HELP
SOURCE
Q&A

Q: I am a CISO of a financial organization. I have a question regarding application security. What are the best practices a CISO should ensure to provide assurance on application security?

A: Providing assurance on application security is a fairly complex task. Applications can be either developed in-house or through a vendor, or can be bought from the product vendor and customized to meet an organization's needs. Assurance for an application, therefore, should meet the organization's security requirements. Having said that, multiple processes need to be established and controls need to be implemented and reviewed on a regular basis or on an as-needed basis to provide assurance on application security. If the application is developed in-house or by a third-party vendor, then the controls should be in the following areas:

- Embed security in the software development life cycle (SDLC). **Figure 1** summarizes the controls to be ensured in each phase.
- When an application is in operations, require maintenance and support if needed due to changes in requirements. Organizations must ensure that a change management process is followed appropriately. Any change in application development must comply with the SDLC requirements listed in **figure 1**.
- Segregate application development, test, preproduction, user acceptance testing (UAT) and production environments physically and logically to ensure segregation of duties (SoD) between testing, development and production. This implies that developers should not have access to testing and production, testing professionals should not have access to development and production, and employees who have access to production should not have access to test and development environments.

  However, while implementing this segregation, a question may arise as to how to move the code from one environment to another for which one needs to have access to all environments. One solution is to automate the movement of code across environments or identify a team—a release team—to move codes. Release teams have access to all environments and are enabled only when such movement is required. Release teams can be associated with the project management office (PMO). In cases when this is

Figure 1—Security Controls for Each Phase of SDLC

SDLC Phase	Security Steps
Requirement definition	• Identify security requirements including compliance for privacy and data loss. • Determine risk associated with security and prepare mitigation plan. • Train users on identification and fixing of security bugs.
Design phase	• Ensure security requirements are considered during design phase (e.g., access controls for privacy-sensitive data). • Identify possible attacks and design controls (e.g., implementing least-privileged principle for sensitive data, applying layered principle for modules).
Development phase	• Develop and implement security coding practices such as inputting data validation and avoiding complex coding. • Train developers on secure coding practices.
Testing phase	• Review code for compliance of secure coding practices. • Develop test cases for security requirement testing. • Ensure security requirements are tested. • Test application for identified attacks.
Implementation phase	• Analyze all functions and ensure that interfaces are secured. • Perform security scan of application after implementation.
Maintenance phase	• Monitor for vulnerabilities on a continuous basis. • Issue patches for fixing the reported vulnerabilities accordingly. • Evaluate the effectiveness of countermeasures periodically.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

© 2018 ISACA. All rights reserved. *www.isaca.org*

not possible due to scarce resources, select individuals can be given access to different environments on an as-needed basis. This access should be disabled when not required and the activities of these individuals or teams logged and monitored.

- Conduct periodic scanning of applications and code reviews to ensure that applications are not vulnerable to known threats.
- As far as possible, avoid using production data for testing. However, when it is required, the production data must be sanitized to prevent intentional or unintentional data breaches.
- Avoid using debuggers in the production environment. When it is required, it may be used in user acceptance testing (UAT) or test environments. It may be required to identify reasons for errors during operations.
- Ensure security and version control of the application code and system documentation.
- Conduct periodic audits to help identify control vulnerabilities.

The environment in which the application will be used also needs to be secured. For example, wide area network (WAN), local area network (LAN), firewall, DMZ security needs to be established, servers need to be hardened, and processes for ensuring that the hardening of devices does not impact the production environment need to be established and implemented.

In the event that the application is procured, one should ensure that the third party that has developed the software follows these practices during application development. Acquired applications may require configuration to meet the organization's requirements. One needs to assess the risk associated with configuration and ensure that security is embedded into the process for configuration. A process of working closely with the application vendor to ensure that all aspects of vulnerabilities and security are addressed by the vendor is necessary. When vulnerabilities are discovered, a process to fix those vulnerabilities using patches is also necessary.

> "ONE NEEDS TO ASSESS THE RISK ASSOCIATED WITH CONFIGURATION AND ENSURE THAT SECURITY IS EMBEDDED INTO THE PROCESS FOR CONFIGURATION."

Although it is not easy to explain application security in a short answer, these steps, at least, can be considered while implementing application security. Also, it must be kept in mind that application security is not a one-off activity. It is a continuous process that calls for strong commitment from the organization in terms of time and resources.

© 2018 ISACA. All rights reserved. *www.isaca.org*