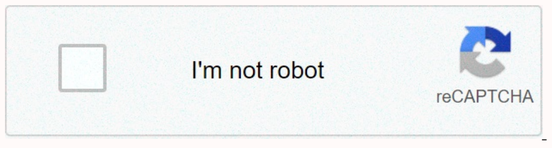

Continue

Ffiec guidelines sdlc

The system development lifecycle is a project management technology that divides complex projects into smaller, more easily managed segments or phases. Segmentation projects allow managers to verify that project phases are successfully completed before allocation of resources to subsequent phases. Software development projects typically include initialization, planning, design, development, testing, implementation, and maintenance phases. However, the phases can be divided differently depending on the organization involved. For example, initial project tasks can be designated as request, requirement definition, and planning phases, or initialization, concept development, and planning phases. End-users of the system under development should be involved in the review of outputs from each phase to ensure that the system is built to deliver the necessary functionality. Note: Reviewers should focus their assessments of development, acquisition, and maintenance activities on the effectiveness of an organization's project management techniques. Reviews should be centered on ensuring the depth, quality and refinement of a project management technique is proportionate to the characteristics and risks of the project being audited. Acquisition projects are similar to development projects because management approves project requests, defines functional, security, and system requirements, and tests and implements products appropriately. Organizations often use structured acquisition methods similar to SDLC when acquiring significant hardware and software products. However, organizations are replacing the SDLC design and development phases with a tender interior design process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties. See the Project Management and Development sections for further details related to general lifecycle phase information. In addition to developing and distributing detailed lists of functional, security, and system requirements, organizations should establish selection criteria for vendors and review the financial strength, levels of support, security controls, etc., of potential vendors before acquiring products or services. In addition, management reviews agreements and licensing agreements to ensure the rights and responsibilities of each party are clear and fair. The primary risks include insufficient requirements, an inefficient assessment of suppliers and insufficient auditof contracts and contracts. Contractual and licensing issues may arise due to the complexity of the contractual requirements. An organization's legal representative should confirm that performance guarantees, source code availability, intellectual property considerations, and software/data security issues are handled appropriately before management signs a contract. institutions sometimes obtain software or services from foreign-based third parties. Organisations should adequately manage the unique risks involved in these arrangements. For example, organizations should decide which country's laws control the relationship and ensure that they and their suppliers comply with U.S. laws that restrict the export of software applications that use encryption technology. See the Software Development And License Agreement discussion for more details on agreements and licenses. See the IT Handbook's Outsourcing Brochure on Technology Services for additional information related to foreign-based relationships from third parties. Institutions and their customers use a wide variety of applications. Such applications include central banking applications, web applications and installable applications (e.g. downloadable mobile applications). A secure software development lifecycle ensures that Internet and client-facing applications have the necessary security controls. The Institution should ensure that all applications are developed safely. In order to verify the controls have been developed and carried out appropriately, management should carry out appropriate tests (e.g. penetration tests, vulnerability assessments and application security tests) before starting or making significant changes to external applications. Issues noted from tests should be addressed before launching applications or moving changes in production. In institutions that engage third parties to develop applications, management should ensure that the third parties comply with the same controls. Applications should provide management with the following: Implement a prudent set of security controls (such as password and audit policies), audit trail of security and access changes, and user activity logs for all applications. Establish application user and group profiles unless part of a centralized identity access management system. Change or disable default application accounts during installation. Review and install patches for applications in a timely manner. Implement validation controls for data entry and processing. Integrate additional authentication and encryption controls, as needed, to ensure the integrity and confidentiality of data and non-reprehenability of transactions. Protect web or Internet-facing applications through additional controls, including web application firewalls, regular scanning for new or recurring vulnerabilities, mitigation or remedial compliance with common security vulnerabilities, and network segregation to restrict inappropriate access or connections to the application or other areas of the network. Mitigate risks from potential flaws in applications that allow remote access of customers and others through network, host, and application layer architecture considerations. Obtain certificates or evidence from third-party developers that the application submitted by the institution necessary security requirements and that identified vulnerabilities or deficiencies are addressed in a timely manner. Carry out ongoing risk assessments to consider the appropriateness of application-level controls in the light of changing threat, network and host environments. Implement minimum controls recommended by the third-party service provider and consider additional controls appropriate. Review available audit reports and consider and implement appropriate control recommendations Collect data to build metrics and reporting configuration management compliance, vulnerability management, and other measurable items as determined by management. Whether the institution acquires or develops applications, management should establish safety control requirements for new systems, system revisions or new system acquisitions. Management should define the requirements for screening based on its risk assessment process and evaluate the value of the information at risk and the potential impact of unauthorized access or damage within existing software development and procurement processes. Management should have a process for determining the risks involved in the system and the necessary safety requirements. Management may also refer to published, generally recognised industry standards as a starting point for determining the institution's safety requirements. Information security personnel should initially participate in the software development process to determine whether security controls are designed, tested and implemented and information security needs are met. Monitoring of the development environment can contribute to the proper functioning of the checks carried out. Institutions that purchase applications typically rely on third-party service providers to develop applications with appropriate built-in security; management should, however, carry out its own verification to determine whether the application meets the institution's safety requirements. Management should analyze the environment where the application will be located. When the environment changes, the safety requirements and hedging requirements for the application may also be changed. Management should use available resources to assist in risk identification and improve the institution's application safety practices. Page 2 Databases are collections of information that are organized to be easily accessible, managed and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps protect the stored information from theft or unauthorized viewing. Management should introduce or enable controls proportionate to the sensitivity of the data stored in or accessed by the database. Database users can be people (such as employees, customers, and contractors) or other applications. Users have different levels of access and Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have limitations on what they can view, manipulate, or store. When a person is the database user, authorizations can be customized to that person, which in the pile limits the amount of information that can be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Consequently, an attack on a database through an application can expose a larger and more harmful collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use. Management should appropriately control the user's access and apply the principle of least privilege in the assignment of authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program. Page 3 Encryption is used to secure communications and data storage, especially credentials and the transmission of sensitive information. Encryption can be used throughout a technical environment, including operating systems, intermediates, applications, file systems, and communication protocols. Encryption can be used as a preventive check, a detective check, or both. As a preventive check, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to enable management to detect unauthorized changes to data. When prevention and detection are associated, encryption can be an important check in ensuring confidentiality, integrity and availability. Department management should use encryption force sufficient to protect information from disclosure. Encryption methods should be reviewed at regular intervals to ensure that the types and methods of encryption remain secure as technology and threats evolve. Decisions about which data to encrypt and at which points to encrypt data are usually based on the risk of disclosure and the cost of encryption. The need to encrypt data is determined by the department's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are also hashed should be salted. Files that contain encrypted or hashed passwords used by systems to authenticate users should only be readable with elevated (or administrator) privileges. Key management is critical to the efficient use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following: Generate keys for different cryptographic systems and different applications. Generate and obtain public keys. Distribute keys to intended users, including how keys are enabled when they are received. Store keys, how authorised users have access to Change or update keys, including rules on when and how keys should be changed. Addressing compromised keys. Archiving, revoking, and specifying how keys should be retired or deactivated. Restore keys that are lost or damaged as part of business continuity management. Logging of auditing key management-related activities. To introduce defined activation and deactivation dates, and limit the usage period of the keys. Page 4 Management should conduct appropriate due diligence in selecting and monitoring third-party service providers. Management should be responsible for ensuring that such third parties use appropriate information security controls when providing services to the institution. When indicated by the institution's risk assessment, management should monitor third-party service providers to confirm that they maintain appropriate controls. Where the third-party service provider stores, transmits, processes or disposes of customer information, management should require third-party service providers to implement, by contract, appropriate measures designed to comply with information security standards. Management should evaluate information security considerations by potential third-party service providers during the first due diligence review. See the IT Handbook Outsourcing Technology Services booklet for more information. Management should verify that third-party service providers implement and maintain controls that are sufficient to adequately mitigate the risks. The institution's contracts should: Include minimum standards for control and reporting. Provide for the right to require changes to standards as external and internal environments change. Indicate that the institution or an independent auditor has access to the service provider to carry out evaluations of the performance of the service provider against the information security standards. See the Third-party reviews of technology service providers section of the IT Handbook Audit booklet for more information. In addition, as part of the oversight of third-party service providers, management should determine whether cyber risks are identified, mitigated, mitigated, monitored and reported by such third parties as third-party cyber threats may have an impact on the institution. Information security reporting by the Institution should incorporate an assessment of these risks from third parties in order to facilitate a comprehensive understanding of the institution's exposure to third-party cyber threats. Page 5 As with other forms of outsourcing, information security implications are key in the cloud computing model. Management may need to revise information security policies, standards, and procedures to incorporate the activities related to a cloud service provider. Refer to FFIEC's Statement Outsourced Cloud Computing for more information. Information.