in mid and large deals in the US \$100 million to US \$999 million range<sup>1</sup>. This trend is expected to create increased competition in the service provider arena, as both large and mid-size players start to face direct competition from each other.
- Although there has been an increased emphasis on the outsourcing partnership model, contract term lengths are declining. Research indicates that the average length of an IT outsourcing contract declined from 6.2 years to 5.3 years from 2003 through 2005. This is attributed to negative vendor experiences from first-generation outsourcing deals that were implemented in a hurry to bring in tactical cost reductions. The trend is to give organizations flexibility and not lock them into a particular service.
- Cost savings continues to be the key driver for IT outsourcing. However, the importance of superior technical skills to improve quality is rising rapidly. This may be corroborated by a growing number of clients using outsourcing as a way to introduce innovation into their organizations. This change in relative importance may be attributed to increased consensus on real cost savings estimated between 15 and 25 percent. Outsourcing arrangements that have focused solely on delivering savings have failed to meet client and service provider expectations.
- Europe will continue to witness significant activity in IT outsourcing and will come close to catching up with the U.S. market share. India will continue to

be the most preferred destination for IT outsourcing, although China is expected to emerge as a formidable competitor in the future.

- Many companies are relying on pilot projects to ensure a good fit between the client organization and vendor. Pilots allow companies to review the vendor's project management process for efficiency and effectiveness. Specifically, the pilot looks at whether project execution is completed within established guidelines, deliverables are timely, and the vendor has adhered to defined quality standards. Pilot projects serve as an excellent way for organizations to check facts before making a final vendor decision. They also let companies experience the benefits of outsourcing before jumping into a long-term relationship. Often, companies will conduct a proof of concept with various vendors to compare results and choose the best vendor.
- Multi-sourcing will be one of the most visible trends. As a result, organizations will need to develop the competencies necessary to manage a multi-vendor environment.
- IT service providers will evolve their businesses around distinct models including:
  - The global champion model. Under this model, the service provider can offer multiple service lines and solutions to large organizations.
  - The IT specialist model. Under this model, service providers focus on three to four major IT industry or cross-industry services.
  - The ADM factory model. Under this model, service providers can position themselves as low-cost developers of applications and maintenance services.

Service providers will have to bring innovation into their business models by focusing on new service lines, such as infrastructure outsourcing. In addition, service providers will need to increase their knowledge domains and enhance the quality of their business environments by providing better services with better technological solutions.

<sup>1</sup>Gartner Research: *Market Trends—Outsourcing Contracts, Worldwide* (2005)

**Agreed-upon procedures (AUP):** In an AUP, a professional services firm is hired to provide a report on a specific activity. AUPs differ from audits because in an audit, the auditors issue opinions based on their findings.

**BS 7799:** The British standard for information security management, which provides a comprehensive set of controls consisting of information security best practices.

**Capability Maturity Model (CMM):** Developed by the Carnegie Mellon University's SEI in the mid-1980s, CMM is a collection of instructions an organization can follow with the purpose of gaining better control over its software development processes. The CMM ranks software development organizations in a hierarchy of five levels, each with a progressively greater capability of producing quality software. Each level is described as a level of maturity and has different instructions to follow.

**Control Objectives for Information and related Technology (CobIT®):** A set of best practices for IT management created by ITGI.

**Customer Operations Performance Center Inc. (COPC):** The world's leading authority on operations management and performance improvement for buyers and providers of customer contact centers and business process outsourcing (BPO) services. The COPC® Performance Management System includes operational certification programs, operational management training, Six Sigma in contact centers, performance improvement consulting, and vendor sourcing and management services.

**Full-time equivalent (FTE):** A way to measure an employee's productivity or involvement. An FTE of 1.0 means that a person is equivalent to a full-time employee while an FTE of 0.5 indicates that an employee's work hours or projected output is only half of that of a full-time employee.

**Integration testing:** Sometimes called integration and testing, this is the phase of software testing in which individual software modules are combined and tested as a group. Integration testing takes evaluated unit modules and groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers an integrated system that is ready for system testing.

**Multi-sourcing:** The management and distribution of different business processes among multiple vendors. One of its key objectives is to mitigate risks by eliminating the need to lock-in with a particular vendor.

**Regression testing:** Any type of software testing that seeks to uncover regression bugs, which occur whenever software

functionality that previously worked as desired stops working, or no longer works in the same way. Typically, regression bugs occur as an unintended consequence of program changes. Common methods of regression testing include running previously used tests and determining whether previously fixed faults have re-emerged.

**Request for information (RFI):** An RFI provides the information needed to complete first-round vendor evaluations. Organizations generally use the RFI to validate vendor interest and to evaluate the business climate in the organization's industry. As opposed to a highly specific formal request for proposal, the RFI encourages vendors to respond freely. It also spells out the business requirements defined by the core team so the vendor understands what the company is trying to accomplish.

**SAS 70:** An internationally recognized audit standard developed by the AICPA. A SAS 70 examination signifies that a service organization had its control objectives and activities assessed by an independent accounting and audit firm.

**Service-level agreement (SLA):** A core concept of IT service management, an SLA is a formal written agreement made between two parties: the service provider and the service recipient. The SLA defines the basis of understanding between the two parties for delivery of the service. The document can be quite complex and sometimes underpins a formal contract. Although SLA contents vary according to the nature of the service itself, they usually include a number of core elements or clauses that define a specific level of service, support options, incentive awards for service levels exceeded, or penalty provisions for services not provided.

**Transmission control protocol (TCP)/Internet protocol (IP):** A set of communication protocols that implement the protocol stack on which the Internet and most commercial networks run. It is sometimes called the TCP/IP protocol suite.

**The IT Infrastructure Library (ITIL):** A best practices framework that facilitates the delivery of high-quality IT services. ITIL outlines an extensive set of management procedures intended to help organizations achieve quality and value for money in IT operations. These procedures are supplier-independent and are developed to provide guidance across different IT infrastructures, developments, and operations.

**The International Organization for Standardization (ISO):** An international standard-setting body that consists of representatives from different industry groups. Founded on Feb. 23, 1947, ISO produces worldwide industrial and commercial standards — the so-called ISO standards.

## GTAG – Glossary of Terms – 8

---

**The U.S. Gramm-Leach-Bliley Act (GLBA) of 1999:** This legislation, which repealed the U.S. Glass-Steagall Act of 1933, opened up competition among banks, securities companies, and insurance companies. While the Glass-Steagall Act prohibited a bank from offering investment, commercial banking, and insurance services, GLBA allows commercial and investment banks to consolidate their services. For example, in its wake, Citibank merged with Wall Street firm Salomon Brothers and eventually became the capital conglomerate Citigroup.

**The U.S. Sarbanes-Oxley Act of 2002:** A federal law passed in response to a number of major corporate and accounting scandals involving prominent companies in the United States. The legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. The act, which contains 11 titles or sections ranging from corporate board responsibilities to criminal penalties, requires the U.S. Securities and Exchange Commission to implement rulings on requirements to comply with the law.

## Authors



**Mayurakshi Ray** is a principal consultant with PricewaterhouseCoopers (PwC) India in the Governance, Risk, and Compliance (GRC) Practice. Ray has more than nine years of experience in the areas of IT risk management, IS and controls, and business process reviews. As part of the GRC, Ray has led a large number of SAS 70 and Sarbanes-Oxley engagements, including readiness advisory services and review and program management support to many offshore IT and BPO companies.

Ray also has extensive experience in the risk and controls area, where she has provided advisory services on internal control frameworks and IS activities, including the review of standalone applications, packaged services, and enterprise resource planning (ERP) solutions; corporate governance and IT process improvement; IS security policy frameworks; and reviews of high-data migration security, IT due diligence, and third-party assurance.

Ray is part of the BS 7799-2: 2002 implementation and certification core team in the PwC Salt Lake Technology Center in Kolkata, India. She is trained in the functional aspects of ERPs, IS risks and controls, and Sarbanes-Oxley requirements. She has a degree in economics and is a chartered accountant and qualified BS 7799 lead auditor.



**Parthasarathy Ramaswamy** is a principal consultant with PwC India in the GRC Practice. Ramaswamy has more than 10 years of experience in the areas of enterprise risk management, performance improvement, cost reduction, activity-based costing, and operational reviews. He has managed Sarbanes-Oxley projects and provided clients with readiness advisory support. His advisory services have focused on IT general computer controls and automated business process controls.

Ramaswamy also has worked as lead functional consultant while managing large ERP implementations and providing offshoring advice to large US-based clients. Ramaswamy is a chartered and cost accountant, a licensed company secretary, a member of the UK's Chartered Institute of Management Accountants, and holds a master's degree in economics.



Advisor, **Jaideep Ganguli**, is a partner with PwC India and leads the GRC and Finance Function Effectiveness practices, where he advises clients on performance improvement initiatives in the finance domain and provides core advisory services in governance, risk, and compliance-related matters. Jaideep has 15 years of experience in the areas of financial management solutions, enterprise applications, internal controls, and business transformation.

He has directed a large number of Sarbanes-Oxley readiness advisory and SAS 70 engagements for many offshore IT and BPO companies. His experience in the risk and controls domain includes advisory engagements for internal controls framework, corporate governance, enterprise risk management frameworks, risk and controls assessments, and third-party assurance reviews.

Jaideep is also India's IT effectiveness leader and has extensive ERP experience. He has directed some of the largest ERP implementation projects in India. Jaideep managed PwC's global rollout of Oracle Financials from the firm's technology center in Tampa, Fla. He also played a key role in developing the firm's Oracle implementation initiative. He was the project director for PwC India's own billing and invoicing solution deployment.

Jaideep is a chartered accountant and has been with PwC since 1991.

## GTAG – Contributors and Reviewers – 10

### Contributors

Madhu Arora, PricewaterhouseCoopers India  
Deepa Seshadri, PricewaterhouseCoopers India

### Reviewers

The following organizations were part of the review process:

- The IIA's Advanced Technology Committee
- The IIA global affiliates
- AICPA
- Center for Internet Security
- Carnegie Mellon University's SEI
- The Information System Security Association
- IT Process Institute
- National Association of Corporate Directors
- SANS Institute

The IIA thanks the following individuals and organizations who provided valuable comments and added great value to this guide:

- AICPA's IT Executive Committee
- IT Audit in Banks Committee, The IIA-Germany
- IT Auditing Speciality Group, The IIA-Norway
- The technical committees of The IIA-UK and Ireland
- Frank Alvern, IIA Norway and Nordea
- Ken Askelson, JCPenney, USA
- Kjetil Berg, OAG Norway
- Lily Bi, The IIA
- Anders Blix, EDB, Norway
- Larry Brown, The Options Clearing Corp., USA
- Claude Cargou, AXA, France
- Faisal R. Danka, Ernst & Young LLP, London, UK
- Reiner Eickenberg, WestLB AG, Duesseldorf, Germany
- Lars Erik Fjortoft, KPMG, Norway
- Terje Graesmo, Nordea, Norway
- Christian Grill, DAB Bank AG, Munich, Germany
- F.M. Hallinan, Chevron Phillips Chemical Co. LLP, USA
- Alf Martin Hansen, Statsbygg, Norway
- Rune Johannessen, OAG Norway
- Juergen Maerz, SEB AG, Frankfurt, Germany
- Steve Mar, Microsoft Corp., USA
- Otto Reimer, Sparkassen-u. Giroverband Hessen-Thueringen, Frankfurt, Germany
- Paula M. Stockwell, IBM Corp., USA
- Stig J. Sunde, OAG Norway
- Jay R. Taylor, General Motors Corp., USA
- Hajime Yoshitake, Nihon Unisys, Ltd., Japan

Billions of dollars are spent every year globally on implementing new or upgrading existing business application systems. Appropriate controls in each application system become vital to help an organization achieve its business objectives. The objective of application controls is to ensure that:

- All input data is accurate, complete, authorized and correct.
- All data is processed as intended in the correct time period.
- All data stored is accurate and complete.
- All output is accurate and complete.
- A record is maintained to track the process of data from input to storage and to the eventual output.

Due to the importance of application controls to risk mitigation strategies, it is important for the chief audit executive (CAE) and his or her team to develop and execute audits of these application controls on a periodic basis in order to determine whether they are designed and operating effectively.

The next publication for CAEs in the Global Technology Audit Guide (GTAG®) will deal with auditing application controls. The objective of GTAG 8 is to provide direction to CAEs regarding:

- What application controls are.
- The internal auditor's role in auditing application controls.
- How to scope various types of application audits including various approaches and considerations.
- Risk assessment and control identification.
- Benefits of relying on application controls.
- Methods for conducting an application controls review.

To further assist CAEs or other individuals who use this guide, we have also included a list of key application controls, a sample audit plan, and a list of some application control review tools.

## GTAG – Sponsor Bio – 12

---

PricewaterhouseCoopers (PwC) provides a broad range of solutions to assist internal audit departments when companies are considering offshoring or outsourcing their Information Technology Operations. Our services can help companies improve internal audit performance and strengthen internal control, risk monitoring and strategic risk management capabilities. We offer insights. We answer the tough questions. We get it done. For more information, please visit us at [www.pwc.com/internalaudit](http://www.pwc.com/internalaudit).

Email: [pwc.internal.audit@us.pwc.com](mailto:pwc.internal.audit@us.pwc.com)

# the importance of making IT outsourcing part of your business plan.\*

Organizations considering offshoring or outsourcing their IT processes need to understand the internal control implications of these decisions.

PwC has significant experience in assisting internal auditors and their organizations to address these issues. Our skills extend globally in areas such as risk management, business operations, technology, human resources, tax, finance, change, and program management.

The right sourcing decisions, implemented in a measured risk and control environment, can improve your business in dozens of ways.

PricewaterhouseCoopers can show you how.  
Visit [www.pwc.com/internalaudit](http://www.pwc.com/internalaudit)

\*connectedthinking

PRICEWATERHOUSECOOPERS 



## What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Guide 1: *Information Technology Controls*

Guide 2: *Change and Patch Management Controls: Critical for Organizational Success*

Guide 3: *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*

Guide 4: *Management of IT Auditing*

Guide 5: *Managing and Auditing Privacy Risks*

Guide 6: *Managing and Auditing IT Vulnerabilities*

Check The IIA technology Web site at [www.theiia.org/technology](http://www.theiia.org/technology)

Order Number: 1027

IIA Member US \$25

Nonmember US \$30

IIA Event US \$22.50



[www.theiia.org](http://www.theiia.org)

07227

