Vendor and Third-Party Management

Table of Contents

Getting Started

When beginning the process of evaluating supplier relationships, the following information and material will be needed:

- **Identify and document** various suppliers and the types of information that they access or manipulate. Use the Comparison of Service Organization Control (SOC) Reports table below to better understand the different types of SOC reports.
- **Identify** current policies and standards that describe or include third party responsibilities and any compliance requirements associated with external providers (e.g., HIPAA, PCI DSS).
- **Review** data classification standards (*see Supplier Service Delivery Management section*) and how these relate to the suppliers and information that they handle. Where applicable, work with your institution's risk manager and/or general counsel to ensure inclusion of information security and data protection in any supplier contracts.
- **Review or develop** a supplier lifecycle process, including initial reviews, monitoring, validation, and ongoing assessments. Reference the Risk Management chapter for assistance in modeling for a supplier lifecycle process.

Organizations with more mature programs will have some or all of this information previously aggregated.

Top of page

Overview

External suppliers are a vital component of business operations. Suppliers may have access to a wide range of information from the supported organization. Once shared with a supplier, direct control of this information is lost, regardless of sensitivity or value. As a result, appropriate technical and contractual controls and mitigation processes must be established with all external suppliers. One essential control would be to ensure the existence of a data sharing agreement that clearly delineates roles and responsibilities. Some data privacy regulations may have specific data sharing requirements that must be met. As an example FERPA (34 CFR §99.31(a)(3)) requires the execution of a written agreement with certain data protection elements that must be met. A data sharing checklist can be found on the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) website.

The contracting organization should understand that the management of external providers is a lifecycle. Part of this cycle is a process to monitor and continuously assess provider performance and compliance. A variety of tools may be used to assess and validate external supplier data protection practices. In almost all cases, some mitigation will be contractual, and requires extensive documentation.

In addition to protecting information handled and used by external suppliers, the organization must also assess service availability. If business critical data or functions are supported by an external entity, then the provider's disaster recovery processes are integral with the recovery processes of the hiring entity. Agreements regarding the return of data in the event of contract termination or unexpected closure should also be considered within the lifecycle.

Additional important elements to consider:

- Information Classification
- Incident Management
- Business Continuity Management

Top of page

Information Security in Supplier Relationships

Objective: Institutions should ensure that third parties adequately secure the information and technology resources that they access, process, and manage. This includes information sharing, defining legal obligations, and ensuring non disclosure agreements are executed to protect confidential information.

Information Security Policy for Supplier Relationships

Institutions should identify and require information security controls that specifically address external parties (contractors, service providers) gaining authorized access to the organization's information in a policy. The controls should also specify processes and procedures that should be followed, either when third party contractors work within the organization or when there are service provider/hosting arrangements.

Suppliers should be managed throughout the lifecycle of a relationship with them--from initially reviewing their contracts and security methods to monitoring their SLAs and performance agreements once they are engaged to perform services and/or provide solutions.

Access control, especially for sensitive information must be accurately defined, managed and monitored. Awareness training for both the organization's staff and supplier staff that handle or interact with this data must be addressed. Finally, service transitions should be documented and include procedures for secure data transfers and availability as the relationship changes during the lifecycle.

For additional guidance, see ISO/IEC 27036:2013+ — IT Security — Security techniques — Information security for supplier relationships and Praxiom's Third Party Service Provider Audit Tool. Materials related to NIST SP 800-171 for higher education are also available in the Resources section below.

Many (but not all) supplier relationships will involve cloud computing services and processes, which should be carefully considered as a part of Supplier Relationship Management. One essential control that the institution can implement is the development of a checklist to assess contractual cloud service providers. If regulated and/or sensitive data is being put out in the cloud, then the institution should consider obtaining formal written assurances from cloud service providers, including the regular submission of independent assessments and/or audits. The institution should always consider asking these cloud service providers for a copy of a SOC2 report, which focuses strictly on reviewing controls related to the confidentiality, integrity, and availability of information and systems. Key findings cited in the 2015 ECAR IT Service Delivery in Higher Education study reinforce the importance of this trend including:

- CIOs believe the next decade will bring a shift in their management focus from primarily managing infrastructure and technical resources to primarily managing vendors, services, and outsourced contracts.
- More than four in five institutions have moved at least one service to the cloud.
- CIOs project that cloud-based services will continue to expand widely over the next 10 years.

Comparison of Service Organization Control (SOC) Reports

	SOC 1 Reports	**SOC 2 Reports**	**SOC 3 Reports**
Purpose	Evaluate a Service Organization's controls over ***financial*** reporting	Evaluate a Service Organization's controls that affect the confidentiality, integrity, availability and privacy of ***users' data***	Same as a SOC 2
Also known as	*Statement on Standards for Attestation Engagements (SSAE), formerly known as a SAS 70 report*		
Types of Reports			
Type 1	Type 1 SSAE 16 assessments determine whether security controls are designed to meet control objectives and if the controls were in place ***at a point in time***	Type 1 reports assess the service organization's control environment and the suitability of the control design	
Type 2	Type 2 SSAE 16 assessments are the same as a Type 1 except the controls report covers a period of time – e.g six months or a year rather than a point in time	Type 2 reports does the same as a Type 1 report in addition to evaluating the effectiveness of the controls	
Intended Users of the Reports	Auditors, management of the service organization and management of the service organization's users	Parties knowledgeable about the service provided by the service organization and evaluating the effectiveness of internal controls Often requires signing of an NDA	Anyone
Professional Standard Used	SSAE 16: Reporting on Controls at a Service Organization	Attestation Standards Section 101: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy	Same as SOC2; uses Trust Services Principles

Useful Resources

- Adopting Cloud Services at NC State: Guidelines and Considerations (North Carolina State University Office of Information Technology)
- Security Considerations for Cloud Computing: A resource developed by the Higher Education Information Security Council that outlines things to think about when considering the application of cloud computing at institutions of higher education.
- Preparing the IT Organization for the Cloud: A 2015 ECAR working group paper series discussing cloud-based services.
- "The Failure of the Security Industry": An article from the April 2015 CSO Magazine by Alex Stamos (CISO, Yahoo), who shares his opinions on the current state of security products and some helpful tips in managing vendor/supplier relations.
- "Outsourcing, Procurement, and Cybersecurity": An article from April 2015 that encourages organizations to verify that vendors or suppliers provide assurance of data protection requirements and security controls.
- "Silver Lining": An August 2014 article from The Economist dealing with current and future trends of cloud computing and the effects the market is playing on the suppliers and their cloud computing offerings.
- Cloud Strategy For Higher Education: Building a Common Solution: A November 2014 ECAR publication discussing higher education IT being "in the midst of an exciting transformation. The economies of scale, resiliency, flexibility, and agility provided by cloud computing are rendering the construction and maintenance of on-premises data centers obsolete. We believe that over the next decade, the availability and advantage of new technology models will result in a substantial decrease in the use of on-premises data centers. In this document, we outline a 'cloud first' strategy for higher education IT that moves from a traditional data center model to one centered on the public cloud and cloud-based services."
- 7 Things You Should Know About Cloud Storage and Collaboration: A 2014 resource found in The 7 Things You Should Know About... series from the EDUCAUSE Learning Initiative (ELI) which provides concise information on emerging learning technologies. As the abstract states, "Higher education has seen a move from consumer-level adoption of cloud services to enterprise deployment of full-scale cloud storage and collaboration platforms. Enterprise services can now offer the convenience of cloud storage and collaboration services with single sign-on through the university's identity management system, integration with other campus services, and contractual assurances of privacy, security, and uptime. The deployment of enterprise cloud storage and collaboration services has introduced new opportunities for how academic assignments are conceived, completed, and submitted. This technology provides the opportunity for students, faculty, and researchers to bring their work wherever they go, access it instantly, and collaborate with colleagues in a private and secure digital environment."

Top of page

Addressing Security within Supplier Agreements

Supplier agreements should be established and documented to ensure there is no misunderstanding regarding both parties obligations to fulfill relevant security, legal, and/or regulatory requirements. Institutions of higher education are increasingly using outsourced services. While sensitive data processes and services might be outsourced, responsibility for the associated risk remains with the institution. Supplier agreements should include (as appropriate) clear and concise information regarding:

- The types of data being accessed and methods of access
- Definitions of data ownership and disposition throughout service lifecycle
- The organization's data classification requirements as it applies to the supplier
- Definition of acceptable uses for the data handled by the supplier
- Establishment of security incident notification requirements
- Processes and procedures for monitoring compliance with the contract requirements
- A "right to audit" the supplier or regular access to external assessments
- Conflict and defect resolution
- Required screening, training or other obligations of the suppliers' staff
- The use of subcontractors to provide services and the extension of security requirements to them

It is important to address the risk early in the procurement phase of the relationship with external parties so that roles, responsibilities and expectations can be clearly defined in agreements or contracts. The following EDUCAUSE resources may provide help with contract language and legal issues:

- Data Protection Contractual Language: An EDUCAUSE toolkit in this *Information Security Guide* that provides sample proposal and contract language for common themes related to data protection, as well as practical guidance as to when and how to consider the themes when drafting or reviewing a request for information (RFI), request for proposal (RFP) or contract.
- It's a Multicloud World: Essential Tenets for a Successful Education Cloud Environment
- The Risks of Click-Through Agreements: How Real Are They, and What to Do?
- Cloud/Crowd/Outsourcing Is Going to Eat Your Lunch
- If It's in the Cloud, Get It on Paper: Six Years Later
- Suggested Readings on Cloud Computing and Shared Services
- Legal and Quasi-Legal Issues in Cloud Computing Contracts
- Security Risk Management (EDUCAUSE resource page)
- Risk Management (EDUCAUSE resource page)
- Foundations for Effective Security Risk and Program Assessment
- Cloud Computing: Clear Skies or Rain?
- Cloud Computing Security: An Oxymoron?
- Cloud Computing Contract Issues
- Do They Measure Up? Assessing the Security Posture of Third-Party Service Providers
- Personal Storage in the Cloud
- Raising the Bar in Cloud Security for Higher Education
- Community and the Cloud: Shaping the Future of Technology Services for Higher Education

Top of page

Information and Communication Technology Supply Chain

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chains.

This section is largely physical in nature and defines additional points to include in supplier agreements, specifically related to their use of technology, both hardware and software. There should be a process to identify a product or service that is a critical capability, and require increased scrutiny. This is especially true for components built outside the supplier organization. The ability to trace origins and compliance with security requirements is integral in ensuring both integrity and availability. Finally, the organization should address the risks of a component or service becoming unavailable or no longer supported.

Supplier Service Delivery Management

Objective: Supplier agreements should be established and documented to ensure there is no misunderstanding regarding both parties' obligations to fulfill relevant security requirements.

Once operations of service providers have started, ensuring that the services delivered conform to the specifications of third-party contracts is important. This can include everything from availability levels of the service to something more granular, such as examining the security controls the service provider agreed to in the contract. If there is a great level of dependency upon third-party service providers, checking into service capabilities, plans for handling information security incidents or service disruptions, and business continuity testing may be warranted. Systematic monitoring and reviews of services and controls is also recommended, including scrutinizing service reports provided by the third-party to ensure the information is sufficient and relevant. As business or information technology requirements are modified, this may also require a change in the provision of third-party services, and procedures should be in place to handle any new requirements. Additionally, modifications may also call for a review of existing information security controls to ensure they are adequate.

Monitoring and Reviewing Supplier Services

Organizations should regularly monitor, review and audit supplier service delivery. Institutions can not overlook the need to manage the risk to their information assets that are accessed, processed, communicated to, or managed by external parties (partners, vendors, contractors, etc.). The service provider should be continuously monitored to assure that services provided are meeting the terms of the contract and security is maintained. There should be ongoing review of service reports, a process to address concerns and issues and periodic audits. This section also encompasses documentation and procedures for handling security incidents, including incident reporting, mitigation and subsequent reviews. Finally, service capability levels must be monitored to insure that the service provider continues to meet the contract terms and needs of the business. In addition to regular review and monitoring of the services provided, the contracting organization should:

- Conduct audits of suppliers in conjunction with outside assessments
- Require the supplier to promptly notify regarding security incidents
- Provide regular audit trails and records for security events
- Have a conflict resolution process that can be invoked if requirements are not met

Some external parties provide independent audits based on the Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) which focuses on the design of controls and their operating effectiveness. When independent audit opinions are not available, institutions might choose to evaluate the risk themselves.

Monitoring can mean different things to different people. It can simply mean to assess, to watch, to keep track of, or to check, usually, with a special purpose. It does not mean or imply to verify or even to test. Actually, monitoring is more of a spectrum that ranges from just "keeping an eye" in the low end to requiring a site audit in the high end. Given the availability of resources at institutions of higher education, verification could be an impractical and significantly costly requirement if applied to all or most suppliers

Effective monitoring of suppliers requires a process or methodology in place that defines the approach to take based on the risk of the supplier or engagement - activities should be more stringent and closer to the high end of the spectrum as risk increases or when exceptional situations warrant them. Institutional policy may refer to instances in which the sharing of sensitive data will result in a significant risk. Again, "significant" can mean a number of things but, ultimately, depends on the institution's risk management practices and risk tolerance (i.e., what is acceptable risk). Only in cases of very high risk or when exceptional situations may warrant it should supplier monitoring include a requirement to perform a site audit, or results of a Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) audit, or results of an audit performed by an independent auditor.

What should an institution do to monitor compliance with agreement requirements in most cases? Define the incremental risk to the institution when engaging a supplier as well as defining a due diligence process for mitigating those risks - third-party risk from remote access, data transmission and offsite storage.

Consider the following as an outline for a contract monitoring process:

1. During System / Application / Process Implementation
    a. Identify the individual(s) responsible for monitoring the relationship with the supplier.
    b. During project status meetings:
        i. Assess and review status reports regarding progress made in the implementation of the security requirements included in the contract and/or statement of work.
        ii. Identify new areas or security requirements that may arise from changes in scope
    c. If applicable, perform or request audit of vendor security practices and procedures and/or perform penetration test. It may be necessary to include a legal review by general counsel, as well.
    d. During final test and prior to sign-off
        i. Test system/application/process security functionality required in the contract
        ii. Review progress reports and determine if all security requirements included in the contract and/or statement of work were completed.
    e. If applicable, perform application scan
2. Post Implementation
    a. Follow up with system/application/process owner.
        i. Require owner to perform a risk assessment based on policy (annual if high risk or mission critical and bi-annual for the rest)
        ii. Review with the owner the risk assessment results. Any concerns? Any problems? Any unknowns that need to be addressed with the vendor?
    b. Follow up with the supplier. Access logs available? Any pending items resolved? Are things on their end as expected? Any owner concerns? Risk assessment identified deficiencies?
    c. Based on risk (annually or bi-annually), resubmit third-party information security risk assessment to assess what has changed, what needs closer scrutiny, or identify inconsistencies with previous assessments
    d. Establish a working relationship with your supplier
    e. Participate in supplier’s product improvement committee. What changes are been considered? How would they impact the institution's risk and security postures
    f. Review security incidents involving the system/application/process. Are these due to non-compliance?
    g. If applicable, based on the contract, require subsequent assurance tests.

For current established suppliers, assess their risk (if it has not already been done), and start with the steps listed in the Post Implementation section above as needed.

It is important to keep in mind that supplier monitoring is the last step of a cascading progression. The initial identification of process and data impacted as well as initial security requirements are used to formulate purchasing requirements. The answers to the requirements are used to evaluate potential suppliers and refine the security requirements. The evaluation and risk assessment of finalists refine the security requirements that will, in turn, be added as language to the contract or statement of work. And, finally, it is the final contract and corresponding risk level that determine the appropriate supplier monitoring approach.

Managing Changes to Supplier Services

All technology systems are undergoing continuous upgrade, change and repair. Changes to service provisions by suppliers should be managed and documented, taking into account the sensitivity of information and services and re-assessment of risks. The contracting organization should determine how to integrate their change management process with that of the supplier. Items to consider include:

- Service enhancements

- Bug fixes
- Use of new technology
- New development tools
- Enhanced security measures
- Change of subcontractor
- Change of physical sites

Where possible, supplier changes should be integrated with the contracting organizations change management processes.

Top of page

Resources

EDUCAUSE Resources

- An Introduction to NIST SP 800-171 for Higher Education Institutions
- Higher Education Cloud Vendor Assessment Tool (HECVAT), developed by EDUCAUSE, Internet2, and REN-ISAC members for the higher education community
- Cloud Computing, EDUCAUSE Resource Center page
- Cloud Security, EDUCAUSE Resource Center page
- Data Security, EDUCAUSE Resource Center page
- Preparing the IT Organization for the Cloud
- Security Considerations for Cloud Computing is a resource developed by HEISC that outlines things to think about when considering the application of cloud computing at institutions of higher education.
- Cloud Computing: Clear Skies or Rain? is a presentation from the 2010 Security Professionals Conference. Two universities that have moved e-mail services to "the cloud" provide a primer on this new buzz phrase, then share their forecasts for security professionals.
- NIST SP 800-171 and CUI with Ron Ross (webinar recording, slides, and chat transcript)
- NIST SP 800-171 Compliance Template (created by members of the Common Solutions Group)
- Stewards for Higher Education: Looking at Clouds & the Top-Ten Issues is an *EDUCAUSE Review* article from 2010 predominately focused on the topic of Cloud Computing.

Initiatives, Collaborations, & Other Resources

- Cloud Security Alliance Collaboration with Internet2: NET+ Initiative CCM v.3 Candidate Mappings
- Shared Assessments
- U.S. Department of Education's Privacy Technical Assistance Center (PTAC) website

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management Chapter 15: Supplier Relationships **ISO/IEC TR 14516:2002**	**800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-30 Rev. 1**: Guide for Conducting Risk Assessments **800-34 Rev. 1**: Contingency Planning Guide for Federal Information Systems **800-39**: Managing Information Security Risk: Organization, Mission, and Information System View **800-53 A Rev. 1**: Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans	**DS2** **AI5.2** **AI5.3** **PO4.15**	**Req 6.4** **Req 6.6** **Req 8.3** **Req A. 1**	**ID.AM-6** **PR.AT-3**	**45 CFR 160.103** **45 CFR 164.504** **45 CFR 164.532**

Top of page