©2015 ARMA International

Principles for Outsourcing Mission-Critical Business Processes

Julie Gable, CRM, CDIA, FAI

Organizations that outsource mission-critical business processes have a distinct challenge ensuring their information is properly managed, as service providers are not just storing the organization's information, they are using highly automated processes to create, process, and use it. This article discusses how it must also be governed.

Cloud-based services such as storage, software-as-a-service, and infrastructure-as-a-service have made it possible to outsource almost anything. Although it has been common to outsource paper and electronic records storage, as well as back-office business processes such as HR benefits administration or payroll processing, organizations now are also outsourcing mission-critical functions and services.

For example, a county government might decide to outsource turnkey social welfare, human services, and correctional functions, while a pharmaceutical company might decide to outsource a regulatory function such as adverse event reporting.

This so-called "second tier" outsourcing is in response to the more recent availability of large service providers offering sophisticated technology and tools, such as big data, business analytics, and industry-specific processing services.

While the traditional rationale for outsourcing has been cost savings, operational flexibility, off-loading non-core competencies, and the short-term tax advantages of outsourcing versus making capital investments in specialized systems, the rationale for outsourcing mission-critical functions is more about gaining access to providers' technology and expertise.

In outsourced customer-related processes, for example, organizations may glean competitive insights through using the service provider's data manipulation capabilities.

Shared IG Responsibility

What happens to information governance (IG) when mainstream

©2015 ARMA International

business processes are transferred to a service provider (SP)? Because IG is about how an organization handles information that arises from its business processes, regardless of where or how those processes are completed, IG principles must apply to how the organization's SPs handle its information, as well.

For this reason, mission-critical outsourcing is becoming a topic for discussion at the enterprise level by the legal, records, and IT members of the IG council or among senior management in consultation with an IG officer.

As the trend to outsource business operations continues – a trend IDC predicted in its "Worldwide and U.S. IS Outsourcing Services 2013–2017 Forecast" would grow 6% per year worldwide, reaching $209.4 billion – organizations need to be aware of how these third parties accomplish their tasks and how they treat the records that are created as part of outsourced business processes.

Tools for Evaluating Providers

The bottom line in this age of compliance, litigation, and operations concerns is that it is reasonable to expect that when SPs create and manage an organization's information, they will do so to the contracting organization's standards.

The Generally Accepted Recordkeeping Principles® (the Principles) are a good source of such standards. With a little tweaking, this highly adaptable tool can be used to:

- Highlight the trade-offs inherent in outsourcing and show areas where higher risks may justify requests for additional third-party IG services
- Evaluate a potential SP's information-handling methods before committing to a contract
- Establish a common understanding of governance at the outset of the relationship
- Help set expectations and evaluate an SP's performance over time

The Principles and the Information Governance Maturity Model (IGMM), which are both available free at *www.arma.org/principles*, are templates for conversations among all the stakeholders involved, providing the basis for arriving at an understanding of what is ideal and what is realistic. The truth is that contracting for extra IG services may incur extra costs. The point is to identify and prioritize those aspects of IG where the reduction of risk is worth the extra cost.

The point is to identify and prioritize those aspects of IG where the reduction of risk is worth the extra cost

Here, then, are possible considerations for using the Principles to assess an SP's IG capabilities.

Evaluating Service Provider Attitudes

The Principles of Accountability, Compliance, and Transparency are the cornerstones of an organization's entire IG program and are not necessarily associated with any one business process. The point in due diligence is to understand how the SP will help (or hinder) efforts at ensuring the outsourced process is performed with reasonable levels of all three Principles in mind.

It is important to realize that an outsourcing organization retains ultimate responsibility for accountability, compliance, and transparency and that the service provider should work as a partner to its goals. There are three primary questions to consider:

Who Is Accountable?

Who at the SP is accountable for the business process and the records it creates? If the answer is the account rep, run! There should be someone at a management and/or technical level who is directly accountable for process oversight, verifying the process gets done correctly and that all aspects of the process, including the information produced, are handled as they should be.

All too often, the real test of an SP's accountability occurs when something goes wrong. Recognize, too, that ultimate responsibility for the validity of the process remains with the outsourcing organization, not with the SP. This implies there is someone within the outsourcing organization who regularly monitors the outsourced business process to ensure it is going as expected.

How Is Compliance Defined?

Does the SP interpret compliance in the same way the outsourcing organization does? Where an outsourced process is regulated, it is important to make sure the SP, even one who specializes in the outsourcing organization's industry, interprets the relevant regulations in the same way.

For example, how does the SP maintain records that demonstrate the outsourcing organization's compliance? If there is a reporting deadline, for instance, how does the SP prove the deadline was met?

Another question to ask is how the SP participates in a regulatory audit. Note that due diligence in compliance capabilities implies the outsourcing organization already knows the compliance requirements for the business process. As noted above for accountability, someone within the outsourcing organization should

©2015 ARMA International

regularly monitor that compliance requirements are met.

Are There Policies and Procedures?

Does the SP have written policies and procedures for the process that go beyond simple programming documentation? Adherence to the Principle of Transparency should be demonstrable by the SP in the form of documented processing and information management rules. Ideally, these should be available to regulators or investigators as needed.

Other aspects to consider are how, and how often, the SP's employees are trained in these rules. Many large SPs have substantial employee turnover, so training should be frequent and documented.

Evaluating Recordkeeping Practices

The Principles of Integrity, Protection, Availability, Retention, and Disposition are directly associated with good recordkeeping practices and IG maturity. They prescribe the quality of services expected from the provider with respect to the records created, used, and stored as part of the business process.

One of the disconnects inherent in outsourcing is that *ownership* of the information remains with the outsourcing organization, but *responsibility* for the information's reliability, security, accessibility, maintenance, storage, and disposition rests with the service provider.

SPs may be unfamiliar with these Principles. Most are organized as information technology-enabled SPs, and their interest is in a business model that stresses automation to deliver process results for each client while leveraging systems and software across many clients. Providers sell their services touting benefits like flexibility, mobility, and accessibility, and they may not be familiar with the risk-related aspects of recordkeeping principles.

Consider including a contractual clause giving the outsourcing organization the right to audit the provider's protection process…

Here is where the biggest potential trade-offs are, and it is wise to go into the outsourcing agreement with an eye not just on present benefits, but also on future risks. Some considerations from the Principles include the following:

Demonstrating Integrity

How does the provider demonstrate that the records it makes and manages on the outsourcing organization's behalf are reliable and authentic? Possibilities include:

- Test results that show its hardware and software consistently produce the same result
- Strict controls on who may edit or change records
- Audit trails to record when and by whom changes are made
- Standards for process timeliness and backlog prevention
- Ongoing training that is refreshed as needed for old and new employees

Often overlooked is the importance of the integrity of record dates. If the provider will import a large batch of the organization's records, be sure the metadata field for record date does not change to the import date. The same is true for paper records that will be scanned by the provider for use in its processes.

Providing Protection

SPs typically have excellent antivirus, anti-hacking, and back-up capabilities, which are important for protecting *systems*. *Records* protection, however, includes generating automated access logs that are updated frequently to ensure that only authorized individuals can work with the process or view the information.

The SP must limit the number of people who may access personally identifiable information and health information. The need for protection extends to information the provider asks the cloud service providers to store.

Because SPs have high turnover rates, it is important that access is denied immediately to employees that leave the company and that functionality controls are in place to prevent unauthorized e-mailing, copying, tweeting, or posting of sensitive information to the Internet.

Consider including a contractual clause giving the outsourcing organization the right to audit the provider's protection processes at regular intervals.

Ensuring Availability

One key benefit of outsourcing is that people with access rights may view records anywhere, from almost any device, at any time. The risk connected to the Principle of Availability is subtle and long term.

For example, an organization has to know whether at the end of the contract its information will be viewable and usable if it no longer has access to the provider's system and software. Some SPs' contracts allow for organizations to continue to use their infrastructure for some time until new arrangements are made either to bring the process back in-house or transfer it to another provider.

Another consideration is for any paper records the SP has scanned. If the paper records require retention

©2015 ARMA International

along with their electronic counterparts, they need to be kept in order. Most scanning processes are throughput-driven, and documents are often simply put back into boxes without the benefit of file folders to separate them or keep them in order. When this happens, the result at the end of an outsource agreement is a truckload of boxed chaos delivered back to the outsourcing organization.

An additional concern related to the Principle of Availability is whether records can be transferred to an e-discovery process, which also may be an outsourced service. Many law firms outsource e-discovery for large cases, so it is important to know in advance exactly how records in the custody of SPs will be designated for legal hold and how they will be made available for discovery purposes.

Effecting Retention and Disposition

Most SPs keep everything forever, which can be a risk, depending on the category of the records. It is rare, though not impossible, for retention codes to be captured as part of the metadata for records as they are created. Adhering to retention rules, particularly when they are event-based, is much more difficult for electronic records and usually requires human intervention. Because the provider's process model relies on automation as much as possible, it may have neither the ability, nor the willingness, to assume responsibility for retention and disposition.

Most organizations would not want an SP to perform disposition, and certainly not without a pre-defined approval process that considers legal hold requirements. It is prudent to document that the records associated with the outsourced business process may be retained in excess of the outsourcing organization's normal policy and acknowledge that the organization is aware of this risk.

'Outsourced,' Not Out of 'Scope'

In the past, few standards for outsourced functions existed other than service level agreements that covered things like system availability, uptime, and security. In the old view, the SP was a "black box" with little or no oversight given to how it operated except to accomplish what was contractually required. Some organizations believed that when they transferred information to SPs, they transferred all responsibility and accountability to them as well.

In the current age of regulatory and legal scrutiny, more organizations realize that outsourced does not mean out of scope of their IG accountability. Luckily, the Principles' clear definitions and the IGMM's specific benchmarks provide guidance in assessing the providers' IG capabilities.

The key is to use these tools to determine what SPs can – and cannot – provide and determine the impact of that on the organization's IG goals. Identifying risks may not impede the decision to outsource, but it does provide the advantage of a long-term perspective and the avoidance of surprises in the future. **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net. *See her bio on page 47.*