Vendor Outsourcing Technology Process

The advent of many different technologies, including virtualized computing and high-speed networks has caused a convergence of technologies and now any or all parts of a technology solution can be outsourced. These include expertise, labor, hardware and/or infrastructure, storage, operating environment, application environment or the entire service as defined below.

Expertise or Labor
Traditionally outsourced through contractors or consultants, this is probably the most well understood mechanism through which outsourcing exists, and is typically used to temporarily augment existing staff, or implement a new solution.

Hardware/Infrastructure
The most popular example of this currently is probably Amazon’s Elastic Computing Cloud (EC2), although other examples exist. Typically through a virtualized environment, this allows the user full control of the Operating system and software over it, while not having to deal with any changes in hardware and storage.

Storage
Again, Amazon’s Simple Storage Solution (S3) is usually the most well-known of the offerings. From an end user perspective, these are often just another NAS (Network Attached Storage) device, and allow for data storage to be an expandable, just in time solution.

Operating Environment
Although not seen as often in recent years, this model allows the user to focus on the application, while the provider manages all OS and hardware maintenance.

Application Environment
The application environment includes those parts of the solution that exist above the operating system layer, and are closest to the functioning of the system.

Service
The service would include all of the components above, where the University would only have an end-user perspective on the solution, and would have no part in the solution management.

The Formal Review Process
In order to assist Ohio University with understanding the potential risks that may exist when using an outsourced service, all units investigating the use of a vendor or company to process data or offer an online service must complete an Outsourcing Technology Workbook. The purpose of the vendor review is not to control the unit’s choice of vendor for an outsourced solution, but to provide an assessment of risks associated with an outsourced solution.
Upon completion of the Outsourcing Technology Workbook, results will be reviewed by the Information Security Office (ISO). If additional questions are required, ISO staff will reach out to the unit sponsor or vendor contact depending upon the nature of the follow-up questions.

Once questions are triaged and reviewed, the Vendor Security work group will meet to discuss. The work group meet twice monthly and consists of representatives from OIT, OIT Project Management and ISO. Depending upon workbook results and concerns raised by the work group additional questions or tasks may result. Technology solutions that access sensitive or restricted data may take longer to obtain approval than solutions that do not access sensitive or restricted data.

Upon approval of a vendor/solution the unit sponsor will be notified via email or an approval message through Bobcat Buy.

Things units should keep in mind when choosing a vendor:

1. Vendors that have an SSAE 16 SOC 2 or similar report are in a good position to meet security standards.
2. Vendors should have a change management policy/procedure in place for the solution.
3. Vendors should have a configuration management policy/procedure in place for the solution.
4. The vendor should have an incident response procedure, including a notification protocol to customers.
5. The solution should have an identified recovery time and point objectives for the solution in the event of a disaster.
6. The solution should have maintenance windows.
7. The ownership of data should be written into any contracts between the vendor and Ohio University.
8. The vendor should have an identified path for the university to recover any data from their solution once the contract is terminated.
9. The solution should support one of the following technologies that enable Single Sign On (SSO) capability: ADFS, CAS, or SAML; with a preference towards CAS.
10. The vendor should have a privacy policy for customer data.
11. Ideally, one customer’s demand should not impact the performance of another customer’s solution. Additionally, one customer’s outage should not impact another customer’s solution.
12. Any solutions that process, store or transmit Protected Health Information (PHI) must have a business associate agreement in place with Ohio University.
13. Any solutions that facilitate credit card processing on behalf of the university need to have an Attestation of Compliance to demonstrate their compliance with Payment Card Industry – Data Security Standards (PCI-DSS).