Secure Coding.
Practical steps to defend your web apps.

Outsourcing

Daniel Accioly Rosa

Outsourcing

What Is Outsourcing?

Outsourcing is the agreement between an organization, either company, government, or nonprofit organization, and a third-party service provider, where the provider is responsible to perform a business activity on a continuing basis that currently is, or could be, undertaken by the organization.

Outsourcing usually occurs for business activities that are not related to the organization's core services and to save money. This allows more focus on the bottom line, more control, and lower costs.

Offshore outsourcing is when the business activity is outsourced to a provider in a different country. Offshore outsourcing has some additional risks to outsourcing mainly related to different legislation, language problems, and distinct business practices between countries.

Why Outsource?

A company might outsource services for many reasons:

- To enhance effectiveness by focusing on organization core services

  Many activities within a company consume resources and need proper management. These activities, although necessary, might not be directly involved with the company bottom line but only exist to support the business. Examples include administrative functions such as payroll; support functions such as IT support; and call centers. By outsourcing these functions, companies can focus their resources on revenue generation areas and enhance the quality of core services to customers.

- To reduce investments in assets and free up these resources for other purposes

  Fixed assets are a cost. By outsourcing the service that uses those fixed assets, companies can free the resources to activities more related to its business activity and more closely connected to the company bottom line.

- To increase flexibility to meet changing business conditions and demand for products, services, and technologies

In a dynamic business environment, conditions and requirements change on a daily basis. The more fixed internal infrastructure to support various business functions a company has, the bigger the effort to change how it is performed.

When a company outsources a business function, it no longer needs to maintain the required fixed internal infrastructure. All assets used to execute the outsourced activity are usually the outsourcer's responsibility. Because of that, it is much easier for the outsourcee to respond to changes by adjusting a contract or contracting new services from the outsourcer.

- To monitor and improve operating performance through SLAs

When an outsourcing contract is created, it is common to have its performance monitored by Service Level Agreements. These measurable indicators allow management to evaluate the service quality much more precisely, allowing for better planning and improvement of service.

- To obtain up-to-date expertise, skills, and technologies cheaper and more easily

  The initial investment to structure a service or to upgrade it is usually high. By outsourcing a service that otherwise would be offered using internal resources, the outsourcee may have expertise, skills, and technology available without needing to invest in building or upgrading its own infrastructure.

- To reduce costs through superior provider performance and the provider's lower cost structure

Because service providers focus on offering the outsourced services, usually they are in better condition to perform the work. It is not only a matter of focus, but outsourcing providers can also share the cost of infrastructure between its clients to have a cheaper price, better infrastructure, and superior service level.

Outsourcing Risks and Challenges

Outsourcing has great benefits, but it also has serious risks. When considering outsourcing a company should evaluate the risks of relying on a third party for a business activity.

Quality of Service

Although the business activity is performed by a third party in an outsourcing agreement, it is important that the organization controls the quality of service. This is because the responsibility for continuous general service and product quality within the organization remains with the organization and not with the outsourcing company. This is reflected either in client response to service levels or regulatory controls from governmental agencies.

An example of the first is the outsourcing of a help desk call center where the call handlers are responsible for managing client complaints. If the outsourcing company that provides this service does not do a good job, it is the organization, and not the outsourcing company, that will lose the clients.

An example of the second is the Australian Prudential Regulation Authority, which regulates financial services companies in Australia. It states in its GPS 231 standard published in October 2006 that "the insurer remains responsible for complying with all prudential requirements that relate to the outsourced business activity," meaning that no matter what the outsourcing company does, the responsibility to its material business processes still belongs to the financial services company.

Performance Management

One of the big risks in outsourcing contracts is when the outsourcing company does not perform to the level required to maintain the organization business activity. In this case,

the organization needs to apply proper quality service management practices to guarantee the continuity of its business processes.

The most common way of managing the quality of service in outsourcing contracts is through Service Level Agreements or SLAs. SLAs are parameters that are used to evaluate the performance of a contract, and they are extensively used in outsourcing. The SLAs are agreed upon beforehand and monitored through the execution of services, giving an idea how well they were performed.

It becomes obvious how important it is to choose which SLAs to use and appropriately set their acceptable levels. Because contract penalties and other conditions are usually linked to performance, that would allow the organization to have a good idea on how the service is being executed, require improvement or corrective actions from the outsourcing company, and even terminate the contract in cases of noncompliance.

Examples of the use of SLAs to manage an outsourcing agreement would be ABA (Abandon Rate), ASA (Average Speed to Answer), TSF (Time Service Factor), and FCR (First Call Resolution). These SLAs are parameters used in Call Centers to measure their efficiency.

An organization might require, for example, that the ABA is lower than 20%. In that case, it monitors the Abandon Rate on monthly reports and, if the number is higher than 20%, it might require improvements on the call handling procedures by the outsourcing company. If the number is lower, then the service level is met and the contract is being fulfilled.

Business Continuity

Although the ultimate responsibility for performing the business activity relies with the organization, it is important to ensure that an outsourcing company provide a service even in the case of a disaster.

Guidelines such as APRA GPS 231 and GPS 222 stress that financial services organizations in Australia must ensure that companies who provide outsourcing services to them have Business Continuity Plans (BCP) and Disaster Recovery (DR) Plans to respond appropriately to incidents while maintaining a minimum level of service.

Organizations should be involved in the outsourcing company BCP and DR plans testing and have full transparent access to its results, respecting confidentiality requirements related to other outsourcing company clients. It is a good idea to have this requirement clearly stated on the outsourcing contract.

Conflicts of Interest

When an organization relies on an outsourcer, it becomes dependant on the service it provides. That trust relationship, governed by metrics such as SLAs, can be such that the interruption of the outsourcing service or breach of contract would cause a serious impact in the organization operations.

If there is any direct or indirect benefit to the outsourcer when it fails to comply with the outsourcing contract (disclosing/using client information, failing to meet SLAs, and

others), then there is a conflict of interest. This can happen when one of the outsourcer shareholders is a direct competitor of the outsourcing organization for example.

The client should have controls in its outsourcing procurement process to mitigate the risk of contracting services from outsourcers who have conflicts of interest.

Security Problems

Security is always a concern. In a good risk management strategy, the outsourcing process risk needs to be mitigated by appropriate controls. Risks in outsourcing include the following

Sharing Infrastructure with Competitors

Outsourcers can provide superior service with a lower cost than in-house operations because they have an economy of scale with multiple clients. One important point that must be observed is that many times those clients are in the same industry and could even be competitors!

A good example is the beer manufacturing industry. The detailed process for every different beer manufactured is a trade secret, and compromising it would be a serious security breach. Breweries make huge investments in developing the beer recipe, manufacturing, marketing, selling, and logistics to make a good profit.

One famous international brewery in South America decided not to use one outsourcer as part of its IT infrastructure because it considered the risk too high, because the outsourcer also had a direct competitor as client.

No matter what type of guarantees an outsourcer gives, an organization should consider the risk of having its data exposed by using a shared environment with its competitors. A threat and risk assessment should be conducted, and the risk of data compromise should be considered before outsourcing.

Offshore Outsourcing and Legislation Problems

There are some advantages to outsourcing a service to an outsourcer that is in a different country. Many developing countries have good infrastructure with low-cost skilled labor and sometime offer financial incentives to organizations willing to do business in their region. That allows not only a better return of investment, but also it sometimes is the enabler to outsourcing.

Unfortunately, there are some challenges that must be faced, such as cultural differences, low level of proficiency with the business language, and legal compliance. All these affect the organization bottom line, which should be mitigated by proper risk analysis before establishing an outsourcing contract.

Privacy Problems

One interesting case of legal compliance problem with offshore outsourcing is privacy. Different countries have different legislation, especially when it comes to consumers.

Several countries have developed strong privacy legislation and have been enforcing compliance through legal action and fines. Australia, for example, has the Privacy Act

and a Privacy Office Commissioner. In Europe, the Directive 95/46/EC of the European Parliament deals with the protection of individuals with regard to the processing of personal data and on the free movement of such data. Other countries are following the same path.

When a company in Europe decides to outsource a marketing function that uses a database with private data, it must ensure that the handling, storage, and use of this data comply with European legislation. If the outsourcer is in the United States, for example, which has different privacy requirements than Europe, the organization must be sure that it will still be compliant to European legislation.

A practical example of this situation is when an outsourcer is required to share the organization data with his local government, even if it might have a confidentiality agreement with the client organization abroad. Although the outsourcer is complying with the local law, it is making the organization abroad to be in breach of its own local law.

It is fundamental that organizations execute a risk assessment, where the cost of compliance is weighted to the probability of legal action from the customers or fines from any government agency.

Audit Rights

Whenever outsourcing a business process, an organization should detain full audit rights to it. This might sound simple, but when multiple clients use a shared infrastructure, conflicts of interest and security issues might arise.

There are cases of outsourcers denying access to its facilities or refusing to share information such as its business continuity plan to client organizations. It should be a procurement requirement that all outsourcing contracts require full audit rights on the business process!

Summary

Although there are a lot of advantages in outsourcing and it seems to be simple to establish it, there are some important steps that shouldn't be overlooked.

A Threat and Risk Analysis, where an organization looks at legal, security, and continuity risks; KPI definition and establishment, where performance metrics are set; performance and contract monitoring, where the organization ensures that the service is being executed according the specified in the procurement phase; and audits are fundamental and should not be overlooked.

Some examples of requirements and cases where these problems might arise were discussed, but every organization has its requirements, and must evaluate them individually to fully benefit from outsourcing.

Last Updated: June 29th, 2017

Upcoming SANS App Sec Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Minneapolis DEV534	Minneapolis, MN	Aug 25, 2017 - Aug 28, 2017	Community SANS
Community SANS San Francisco DEV541	San Francisco, CA	Aug 28, 2017 - Aug 31, 2017	Community SANS
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - DEV522: Defending Web Applications Security Essentials	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced