Acquisition and Development Lifecycle

Table of Contents

- **Getting Started | Overview | Resources | Standards**
- **Security Requirements of Information Systems**
- **Security in Development and Support Processes**
- **Test Data**

✓ **Getting Started**

Security risks and events occur throughout a system's lifetime. This is true whether the system is developed internally or purchased for on premise hosting or cloud implementation. Security should be embedded throughout all phases of the system development life cycle, assessed during system acquisition processes, and monitored during system maintenance, including disposal.

System Development–For systems developed by the institution:

1. **Investigate** and review how your institution manages software development for release to the campus community.
2. **Revise** the process to ensure the security team is involved at key points in your institution's software development life cycle (SDLC). Having security "at the table" early and throughout the SDLC ensures that security requirements are designed, tested and implemented when they are the least costly. It is particularly critical to be involved in defining security requirements at the beginning of a development project and prior to implementation to validate security requirements are met.
3. **Review** Microsoft's Security Development Lifecycle that parallels the system development lifecycle and can be used to assist in developing the role of security in each of the SDLC phases.

System Acquisition–For systems purchased by the institution:

1. **Investigate and review** how your institution acquires new software. Understand the procurement processes in place when selecting vendors; particularly for cloud services.
2. **Determine** whether processes encourage proper assessment of vendor relationships and cloud environments before contracting. For example, Northwestern University has a clearly defined process for assessing vendors–Service Provider Security Assessment.
3. **Verify** that processes include acceptance criteria which will give assurances that security requirements are met.
4. **Review and evaluate** previous vendor contractual agreements for security protections. Helpful documents:

    a. Data Protection Contractual Language contains sample contractual language for contracts.
    b. Legal and Quasi-Legal Issues in Cloud Computing Contracts contains information that may be useful in specifying security requirements.

5. **Develop** a plan, if needed, for improving the contracting process with campus procurement and/or other stakeholders.
6. **See** Supplier Relationships for more information on supplier relationships and security controls.

System Maintenance–For systems maintained by the institution:

1. **Review** other chapters which contain security controls and techniques for ensuring system are adequately maintained and monitored after implementation. See: Operations Security, Communication Security, Asset Management, Access Control, Cryptography, and Physical and Environmental Security.

Top of page

Overview

To be most effective, information security must be integrated into the system lifecycle from system inception through system disposal. Regardless of the formal or informal lifecycle methodology employed, security can be incorporated into information systems acquisition, development and maintenance by implementing effective security practices in the following areas.

- Security requirements for information systems
- Security in development and support processes
- Test data

Information systems security begins with incorporating security into the **requirements** process for any new application or system enhancement whether that application is purchased from a vendor or internally developed. Designing security requirements in systems is most effective at the early stages of system development. Similarly, security requirements are presented to the vendor during the requirements phase of a product or cloud service purchase. Formal testing should be done to determine whether the product meets the required security specifications prior to purchasing the product or moving the application to production.

Security in development and support processes is an essential part of a comprehensive quality assurance and production control process and usually involves training and continuous oversight by the most experienced staff. Rules for system and software development should be developed. These rules should incorporate secure software development techniques such as user authentication, session control, logging, and data validation and sanitization. Unit, system, integration and regression testing should include testing of security requirements prior to deployment. Changes to the system as well as its operating environments should be managed, tested and approved. Support processes are closely related to Security Operations. As system maintenance occurs secure operational processes with regard to change control, separation of development, test and production environments as well as other operational controls provide many of the post implementation support processes and control.

System and acceptance testing usually requires **Test data** that is as close as possible to production data. Using production data for test data should be avoided unless mechanisms for removing or masking personally identifiable information or other sensitive information in test data is developed.

Top of page

Security Requirements of Information Systems

Objective: To ensure that security requirements are established as an integral part of the entire lifecycle of an information system.

The acquisition of a system or application often includes a Request for Proposals (RFP), which is a formal procurement process. During this process, security requirements need to be identified. Indiana University includes both a security review and a security questionnaire as part of the RFP process. Learn more about this effective practice by viewing Building Security into the RFP Process.

The University of Illinois Urbana-Champaign has developed a procurement process for evaluating whether an electronic service is considered to be low-risk, and potentially eligible for purchase using a P-Card. The criteria are included in Purchasing Software and Electronic Services with a P-Card.

Many institutions are looking to the cloud for information system solutions. Cloud Computing Security considerations are essential! Security professionals from EDUCAUSE member institutions published an excellent article, Cloud Services: Policy and Assessment, in the EDUCAUSE Review. Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide provides information to consider in evaluating the risk of moving applications to the cloud. Institutions need to perform due diligence to assess the security of cloud service providers. The Cloud Security Alliance has also published several resources to help assess security of cloud services. The Cloud Controls Matrix may prove particularly beneficial to those who are evaluating services prior to purchase.

George Mathew outlined security considerations for applications in the cloud at the 2011 Security Professionals conference. His Application Security in the Cloud session was recorded. Navigating the Clouds with an Enterprise IT Strategy, presented at the 2013 Security Professionals Conference, offers guidance from Furman University on creating a cloud security strategy. The University of Pennsylvania shared experience, lessons learned, and recommendations for creating a cloud policy, contracted solutions, and security assessments in Bring Your Own Cloud: Data Management Challenges in a Click-Through World, a presentation at the 2013 Security Professionals Conference.

As electronic commerce and online transactions become more prevalent, controls should be implemented to protect the information involved in this activity from various threats associated with this way of doing business. A review of potential information security controls that can be implemented for risk reduction should be considered, such as encryption, authorization processes, segregation of duties, network security controls, checks and balances to verify transactions, non-repudiation, etc. Care should also be taken to verify the validity and integrity of publicly available information provided over the internet, and protect this information from unauthorized access and compromises.

- Conducting Internal PCI DSS Assessments
- EDUCAUSE PCI DSS (Payment Card Industry Data Security Standard) Library Page
- Leading the Way to PCI Compliance: It's All About Planning and Collaboration

As applications are developed for mobile computing, security requirements need to be included from the beginning. Developing a Campus Mobile Strategy: Guidelines, Tools, and Best Practices is an EDUCAUSE resource that offers an excellent strategy for mobile devices, including security considerations.

An important aspect of overall information systems design involves the credentials that will be used to access the system. The InCommon Identity Assurance Profiles Bronze and Silver (IAP) document specifies requirements that Identity Provider Operators must meet in order to be eligible to include InCommon Identity Assurance Qualifiers in Identity Assertions that they offer to Service Providers. The IAP provides excellent security requirements for identity management systems. In particular, Section 4.2.3, Credential Technology specifies requirements for issuing and securing credentials. Further guidance involving credential technology can be found in NIST SP 800-63.

Top of page

Security in Development and Support Processes

Objective: To ensure that development lifecycle processes are established to maintain the security of information systems as the systems are designed, developed, tested, and maintained.

One of the security layers that can expose serious vulnerabilities is the application layer. Inventorying and securing all applications, software interfaces, or integration points that "touch" sensitive data is crucial in any organization that handles personal identity data, HIPAA, PCI, or any data that can lead to identifying confidential information. Unfortunately, this layer is subject to extensive variations and stretches across many technologies, human competencies, and organizational controls, practices, and standards. As such, it is difficult to secure and sustain, usually requiring departments to re-evaluate much of their software development, acquisition, and production control organization, staffing, and practices. Moreover, since applications are enhanced to adapt to changing business needs relatively often, even while the technology they depend on may also be changing, a consistent and "routinized" approach to maintaining their security must be adopted. Fortunately, there are many excellent resources to help organizations get started.

The Information Technology Infrastructure Library (ITIL) is one of the oldest and most mature frameworks for IT service management, and offers a wealth of best practice documents.

JIRA is a project tracking tool that is very useful for bug tracking and change management. Jira workflows can be customized and used to formalize testing procedures.

The need for highly skilled developers and support personnel cannot be emphasized enough. Security training is expensive, but can save the institution both dollars and reputation in the long run. The SANS Educational Institutions Program is a partnership that helps to lower the cost of training for higher education security professionals. Relevant courses for software developers are listed in the SANS Secure Software Development Training Curriculum. System administrators will benefit from the SANS System Administration Training Curriculum.

The OWASP Top Ten is a baseline for addressing the most prevalent web development risks. Application developers should be well trained in coding techniques that control these risks, and software purchasers should require that products not be susceptible to them. At the 2013 Security Professionals Conference, the University of Pennsylvania presented a valuable methodology for securing web applications in Proven Strategies for Web Application Security.

Top of page

Security of Test Data

Objective: To ensure the protection of data used for testing.

Data used in testing environments such as quality assurance, test and development must be protected against unauthorized access. For example, test environments may be firewalled to restricted to campus systems. Accounts may be disabled so that only a subset of accounts can be used for testing. Copying data between production and test environment should be approved. Where possible data used for testing should not contain personally identifiable information. Guidelines for Data De-Identification or Anonymization should be followed to remove sensitive information or to modify it beyond recognition when used for testing purposes. If production data is used unchanged for testing, the data should be protected with the same level of controls used for the production system.

Top of page

Resources

EDUCAUSE Resources

- Application Security and Software Development Life Cycle
- Thinking Outside the Black Box: COTS Web App Security with Apache
- Building Security into the RFP Process
- Guidelines for Data De-Identification or Anonymization
- Cloud Computing Security
- Application Security in the Cloud
- Cloud Services: Policy and Assessment
- Developing a Campus Mobile Strategy: Guidelines, Tools, and Best Practices
- Navigating the Clouds with an Enterprise IT Strategy
- Bring Your Own Cloud: Data Management Challenges in a Click-Through World
- Proven Strategies for Web Application Security

Initiatives, Collaborations, & Other Resources

- OWASP Top Ten Project
- Purchasing Software and Electronic Services with a P-Card
- Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide
- Cloud Security Alliance
- SANS Partnership and Training
- Security Tools Benchmarking

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 14**: System Acquisition, Development, and Maintenance **27034 -1 Application Security** - **Overview and Concepts**	**800-53**: Recommended Security Controls for Federal Information Systems and Organizations (specifically System and Services Acquistion-SA) **800-23**: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products **800-64**: Security Considerations in the System Development Life Cycle **800-144**: Guidelines on Security and Privacy in Public Cloud Computing	**APO01.06** **APO07.06** **APO13.01** **APO13.02** **BAI10.01** **BAI10.02** **BAI10.03** **BAI10.05** **DSS05.02** **DSS06.06**	**Req 2** **Req 3** **Req 4** **Req 6** **Req 11**	**PR.DS-2** **PR.DS-5** **PR.IP-2** **PR.IP-3** **DE.CM-6** **DE.DP-3**	**45 CFR 164.308(a)(5)** **45 CFR 164.308(a)(1)** **45 CFR 164.308(a)(8)**

Top of page