CHAPTER 14

Auditing Cloud Computing and Outsourced Operations

In this chapter, we will discuss key controls to look for when you are auditing IT operations that have been outsourced to external companies, including the following:

- Definitions of cloud computing and other forms of IT outsourcing
- SAS 70 reports
- Vendor selection controls
- Items to include in vendor contracts
- Data security requirements
- Operational concerns
- Legal concerns and regulatory compliance

Background

The concept of outsourcing IT operations to external service providers is not a new one. Companies have been implementing this concept for years, from hosting their applications via an application service provider (ASP), to storing their computer equipment in a co-location data center (also called a *colo*), to hiring an external company to run their IT operations. The decision to outsource operations is usually based on a desire to reduce costs and to allow a company to focus on its core competencies. In other words, if I own a company that makes hockey sticks and my core competency is designing and building those hockey sticks, I might not want to invest the time and money required to run a data center to support my operations. It's expensive and it's not what I'm good at. Instead, I can pay someone who runs data centers for a living to do that for me. They can probably do it better than I could and at a lower cost, and it allows me to focus on those hockey sticks.

Recently, a new concept has been introduced into the outsourced operations world called *cloud computing*, where IT services are provided through the Internet (that is, the cloud) using shared infrastructure. This has resulted in a new trend of companies moving their IT services to external providers.

Although outsourced operations can provide benefits to a company in terms of cost and resource efficiency, they also introduce additional risks, as the company gives up control over its data and IT environment.

The methods used for outsourcing IT operations can be defined, separated, and categorized in multiple ways. None of those methods will be perfect or all-encompassing, but for the purposes of this chapter, they are divided into two major categories:

- IT systems and infrastructure outsourcing
- IT service outsourcing

IT Systems and Infrastructure Outsourcing

IT systems and infrastructure outsourcing is the practice of hiring another company to provide some or all of your IT environment, such as data center, servers, operating systems, business applications, and so on. This service can be provided using either cloud computing or dedicated hosting.

Cloud Computing

As a relatively recent trend, the industry is still settling on the definitions of cloud computing. Gartner defines it as "a style of computing that provides scalable and elastic, IT-enabled capabilities 'as a service' to external customers via Internet technologies." The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Basically, cloud computing provides IT services over the Internet in such a way that the end user doesn't have to worry about where the data is being stored, where the infrastructure is located, and so on. The user receives the service without worrying about any of the details of how it's provided. Also, as a consumer of cloud computing, you are sharing the backend infrastructure that provides the service with other users; it is not dedicated to you and your company. This is analogous to the utilities you use at home. You don't know or necessarily care how you get your electricity; but you do care that it works. You let the electric company worry about what it takes to provide the service. And you don't have your own dedicated infrastructure at the electric company; you share it with all of your neighbors. Also, just like with your electricity at home, you pay for only what you use with cloud computing.

On a personal level, you've likely experienced cloud computing at home. If you have a personal e-mail address with a provider such as Yahoo! or Gmail, you are receiving your e-mail in the cloud. You don't know and don't care where your data is stored and what sort of infrastructure is being used to provide the service to you. All you care about is that you can send and receive e-mail and manage your contacts. Also, you do not have a dedicated e-mail server on the backend; many other e-mail accounts are on the same server as yours. As to how many there are and who they are, you don't know and don't care. All you know and care about is that your e-mail is available and secure.

Cloud computing at the corporate level expands on this concept, resulting in enterprise business applications, client (PC) applications, and other aspects of the IT environment being provided over the Internet using a shared infrastructure.

A number of attempts have been made to determine what truly defines something as cloud computing, but we'll use the NIST definition here. According to NIST, for something to qualify as cloud computing, it must exhibit five characteristics:

On-Demand Self-Service This means that you can provision computing capabilities, such as storage, as needed automatically without requiring human interaction with each service's provider. It also implies that the implementation details are hidden from (and irrelevant to) the consumer. For example, the customer need not worry about what storage technology is used, but simply needs to define their business requirements and let the service provider determine how those requirements will be met.

Broad Network Access This means that capabilities should be accessible from anywhere and from any device (such as laptops and mobile devices) as long as Internet connectivity is available.

Resource Pooling This means that the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. It provides a sense of location independence in that the customer generally has no control over or knowledge of the exact location of the provided resources. Examples of resources in this context include storage, processing, memory, network bandwidth, and virtual machines.

Rapid Elasticity This means that capabilities can be rapidly and elastically provisioned (often automatically) to scale out quickly, and rapidly released to scale in quickly. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service This means that cloud systems automatically control and optimize resource usage by leveraging metering capabilities appropriate to the type of service (such as storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the service. This also implies transparency in cost, allowing the consumer to know that he is paying for only what he is using.

If a service your company is procuring does not meet those five criteria, it is likely not truly using cloud computing, but is instead using some form of dedicated hosting (discussed later in this chapter).

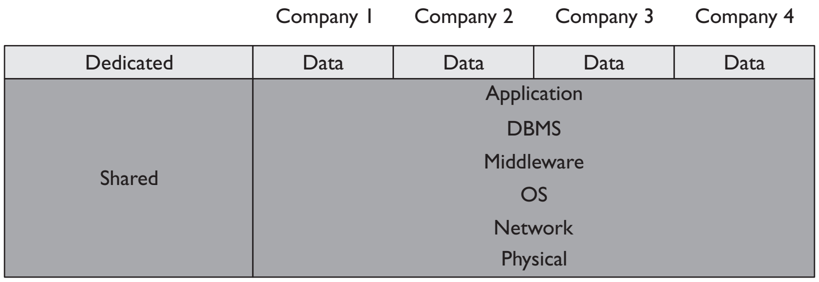
Cloud computing appeals to companies because it allows them to avoid the investment in physical infrastructure (and the operations for managing that infrastructure) and instead rent infrastructure (hardware and software) from another company, paying for only the resources they use.

The next important concept to understand is the three primary models of cloud computing. The classifications of these three models have been relatively broadly accepted, but once again we'll lean on the NIST definitions.

Software as a Service (SaaS) In this model, you will access the cloud provider's applications, which are running on a cloud infrastructure. The applications are accessible from client devices through a thin client interface such as a web browser (for example, web-based e-mail). As the consumer, you don't manage or control the data center, network, servers, operating systems, middleware, database management system (DBMS), or even individual application capabilities (with the possible exception of limited user-specific application configuration settings), but you do have control over your data. Common examples of this form of cloud computing include salesforce.com, Google Apps, and Microsoft's Business Productivity Online Suite. Figure 14-1 shows a representation as to what layers of the infrastructure are dedicated to your company and what layers are shared with other customers in the SaaS model.

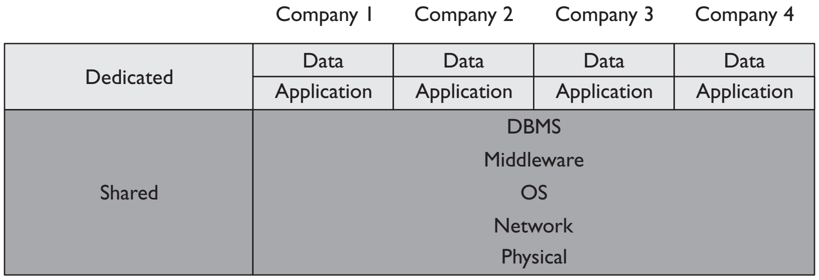
Platform as a Service (PaaS) In this model, you will deploy applications you created or acquired onto the provider's cloud infrastructure, using programming languages and tools supported by the cloud provider. As the consumer, you don't manage or control the data center, network, servers, operating systems, middleware, or DBMS, but you do have control over your data and the deployed applications and possibly application hosting environment configurations. Figure 14-2 shows a representation as to what layers of the infrastructure are dedicated to your company and what layers are shared with other customers in the PaaS model.

Infrastructure as a Service (IaaS) In this model, processing, storage, networks, and other fundamental computing resources are rented from the cloud provider. This allows you to deploy and run arbitrary software, which can include operating systems and applications. As the consumer, you don't manage or control the data center or network, but you do have control over your data and the operating systems, middleware, DBMS, and deployed applications. Figure 14-3 shows a representation as to what layers of the infrastructure are dedicated to your company and what layers are shared with other customers in the IaaS model.



	Company 1	Company 2	Company 3	Company 4
Dedicated	Data	Data	Data	Data
Shared	Application DBMS Middleware OS Network Physical			

Figure 14-1 SaaS model

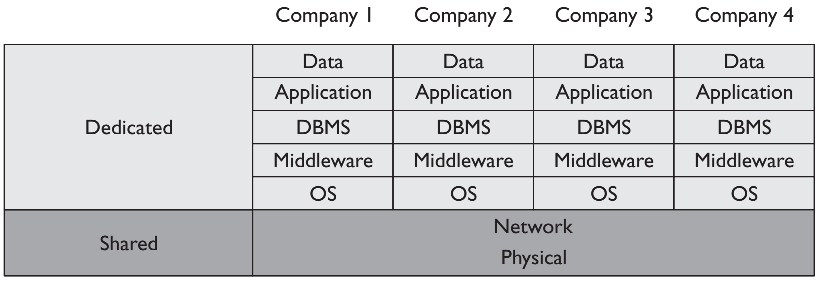


	Company 1	Company 2	Company 3	Company 4
Dedicated	Data	Data	Data	Data
	Application	Application	Application	Application
Shared	DBMS Middleware OS Network Physical			

Figure 14-2 PaaS model

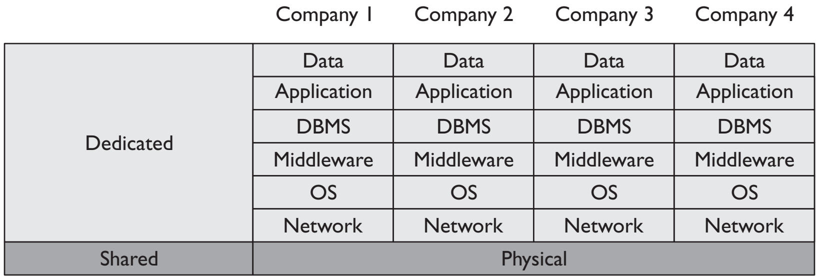
Dedicated Hosting

Dedicated hosting is conceptually similar to cloud computing, in that you're hiring someone else to provide (and probably manage) your infrastructure. The key difference is that, with dedicated hosting, your company will have dedicated infrastructure, potentially sharing no more than the physical layer with the vendor's other customers. An example of this would be a co-location (colo) data center, where you place your infrastructure (such as servers) in another company's data center, saving you the cost of building out and operating your own data center. Another example of this would be an application service provider (ASP) that hosts a business application for you, differentiated from SaaS only by the fact that you're on dedicated server(s) not shared with the vendor's other customers. In contrast, with cloud computing, your data will be segregated but you may be sharing the rest of the infrastructure (such as network, servers, middleware, and so on) with the vendor's other customers. Figure 14-4 shows a representation as to what layers of the infrastructure are dedicated to your company and what layers are shared with other customers in the dedicated hosting model.



	Company 1	Company 2	Company 3	Company 4
Dedicated	Data	Data	Data	Data
	Application	Application	Application	Application
	DBMS	DBMS	DBMS	DBMS
	Middleware	Middleware	Middleware	Middleware
	OS	OS	OS	OS
Shared	Network Physical			

Figure 14-3 IaaS model



	Company 1	Company 2	Company 3	Company 4
Dedicated	Data	Data	Data	Data
	Application	Application	Application	Application
	DBMS	DBMS	DBMS	DBMS
	Middleware	Middleware	Middleware	Middleware
	OS	OS	OS	OS
	Network	Network	Network	Network
Shared	Physical			

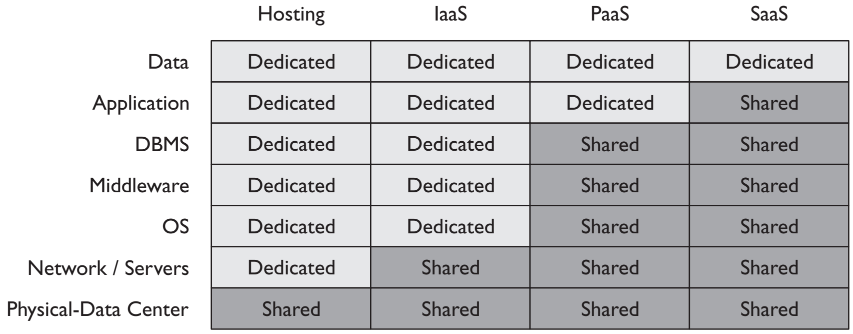
Figure 14-4 Dedicated hosting model

Although the concepts of what you need to protect may be the same between dedicated hosting and cloud computing, implementation will be vastly different. With dedicated hosting, you will look at how your network is isolated from other customers' (such as via firewalls). With cloud computing, you will look at how your data is segregated since you're sharing the infrastructure. With dedicated hosting, encryption within your isolated network area may not be important. With cloud computing, you will want to see your data encrypted end-to-end since it is comingled on the same infrastructure as other customers' data.

Because you're operating on dedicated infrastructure, dedicated hosting may not have the characteristics of cloud computing regarding on-demand self-service (the ability to provision additional capacity or other capabilities may not be automatic), broad network access (access may not be available via general Internet connections), resource pooling (you're on your own dedicated infrastructure), rapid elasticity (the ability to provision additional capacity or other capabilities may not be rapid, as procurement and setup time may need to be encompassed), or measured service (resource usage may not be automatically controlled and optimized).

There is often a fine line between whether you're using cloud computing or dedicated hosting. If you're not sure whether something is cloud or hosting, run a scenario by your provider. For example, tell them that you've just acquired another company and ask what it will take to scale the application to handle another 30,000 employees. If they say that they can handle it basically immediately, it's probably a cloud computing model. But if they say they need some time to expand your environment to accommodate the additional needs, it's probably dedicated hosting. This isn't a perfect test, as it will depend on your service provider and the amount of resources they have "on the bench" at the time, but it will give you a good indication.

Figure 14-5 shows a comparison of dedicated hosting and the three cloud computing models.



	Hosting	IaaS	PaaS	SaaS
Data	Dedicated	Dedicated	Dedicated	Dedicated
Application	Dedicated	Dedicated	Dedicated	Shared
DBMS	Dedicated	Dedicated	Shared	Shared
Middleware	Dedicated	Dedicated	Shared	Shared
OS	Dedicated	Dedicated	Shared	Shared
Network / Servers	Dedicated	Shared	Shared	Shared
Physical-Data Center	Shared	Shared	Shared	Shared

Figure 14-5 IT systems and infrastructure outsourcing model comparisons

NOTE Be aware that the definitions and distinctions among the various types of cloud computing and hosting are not always clear and are still maturing. Overlap can occur between these models and customizations (based on specific data protection requirements, cost constraints, and so on) can lead to hybrid models. Also, people do not always use the terminology consistently or accurately. You will often find people who, for example, say they are using SaaS when they actually have dedicated hosting of their application (or vice versa). The auditor needs to be familiar with the concepts and standard models but should also realize that real-world scenarios will not always be as neat and tidy as what is reflected here. Not everyone will agree on the same terminology and definitions, so don't get too caught up in semantics.

IT Service Outsourcing

IT service outsourcing is the practice of hiring another company to perform some or all of your IT operations functions (that is, hiring the company to provide the people and processes necessary to perform the function). Commonly outsourced operations include help desk operations and PC support. This can obviously go hand-in-hand with the outsourcing of IT systems and infrastructure. For example, if you have placed your IT equipment in another company's data center, you are also likely to hire that company to perform data center operation activities (such as tape operations, hardware support, and so on). Similarly, if you deploy cloud computing, it is a given that the cloud provider will perform the operations over the cloud infrastructure.

Two types of IT service outsourcing are available, on-site and off-site, though there are obviously hybrids of these models, where portions of the function are performed onsite and portions are performed offsite.

On-site

This model is used when a company outsources an operation but wants or needs for that function to be performed on company property. The external company is responsible for providing and training the people and establishing and monitoring the operational processes necessary for performing the function, managing all day-to-day aspects of the operation. However, the employees performing the function physically sit on the company's premises, using the company's network and IT environment.

Off-site

This model is used when a company outsources an operation without any on-site activity. Not only is the external company responsible for providing the personnel and processes necessary for performing the function, but they are also responsible for providing the facilities and infrastructure necessary for performing the function (often with connectivity back to the hiring company).

Other Considerations for IT Service Outsourcing

Additional topics related to IT service outsourcing are supplemental labor and offshoring.

Supplemental Labor

Many companies hire supplemental (contract) labor to assist in their day-to-day operations. This is often done to assist with short-term needs or to perform jobs that require workers with skills that are easy to find and replace. This sort of activity should not be confused with truly outsourced operations. Supplemental labor workers perform activities under the day-to-day guidance and direction of your company's staff and therefore are subject to the controls and security already established for the functions your employees are performing. This is vastly different from a function where day-to-day operations have truly been outsourced.

Offshoring

Many companies have moved IT functions to locations in the world that provide lower-cost resources. This can occur both with operations that have been outsourced as well as by hiring employees to work for your company in those lower-cost regions. Although sourcing operations from remote locations can provide significant cost benefits, it also presents unique internal control challenges and additional complexities into the environment, especially in the areas of coordination and communication.

IT Service Outsourcing Models

In summary, when it comes to staffing IT services, the following basic models are used:

- Internal employees only
- Internal employees plus supplemental labor
- Outsourced: on-site

- Outsourced: off-site
- Outsourced: on-site/off-site mix

For each of these provisioning models, the following deployment options are used:

- Onshore
- Offshore
- Onshore/offshore mix

SAS 70 Reports

When auditing vendors, you need to understand SAS (Statement on Auditing Standards) 70 reports. SAS 70 is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to deal with service organizations. It essentially provides a standard by which service organizations (such as those that provide IT services) can demonstrate the effectiveness of their internal controls without having to allow each of their customers to come in and perform their own audit. Without this standard, service organizations would expend a prohibitive volume of resources responding to audit requests from each customer. With this standard, service organizations can hire a certified independent service auditor (such as Ernst & Young) to perform a SAS 70 audit and issue a report. This report can in turn be presented to any customers requiring evidence of the effectiveness of the service organization's internal controls.

SAS 70 reports have become particularly important since the implementation of Section 404 of the Sarbanes-Oxley Act in 2002, as companies can use them as evidence of the effectiveness of internal controls over any aspects of financial processing and reporting that have been outsourced. Without them, any company providing financial services would be bombarded with Sarbanes-Oxley audits from all of their customers, as opposed to being able to hand each customer the same SAS 70 report.

SAS 70 service auditor reports are of two types: Type 1 and Type 2. Both types include a description of and opinion on the design of the service organization's internal controls at a point in time. However, only a Type 2 report contains the results of testing by the service auditor regarding whether the controls were operating effectively during the period under review to provide assurance that the control objectives were achieved. As an auditor, you will want your service providers to provide a Type 2 report, as Type 1 reports do not provide evidence that the controls are operating effectively.

For Sarbanes-Oxley purposes, it is also recommended that you influence your vendors to have their SAS 70 Type 2 audits performed with an end date of the examination period that falls within three months of the end of your fiscal year. Type 2 examinations are usually performed with an examination period of six to twelve months. So if the review period ends 6/30 and your fiscal year ends 12/31, the results will be six months' old by the time you use it for your certification. This is not ideal, but Sarbanes-Oxley guidance does provide directions for how to deal with it, so the report still has value.

Test Steps for Auditing Cloud Computing and Outsourced Operations

Here are a few notes on the test steps in this chapter.

First and foremost, whatever audit steps you would want to perform if the service were being performed by your company (that is, if it were not outsourced) should be considered when you're auditing an outsourced function. The same risks likely exist and will need to be mitigated. For example, if a business application is hosted in the cloud via SaaS, you will need to review for the sorts of application controls that are documented in Chapter 13. Those risks don't go away just because the application has been outsourced, and they are all still relevant to an audit program. However, the way you audit for them may be vastly different if the function has been outsourced.

Second, you need to determine whether you will be auditing the vendor and evaluating its controls or whether you will be auditing your own company and asking how it ensures that the vendor is providing the necessary controls. Both approaches are valid, and it may depend on what sort of right to audit and influence you have with the vendor. However, in general, it is preferable that you ask the questions of the vendor directly as opposed to using a middleman. You're more likely to get thorough and accurate answers. It's also sometimes interesting to ask the same question of both the vendor and your own internal IT team and compare their answers. This can tell you how well your company understands and reviews the controls over the outsourced operations.

Finally, for each step in this section, we will note which types of outsourcing (such as cloud computing, dedicated hosting, service outsourcing) are most applicable to that step. These are not intended to be absolute, because the scope of each outsourcing engagement is unique, but instead are intended to be guidelines.

Preliminary and Overview

1. Review the audit steps in the other chapters in this part of the book and determine which risks and audit steps are applicable to the audit being performed over outsourced operations. Perform those audit steps that are applicable.

The risks present for an insourced function are also present for an outsourced function. Remember that the components and functions of what you've outsourced are similar in many cases to what you would have internally. They are simply being handled by a different entity. Regardless of who is responsible for your data and applications, you still have controls that must be put in place. Although additional risks are present when a function is outsourced, you still must review for the basic controls that you would expect of an internally sourced function. For example, if you outsource a business application, you will still be interested in access controls, data input controls, and software change controls over those applications. Those controls are still critical to the confidentiality, integrity, and availability of that application. And if you outsource your data center, you will still be concerned as to how the people running that data center ensure physical security and continuity of operations.

This step is applicable to all forms of outsourcing.

How

Although you could argue that you would perform all of the same steps for an outsourced function as you would for an insourced one (again, because the risks are all still present), in reality, you probably won't have the same level of access with an outsourced process that you would get for an internal process, so you need to pick your battles. For example, if you want to review operating system security, the vendor may not give you access to accounts on its operating systems so that you can review system configuration. Maybe it will, and it's certainly worth asking, but you will often be limited by contractual rights. Perhaps instead, you will focus on their processes for keeping their systems patched and for regularly monitoring the security of the systems themselves (that is, review their processes regarding ensuring system security rather than reviewing the configuration of specific servers), and you ask the vendor to run a set of read-only scripts that pull key system configuration information from their environment and send you the output. After developing your wish list of steps you would like to perform during the audit, you might go ahead and determine which ones are the most critical to you so that you'll know which ones to fight for should you encounter resistance from the vendor.

Significant variability will be the norm with regard to how you perform these steps—it all depends on the rights, influence, and relationship you have with your supplier. Some may allow you to come in and audit their processes and infrastructure just as if you were their own internal auditors. Others will hand you a SAS 70 report and be done with you, informing you that they have fulfilled their obligation. You will have to negotiate each instance separately and enlist the aid of your procurement, legal, and operations groups to see how far you can push for transparency from your supplier. This is why it is critical to establish robust "right to audit" clauses in your contracts to deal with these situations up-front, while you still have leverage.

NOTE This is a critical step. For efficiency's sake, we are not duplicating the audit steps from other chapters here. However, if, for example, you are performing an audit of data center operations that have been outsourced to a co-location facility, it is critical that you perform not only the steps in this chapter but also the steps in Chapter 4. Likewise, if you are performing an audit of a business application that uses the SaaS model, you must perform not only the steps in this chapter but also the steps in Chapter 13 (at a minimum). In fact, just as when you're auditing an internal application, you might also want to perform steps from Chapters 6 to 9 on auditing the pertinent operating system, the database, and so on.

2. Request your service provider to produce independent assurance from reputable third parties regarding the effectiveness of their internal controls and compliance with applicable regulations. Review the documentation for issues that have been noted. Also, determine how closely these certifications match your own company's control objectives and identify gaps.

Although you are attempting to perform your own audit of your service provider's controls, experienced service providers will already be engaging third parties for regular assessments. These assessments can be used to reduce your need to audit the service provider's functions, thereby reducing the scope of your audit. In fact, many service providers, especially the larger ones, will insist that you use these assessments in lieu of performing your own audit.

This step is most applicable to cloud computing, dedicated hosting, and offsite service outsourcing.

How

Request this information from your vendor. The type of independent assurance you ask for will vary depending on your industry, but the most common assessment you should look for will be a SAS 70 report. Make sure you request a Type 2 SAS 70 assessment. Another common assessment you may see is ISO 27001, which is a standard dealing with information security that is intended to form a basis for a third-party audit of security. You will need to determine what assessment(s) should be expected based on your industry, the type of outsourcing being performed, and the type of auditing you're performing. For example, if you're performing an audit of an outsourced website, you should expect to see some form of web security certification. As part of this exercise, you will need to determine whether your vendor subcontracts any relevant functions to additional third parties (for example, if you're using a SaaS vendor and it uses another vendor's data center facilities to host its systems). If so, request that your vendor obtain applicable independent assessments from those subcontract vendors and provide them to you.

Once you receive whatever assessments are available, you must review them in a number of areas. First, obviously, you must review the results of the assessment to understand any issues noted and the vendor's remediation plans. You will want to track these items to ensure that they have been remediated satisfactorily (which again you may need to determine via a third-party assessment). It is also important to ensure that the assessment was performed by a qualified independent third party and to determine the time period covered by the assessment to be sure it is still relevant.

You will also need to review the scope of the assessment performed and determine how many of your control objectives were addressed by the assessment. You will likely see some gaps between your company's control objectives and the control objectives addressed by the independent assessment. Once you identify these gaps, you can attempt to perform your own assessments of those items not covered by the third-party assessment. You will have to negotiate each instance separately and enlist the aid of your procurement, legal, and operations groups to see how far you can push for the ability to perform your own audit. This again emphasizes the importance of placing a “right to audit” clause in your contracts.

If you find that your vendor does not have appropriate third-party assessments, you will have to attempt to perform all pertinent audit steps yourself (which may be limited by your right to audit). If this is the case, you should push your vendor to obtain a SAS 70 Type 2 and/or other pertinent independent assessments, possibly making this a negotiating point at contract renewal time. You should expect to see this type of assessment for any form of IT systems and infrastructure outsourcing (such as cloud computing). It may not be reasonable to expect it for IT service outsourcing models where you are providing significant guidance on day-to-day activities (such as when you outsource a function but leave it onsite using your own systems).

Vendor Selection and Contracts

3. Review applicable contracts to ensure that they adequately identify all deliverables, requirements, and responsibilities pertinent to your company’s engagement.

The contract is your only true fallback mechanism should you have issues with the vendor. If it’s not spelled out in the contract, it becomes very difficult, if not impossible, to enforce requirements and/or seek restitution should there be issues.

This step is applicable to all forms of outsourcing.

How

The best time to perform this step is before the contract is finalized and signed, because that’s when you can make changes and influence the contents of the contract relatively easily. However, if you are performing the audit after the contract has been signed, it is still relevant for two reasons: First, it will give you an idea as to what you’re working with and what sort of leverage you will have during the audit. Second, it will allow you to provide input as to what changes need to be made in the contract when it’s time to renegotiate.

Regardless of whether you’re reviewing a signed contract or providing input before the fact, you should make sure the following areas are addressed in the contract:

- Specify how performance will be measured, including Service Level Agreements (SLAs) that specify requirements for availability (such as expected uptime), performance (such as speed of transaction response after the ENTER key is pressed), response time (such as whether the vendor will respond to problems 24/7 or only during normal business hours), and issue resolution time (such as how quickly you should expect issues to be fixed).
- SLAs for security (that is, requirements for controls to protect the confidentiality, integrity, and availability of data) can include requiring specific control frameworks (such as COBIT) to be followed and requirements for third-party assessments. It should also include requirements for how data should be stored (such as encryption, including requirements for the algorithm and key length),

who may be granted access to it, how business continuity and disaster recovery will be ensured, how investigations will be supported, what security training and background checks are required for personnel who will access your systems and data, how data retention and destruction should occur, and so on. Overall, you want to make sure your vendor takes contractual responsibility for security.

- Other key metrics and performance indicators should be included, which can be used by your company to measure the quality of the service. For example, if you have outsourced your helpdesk function, you might want to set an expectation as to tickets closed per analyst and customer satisfaction rating.
- Outline requirements for compliance with applicable laws and regulations (such as PCI, HIPAA), including requirements for independent assessments certifying compliance.
- Provide provisions for penalties upon nonperformance or delayed performance of SLAs and conditions for terminating the agreement if performance goals are not met.
- Add a right to audit clause, specifying what your company is allowed to audit and when. You obviously will want to push for a broad right to audit, allowing you to audit whatever you want, whenever you want (including the ability to perform surprise audits). You can negotiate from there. The broader you make this clause, the more freedom you will have.
- Include provisions for your right to audit and review independent assessments (such as SAS 70) for functions that your vendor subcontracts out to other vendors (for example, if your SaaS vendor is hosting its systems with another third party). If possible, dictate in the contract what functions (if any) your vendor is allowed to subcontract and/or obtain the right of approval for any subcontracting relationships.
- Gain assurance that you can retrieve your data when you need it and in the format you desire.
- Add language prohibiting the vendor from using your data for its own purposes (that is, for any purposes not specified by you).
- Include nondisclosure clauses to prevent the vendor from disclosing your company's information.
- Include evidence that the contract was reviewed by your procurement and legal organizations, as well as applicable operations groups.
- Basically, include anything you expect from the service provider that needs to be specifically outlined in the contract. Consider the other steps in this chapter for ideas as well.

4. Review and evaluate the process used for selecting the outsourcing vendor.

If the process for selecting the vendor is inadequate, it can lead to the purchase of services that do not meet the requirements of the business and/or poor financial decisions.

This step is applicable to all forms of outsourcing.

How

Obviously, your goal should be to perform this step prior to vendor selection, when you can influence the decision. However, if your audit is being performed after the fact, there is still value in understanding the vendor selection process. It can identify gaps that must be addressed and provide information that can be used when it's time to renew the contract or enter into other contracts.

Review the vendor selection process for elements such as these:

- Ensure that multiple vendors are evaluated and involved in the bid process. This provides for competitive bidding and lower prices.
- Determine whether the vendors' financial stability was investigated as part of the evaluation process. Failure to do so may result in your company signing up with a vendor that goes out of business, causing significant disruption to your operations as you attempt to bring them back in-house or move them to another vendor.
- Determine whether the vendors' experience with providing support for companies of similar size to yours and/or in a similar industry was evaluated. This can include obtaining and interviewing references from companies that currently use the vendor's services. You generally want to use vendors who have already demonstrated that they can perform the types of services you're looking for at a similar scale.
- Ensure that the vendors' technical support capabilities were considered and evaluated.
- Ensure each vendor was compared against predefined criteria, providing for objective evaluations.
- Determine whether there was appropriate involvement of procurement personnel to help negotiate the contract, of operations personnel to provide expert evaluations as to the vendor's ability to meet requirements, and of legal personnel to provide guidance on potential regulatory and other legal ramifications of the outsourcing arrangement.
- Ensure that a thorough cost analysis was performed. The total cost of performing the operation in-house should be developed as well as the total cost for using each vendor. This analysis should include all relevant costs, including costs for one-time startup activities, hardware and related power and cooling, software, hardware maintenance, software maintenance, storage, support (labor), and so on. Too often, companies make decisions without considering all relevant costs. For example, some of the cost savings from cloud computing may be offset by increased monitoring to ensure that requirements are met. These costs need to be included in the analysis to ensure that the company is making an informed decision.

Data Security

For all of the steps in this section (except step 8), your first option should be to determine whether an evaluation of the area is available via a third-party assessment (such as SAS 70). If it is not, you'll need to work with your operations, procurement, and legal departments to determine your rights to audit the vendor in this area. Hopefully, those rights are spelled out in the contract. If they are not, your company will need to attempt to press for that right, possibly using the next contract renewal as negotiating leverage.

If the area is not covered by an assessment such as a SAS 70 and if you have the right to audit it, you will need to interview the vendor and review their documentation regarding their technical controls and processes, testing those controls as you're able.

You will also want to see your company's requirements for these controls spelled out in your contract and look for evidence that those specific requirements are being met.

5. Determine how your data is segregated from the data of other customers.

If your company chooses a form of outsourcing in which your data is being stored on the vendors' systems at their site (such as in cloud computing and dedicated hosting), you no longer have full control over your data. Your data may be comingled with other customers' data (a likely scenario with cloud computing). This creates a number of risks. For example, if data is not properly segregated, another customer (including one of your competitors) on the same shared infrastructure may be able to access your data. Likewise, if one customer's system is breached, the confidentiality, integrity, and availability of other customers in the same environment may be at risk. For example, viruses might be transmitted from one customer to another or an attacker might be able to download data from all customers in the environment.

This step is most applicable to cloud computing and dedicated hosting.

How

Review the technical controls and processes for assuring segregation and protection of your systems and data. There's no single way to do this, and the implementation will differ depending on the technologies being used by your vendor, but the vendor needs to demonstrate how they have segregated and compartmentalized systems, storage, network, and so on. For example, in a dedicated hosting environment, you'll be looking for network devices (such as firewalls) to segregate the network hosting your systems from the networks hosting other customers. In a SaaS environment, you'll be looking for segregation of databases containing customer data. Ideally, you would like to perform your own tests to validate that their controls are working as designed. Again, the nature of these tests will depend on the technology and the implementation.

6. Review and evaluate the usage of encryption to protect company data stored at and transmitted to the vendor's site.

If your data is no longer fully under your control (that is, it is being stored at a third-party site and possibly being comingled with data from other customers), it is critical that the data be encrypted to protect against possible compromise. This reduces the risk of a breach impacting the confidentiality or integrity of your data. If you have unencrypted data in a shared environment (such as cloud computing), you can assume that it is no longer confidential.

This step is most applicable to cloud computing, dedicated hosting, and offsite service outsourcing.

How

Look for encryption of data both in transit (for example, via SSL for browser-enabled transactions) and at rest (that is, in storage), because both are outside of your control if your data is stored at a third-party site. Evaluate the strength of the encryption. Hopefully, you will have contractually-dictated requirements for encryption (such as algorithm and key length) against which you can compare the system.

Determine how key management is performed and how your keys are separated from those of other customers in your environment. Ideally, this function should be performed either by your company or by a separate vendor from your standard outsourcing vendor, providing for segregation of duties.

7. Determine how vendor employees access your systems and how data is controlled and limited.

If your data is being stored or processed by employees outside of your company and you do not maintain ownership regarding who has access to that data, you're putting its confidentiality, integrity, and availability at risk.

This step is applicable to all forms of outsourcing.

How

Determine who has access to your data and systems and review for appropriateness. Determine how appropriate segregation of duties is maintained. Ensure that the concept of "minimum necessary access" is followed.

Review the approval process for determining who will have access to your systems and data. Ideally, the data owner at your company will be the gatekeeper for approval. Your company should maintain the right (hopefully spelled out in the contract) to deny access to your data from vendor personnel.

Review your vendor's processes for hiring and screening employees, ensuring that appropriate background checks are performed and rules regarding security and management of your environment are communicated to the employees. These requirements should be dictated in the contract.

Ask for a listing of any third-party relationships that your vendor has and any interfaces those additional parties have to your systems. Each of these represents additional exposure of your data.

8. Review and evaluate processes for controlling non-employee logical access to your internal network and internal systems.

If you're using service outsourcing and/or supplemental (contract) labor, you are likely allowing a third-party vendor's personnel to have a degree of logical access to your network and systems. Because these personnel are not employees of your company, they are less likely to have a personal investment in the company's success or an awareness of its policies and culture. If their access to company information assets is not governed and if expectations regarding their usage of that access are not communicated, it is more likely that company information assets will be unnecessarily exposed or misused.

This step is most applicable to onsite and offsite service outsourcing plus supplemental labor.

How

Ensure that policies require approval and sponsorship from an employee prior to a non-employee obtaining logical access to company systems. If feasible, obtain a sample of non-employee accounts and validate that they have appropriate approval and sponsorship.

Review and evaluate processes for communicating company policies (including IT security policies) to non-employees prior to granting them system access. Look for evidence that this communication has occurred. For example, if all non-employees are required to sign a statement that they have read and agree to the policies, pull a sample of non-employees and obtain copies of these agreements.

Review and evaluate processes for removing logical access from non-employees when they have ceased to work with your company or otherwise no longer need access. Consider obtaining a sample of current non-employee accounts and validating that those non-employees are still working with your company and still have a need for their current level of access.

Ensure that nondisclosure agreements (NDAs) are signed by non-employees to legally protect your company from inappropriate use of company data. Pull a sample of non-employee accounts and obtain a copy of the NDA for those accounts.

Ensure that consideration has been given to identifying data that should not be accessed by non-employees and activities that should not be performed by non-employees. For example, your company may decide that access to certain levels of financial data should never be granted to non-employees. Or it may decide that non-employees should never be granted system administration duties. The answer will depend on your company's industry and philosophies; however, an evaluation process should take place and the results of that evaluation should be documented in company policy and enforced.

9. Ensure that data stored at vendor locations is being protected in accordance with your internal policies.

No matter where you store your data, it is still subject to your internal policies. Outsourcing storage to a third party does not absolve your company of responsibility to comply with policies and ensure proper security of the data.

This step is most applicable to cloud computing and dedicated hosting.

How

Ensure that data stored at third-party sites has been classified in accordance with your company's data classification policy and is being protected in accordance with that policy. Data with certain levels of classification might be inappropriate to store outside the company (such as employee and customer personal information). Review your company's policies on data security and ensure that off-site data is being protected in accordance with those policies. Encrypting data that is stored with the vendor will greatly benefit you in this area.

10. Review and evaluate controls to prevent, detect, and react to attacks.

Without appropriate intrusion detection and prevention techniques, your systems and data are at an increased risk of compromise. This risk is increased in an outsourced model, specifically when outsourcing systems and infrastructure, because of the shared infrastructure,—an attack and compromise on one customer could result in compromise of your systems.

This step is most applicable to cloud computing and dedicated hosting. Also, consider whether this risk is applicable if you're using offsite service outsourcing, as the service provider may store your data on their systems and/or have connectivity to your internal systems.

How

This step might be divided into separate substeps. For infrastructure and systems located at third-party sites, determine the effectiveness of processes such as those listed next.

Intrusion Detection Look for the usage and monitoring of Intrusion Detection Systems (IDSs) to detect potential attacks on your systems and integrity checking tools to detect potential unauthorized changes to system baselines.

Intrusion Prevention Look for the usage and monitoring of Intrusion Prevention Systems (IPSs) to proactively detect and cut off potential attacks on your systems.

Incident Response Look for clearly defined processes for responding to potential security incidents, including notification and escalation procedures.

Discovering and Remediating Vulnerabilities Look for the usage and monitoring of vulnerability scanning tools to detect and mitigate potential vulnerabilities that might allow an intruder to access and/or disrupt your systems.

Logging Look for the logging of significant activities (successes and failures) on your systems, for the monitoring of these logs, and for the storage of these logs in a secure location for an adequate period of time.

Patching Look for procedures to receive and apply the latest security patches so that known security holes are closed.

Protection from Viruses and Other Malware Look for the usage of antivirus software and the application of new signature files as they are released.

11. Determine how identity management is performed for cloud-based and hosted systems.

Proper identity management practices are critical for controlling access to your systems and data. Distributed computing became popular in the 1990s. When each user was required to track IDs and passwords on multiple systems, it led to problems such as employees sharing accounts, inconsistent password controls (for example, password strength, aging), accounts not being removed when no longer needed, employees with more access than they needed, and other issues. Without some form of central control, no real governance was possible. To resolve these issues, many companies deployed enterprise IDs, giving users one account name for all systems, as well as strong enterprise passwords, which can be used to authenticate to multiple systems.

As your company begins adopting cloud computing, you run the risk of seeing the same issues arise again. Users may end up with accounts with multiple cloud providers, each with a different ID and password. If you're not careful, you'll encounter the same issues that companies encountered in the '90s with distributed computing.

This step is most applicable to cloud computing, particularly SaaS, and dedicated hosting, particularly of purchased applications.

How

Although it's possible to review the identity management controls over each outsourced system (checking each for appropriate password controls, account management controls, and so on), you should prefer to have a federated identity management capability. This will allow your users to authenticate to your internal systems with their enterprise ID and password and then for your vendor to trust your assertion that each user has been properly authenticated. This offers the benefits of centralized identity management and allows you to avoid storing user credentials with your vendor.

If you implement this form of federated identity management, be sure that your internal credential data (such as IDs and passwords) are not being made directly available to your vendor (that is, they should not be able to make direct calls against your internal identity management systems) and that they are not being transmitted in the clear or stored in the clear at your vendor's site. These requirements will preferably be dictated in your contract. If you are unable to implement federated identities, you will need to review the identity management controls over your outsourced systems to ensure that they meet the requirements of your policies. An alternative solution is to use an identity management service as a "middle man" between your company and your vendor, but of course that solution introduces another third party that you must audit into your environment.

12. Ensure that data retention and destruction practices for data stored offsite comply with internal policy.

If the lifecycle of data is not defined, data might be retained longer than necessary (resulting in additional storage costs and possible legal liabilities) or may be destroyed prematurely (leading to potential operational, legal, or tax issues).

This step is most applicable to cloud computing, dedicated hosting, and offsite service outsourcing (if the supplier is storing your data).

How

Determine whether lifecycle requirements have been defined for data stored with vendors. For a sample, review the documentation of the data's lifecycle requirements, including retention, archive, and destruction requirements. Ideally, requirements will be identified for how long the data should be active (online, easily accessible, modifiable if appropriate, and backed up periodically), when and for how long it should be archived (possibly offline, not necessarily easy to access, no longer modifiable, and no longer backed up periodically), and when it should be destroyed. Ensure that these requirements appropriately reflect the nature of the data (for example, external public content on your website should be treated differently than customer data). The contract should dictate that the vendor manage data per your lifecycle requirements. Review evidence that lifecycle requirements have been implemented, concentrating especially on evidence that your vendor has destroyed data per your requirements. Note that data destruction can often be very difficult to prove in the cloud, increasing the importance of using strong encryption for your data, as described earlier.

13. Review and evaluate the vendor's physical security.

Physical security impacts logical security, because physical access can override some logical access controls. You can have excellent logical security, but if someone can walk in off the street and walk off with the computer (or perhaps just the disk drive or tape cartridges) containing your systems and data, you will at a minimum experience a disruption of service, and if the data is not adequately encrypted, you may also be looking at a security breach.

This step is most applicable to cloud computing, dedicated hosting, and offsite service outsourcing.

How

Review the vendor's physical security for controls such as these:

- Badge readers and/or biometric scanners
- Security cameras
- Security guards
- Fences
- Lighting
- Locks and sensors
- Processes for determining who will be granted physical access

See Chapter 4 for additional information on auditing physical security controls.

Operations

14. Review and evaluate your company's processes for monitoring the quality of outsourced operations. Determine how compliance with SLAs and other contractual requirements are monitored.

Although you have hopefully dictated expectations in your contract, unless you monitor for compliance with those expectations, you will have no way of knowing whether they're being met. If those expectations are not met, the availability, efficiency, and effectiveness of your operations and the security of your systems and data can be impacted.

This step is applicable to all forms of outsourcing.

How

Review the contract to understand requirements. Interview your company's internal management to determine their processes for monitoring that each of those requirements is being met. Obtain and review metrics, slides from operations reviews, and other materials, and compare the results to the requirements stipulated in the contract. Where deviances have occurred, review for corrective action plans and evidence that those plans have been implemented and were effective.

If requirements have not been dictated in the contract, determine how the quality of services is monitored and how the vendor is held accountable. The inclusion of SLAs should be a requirement when the contract is renewed.

Ensure you cover the following basic topics in performing this step:

- Availability (such as expected uptime)
- Performance (such as speed of transaction response after the ENTER key is pressed)
- Response time (such as whether the vendor will respond to problems 24/7 or only during normal business hours)
- Issue resolution time (such as how quickly you should expect issues to be fixed)
- Security and compliance requirements
- Other key metrics and performance indicators that can be used by your company to measure the quality of the service

15. Ensure that adequate disaster recovery processes are in place to provide for business continuity in the event of a disaster at your service provider.

Just as with internally-hosted systems, you must to prepare for recovery from a disaster when outsourcing operations. Failure to do so will likely result in extended outages and business disruptions if a disaster occurs with your vendor.

This step is most applicable to cloud computing, dedicated hosting, and offsite service outsourcing.

How

You should expect that your vendor will follow sound disaster recovery disciplines, such as those you would look for when auditing your internal operations. This includes steps outlined elsewhere in this book, such as reviewing for offsite backups, up-to-date documented recovery procedures, periodic testing, hardware redundancy, and so on. Your first option should be to determine whether an evaluation of this area is available via a third-party assessment (such as SAS 70). If not, you'll need to work with your operations, procurement, and legal departments to determine your rights to audit the vendor in this area. Ideally, that right is spelled out in the contract. If not, your company will need to attempt to press for that right, possibly using the next contract renewal as negotiating leverage.

If the area is not covered by an assessment such as a SAS 70 and if you have the right to audit it, you will need to interview the vendor and review their documentation regarding their controls and processes, testing those controls as you're able. You will also want to see the requirements for disaster recovery controls, including recovery time objectives (how quickly your systems should be back up after a disaster) and recovery point objectives (how many days' worth of data you're willing to lose), spelled out in your contract. Determine how the vendor ensures compliance with the requirements in the contract.

While it is important that you understand your vendor's disaster recovery procedures, you should also expect that your company will have documented procedures regarding how they would recover in the event of a disaster at your vendor. This should include notification and escalation procedures, any necessary hand-offs between your company and the vendor during the recovery, and potential manual workarounds while waiting for recovery. It should also include contingency plans should the vendor be unable to recover for an extended period of time (or ever). Request information regarding the location of your data and regarding any replication in the architecture. If the data and infrastructure are replicated across multiple sites, your vulnerability and need for contingency plans decrease. If your systems are at a single location, it becomes more critical for your company to document contingency plans, which need to include a method for obtaining your data and bringing it back in-house if necessary.

16. Determine whether appropriate governance processes are in place over the engagement of new cloud services by your company's employees.

Cloud computing makes it easy for business unit personnel to meet their needs without ever engaging corporate IT. Because most cloud services can be accessed via an Internet-connected browser, a business unit can engage a cloud vendor and outsource the systems and data related to one of their business processes without really having to tell anyone else. This has the potential to bypass all of the governance processes normally in place to ensure proper security of company data, interoperability of systems, appropriate support capabilities, and so on.

This step is most applicable to cloud computing.

How

Review company policies to determine whether this topic has been addressed. Policies should be in place requiring company personnel to follow specific procedures when engaging vendors for this sort of service. If this policy exists, review it for adequacy. It should require that IT be engaged and that specific security and operational needs be addressed. Determine how employees are made aware of the policy. Also, determine how the policy is enforced. For example, if your company has a centralized procurement organization that must be engaged to sign contracts and pay invoices, you can use them as the gatekeeper for ensuring that proper procedures are followed for new engagements.

17. Review and evaluate your company's plans in the event of expected or unexpected termination of the outsourcing relationship.

Your company might terminate the outsourcing relationship in the future for many reasons. The provider could go out of business or discontinue the service you're using. You could be unhappy with the provider's cost or performance. You might engage in a new competitive bid at the end of your contract and another vendor may win the business.

If you can't bring the service back in-house or switch it to another vendor, you'll find yourself locked in with your vendor, which greatly damages your leverage to influence price and service quality. And if that company goes out of business, you'll experience significant business disruption.

This step is applicable to all forms of outsourcing.

How

Determine whether your company has a documented plan indicating how they would bring the functions back in-house (or move them to another vendor) if necessary. If bringing the function in-house is unrealistic, you should see evidence that alternative service providers have been identified. Ensure that an analysis has been performed regarding how long it would take to transition the services and determine whether appropriate contingency plans are in place to keep the business running in the interim.

Look for contractual requirements for your vendor to return your data and assets upon request. If this has not been indicated in the contract, the vendor can hold your data hostage or can comingle it with other customers' data in such a way that it's nearly impossible to extract your data. Your company should require that your vendor deliver copies of your data to you periodically in an agreed-upon format (one that can easily be ported to a new application). Where applicable, ensure that code is put in escrow to protect against the vendor going out of business.

For IaaS and PaaS, your systems should be developed and deployed so that they are easily portable to new environments. Review your company's processes for ensuring that portability is a key goal in any development for cloud-based services.

18. If IT services have been outsourced, review the service provider's processes for ensuring quality of staff and minimizing the impact of turnover. If those services are being performed offshore, look for additional controls to ensure employee attendance and effective communication and hand-offs with the home office.

If service provider employees aren't qualified to perform their jobs or the provider experiences high levels of turnover, the quality of IT services will obviously be poor. This risk generally increases with outsourced operations, where turnover tends to be higher.

Outsourced operations that are performed offshore contribute to the risks of communication breakdowns and absenteeism that can impact the quality of service received.

This step is most applicable to IT service outsourcing (onsite and offsite).

How

Review the contract to ensure job descriptions and minimum qualifications for each position are documented (such as education level, skills, experience). Pull a sample of supplier employees and verify that these minimums have been met. Review the provider's employee screening process to verify that appropriate background checks and qualification reviews take place prior to employment offers.

Determine how continuity of services is ensured in the event of turnover of service provider employees. Review staffing assignments and determine whether any single points of failure exist. Review cross-training processes.

Review the vendor's processes for providing training to update skills and knowledge. Request evidence that the training policy is being followed for a sample of employees.

Review the vendor's processes for monitoring attendance. This is particularly important if the services are being performed offshore, where absenteeism tends to be high. This should include reviews of physical security logs and system access logs. Request copies of these logs and verify the attendance of a sample of employees.

For offshore outsourcing, determine how appropriate language skills are ensured. This could include a language test with minimum test score requirements defined, conducting spoken and written interviews in the required language, and so on. You should also determine how the inherent complexity of communication and hand-offs is mitigated. Look for the existence of periodic hand-off and status meetings between countries. SLAs should be documented and monitored. An employee of your company at the offshore site (or at least in the same city with easy access to the site) should be available to act as your liaison and perform monitoring and oversight of the operations.

Requirements for all of these items should be dictated in the contract. Review the contract to verify this.

Legal Concerns and Regulatory Compliance

19. Review and evaluate your company's right and ability to obtain information from the vendor that may be necessary to support investigations.

Your company may be required to perform e-discovery (electronic discovery) in support of litigation. Inability to produce applicable data may result in legal ramifications, as your company will be held legally responsible for your information, even if it's being stored and processed by a third-party provider. Your company may also need to perform investigations for its own reasons (for example, to investigate inappropriate activities such as fraud or hacking attempts). An inability to access appropriate logging and other data will prevent you from performing your investigations, leaving you with no real recourse when those inappropriate activities occur.

This step is most applicable to cloud computing.

How

Because cloud providers often comingle their customers' data, especially logging data, it is critical that you receive a contractual commitment from your vendors to support investigations. Review the contract and ensure this is documented as a requirement, including details as to the kind of investigative support you may need (such as specific log information, data format requirements) and the required response time for requests. It is also important that the contract define the responsibilities of both the cloud provider and your company related to e-discovery (for example, who is responsible for conducting the searches, for freezing data, for providing expert testimony, and so on). Review the vendor's processes to ensure that a formal process is in place to cooperate with customer investigations and to handle subpoenas for information.

If you find that the cloud provider is incapable of (or unwilling to) providing adequate support of investigations, your company may need to maintain copies of its data in-house. If this is the case, the costs of doing so will affect the benefits of the cloud relationship.

20. Review requirements for security breach notification. Ensure that requirements are clearly defined regarding when and how the vendor should notify your company in the event of a security breach and that your company has clearly defined response procedures when they receive such notification.

A security breach at your service provider not only puts your data and operations in jeopardy but may also have legal implications. For example, if you're hosting personal information and a security incident occurs, you may be legally required to notify all users who may have been impacted. It's therefore critical that the service provider notify you in a timely fashion as to what has happened so that you can put together any necessary response.

This step is most applicable to cloud computing and dedicated hosting.

How

Review the contract for existence of requirements and evaluate those requirements for adequacy. Look for requirements regarding what constitutes a breach, how quickly a breach needs to be communicated to your company, and the method by which it should be communicated. Determine whether penalties have been built into the contract so that your company can be compensated for the costs incurred because of a breach.

Obtain a copy of your company's response procedures and ensure that they cover the basic information regarding what processes should be followed, who should be notified, when they should be notified, and how any compensating processes should be enacted.

If a breach has been reported, review for evidence that the correct processes were followed.

21. Determine how compliance with applicable privacy laws and other regulations is ensured.

Regardless of where your data is stored and who manages it, you are still responsible for making sure that your company is complying with all applicable laws and regulations. If your company is found to be in violation of applicable laws and regulations, it can lead to stiff penalties and fines, a damaged reputation, lawsuits, and possibly the cessation of the company. The fact that it was being managed by a cloud provider will not be an acceptable defense.

This step is most applicable to cloud computing and dedicated hosting.

How

Review the contract, and look for language requiring that the vendor obtain third-party certification regarding compliance with applicable regulations (such as PCI and HIPAA) as well as requiring SAS 70 assessments. If you find such language, review evidence that your company is requesting these reports from the vendor and reviewing the results. Review the most recent reports for any issues that have been noted and determine how your company is tracking those issues.

The contract should require that the vendor disclose where your data is located and provide assurance that they are complying with local privacy requirements related to your data. The contract should also contain language specifying who is liable in the event of noncompliance.

If the contract does not require these certifications and/or the vendor will not undergo these assessments, determine how your company is certifying compliance with applicable regulations. If this is the case, your company should seriously consider a withdrawal strategy.

22. Review and evaluate processes for ensuring that the company is in compliance with applicable software licenses for any software hosted offsite or used by non-employees.

Using software illegally can lead to penalties, fines, and lawsuits. If companies do not develop processes for tracking the legal usage of software and licenses, they may be subject to software vendor audits and will not be able to account properly for the company's use of the vendor's software. This becomes more complex when dealing with outsourced operations, as purchased software may be hosted on third-party infrastructure and/or used by outsourced service provider employees. You must ensure that copies of the software continue to be tracked and that the usage is in compliance with the terms of agreement.

This step is applicable to all forms of outsourcing.

How

Look for evidence that the company maintains a list of enterprise software licenses (such as Microsoft Office, ERP application accounts, and so on) and that it has developed a process for monitoring usage of those licenses and complying with the terms of agreement. Ensure that this process incorporates copies of your software that are hosted by a third party and copies of the software used by non-employees.

Knowledge Base

The knowledge base for cloud computing security and audit techniques is still developing. However, a few organizations have begun to focus on this area and have produced some useful results:

- The National Institute of Standards and Technology (NIST) has developed definitions and standards related to cloud computing, as well as guidance for secure usage. See http://csrc.nist.gov/groups/SNS/cloud-computing/.
- The Cloud Security Alliance (CSA) promotes best practices for security with cloud computing. CSA developed one of the most comprehensive security guides for cloud computing in 2009. This document, along with other useful information on the topic, can be viewed at www.cloudsecurityalliance.org.
- ISACA has produced some research on the topic, including an excellent white paper on cloud computing security in 2009, which can be accessed at http://isaca.org/.
- The cloud security blog at http://cloudsecurity.org/ also provides an array of useful research and viewpoints on the topic.

Regarding materials on auditing general (non-cloud–specific) IT outsourcing, your best bets are to search for relevant materials on the ISACA website (http://isaca.org/), specifically within the COBIT framework.

Master Checklist

The following table summerizes the steps listed herein for auditing cloud computing and outsourced operations.

Auditing Cloud Computing and Outsourced Operations

Checklist for Auditing Cloud Computing and Outsourced Operations	
❑	1. Review the audit steps in the other chapters in this part of the book and determine which risks and audit steps are applicable to the audit being performed over outsourced operations. Perform those audit steps that are applicable.
❑	2. Request your service provider to produce independent assurance from reputable third parties regarding the effectiveness of their internal controls and compliance with applicable regulations. Review the documentation for issues that have been noted. Also, determine how closely these certifications match your own company's control objectives and identify gaps.
❑	3. Review applicable contracts to ensure that they adequately identify all deliverables, requirements, and responsibilities pertinent to your company's engagement.
❑	4. Review and evaluate the process used for selecting the outsourcing vendor.
❑	5. Determine how your data is segregated from the data of other customers.
❑	6. Review and evaluate the usage of encryption to protect company data stored at and transmitted to the vendor's site.
❑	7. Determine how vendor employees access your systems and how data is controlled and limited.
❑	8. Review and evaluate processes for controlling non-employee logical access to your internal network and internal systems.
❑	9. Ensure that data stored at vendor locations is being protected in accordance with your internal policies.
❑	10. Review and evaluate controls to prevent, detect, and react to attacks.
❑	11. Determine how identity management is performed for cloud-based and hosted systems.
❑	12. Ensure that data retention and destruction practices for data stored offsite comply with internal policy.
❑	13. Review and evaluate the vendor's physical security.
❑	14. Review and evaluate your company's processes for monitoring the quality of outsourced operations. Determine how compliance with SLAs is monitored.
❑	15. Ensure that adequate disaster recovery processes are in place to provide for business continuity in the event of a disaster at your service provider.
❑	16. Determine whether appropriate governance processes are in place over the engagement of new cloud services by your company's employees.

Checklist for Auditing Cloud Computing and Outsourced Operations ***(continued)***

❑ 17. Review and evaluate your company's plans in the event of expected or unexpected termination of the outsourcing relationship.

❑ 18. If IT services have been outsourced, review the service provider's processes for ensuring quality of staff and minimizing the impact of turnover. If those services are being performed offshore, look for additional controls to ensure employee attendance and effective communication and hand-offs with the home office.

❑ 19. Review and evaluate your company's right and ability to obtain information from the vendor that may be necessary to support investigations.

❑ 20. Review requirements for security breach notification. Ensure that requirements are clearly defined regarding when and how the vendor should notify your company in the event of a security breach and that your company has clearly defined response procedures when they receive such notification.

❑ 21. Determine how compliance with applicable privacy laws and other regulations is ensured.

❑ 22. Review and evaluate processes for ensuring that the company is in compliance with applicable software licenses for any software hosted offsite or used by non-employees.