ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.6. Secure development environment
The organization should establish and protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Development environment includes people, processes and technology

Aspects to be considered in defining security requirements for the development environment:
- sensitivity of the data being processed, stored and transmitted;
- regulations applicable –external or internal policies;
- trustworthiness of personnel involved;
- outsourced activities;
- access control to the development environment;
- storing backups in secure offsite locations.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.7. Outsourced development
Outsourced system development should be supervised and monitored.

Development outsourcing involves risks since the process is not under the control of the organization.

The organization should have clear agreements with the software development suppliers to protect against risks and to ensure on-time delivery of the product and functionality aspects.

Control of the software development supplier depends on the risks involved:

- testing of deliverables
- auditing the supplier organization's development environment.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.8. System security testing
The organization should test security functionalities during development.

Security testing should be carried before operational implementation of the product.

For in-house developments such tests should be performed by the development team and the extent of testing should be of course proportional to the importance and nature of the system.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Control – 14.2.9. System acceptance testing
The organization should establish acceptance testing programs and criteria for new information systems, upgrades and for new versions.

New or changed systems can bring in unknown vulnerabilities.

The organization should define ***acceptance criteria*** and ***testing to ensure*** that those ***criteria are met*** before the new system is introduced.

Automated tools can be used – like code analysis tools or vulnerability scanners and security related defects should be remediated.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (2)-

Security category – 14.3. Test data

Control – 14.3.1. Protection of test data
Test data should be selected carefully, protected and controlled.

Avoid the use of operational data containing personally identifiable information or any other confidential information for testing purposes.

Guidelines of ISO/IEC 27002 for protecting operational data used for testing:
- Use the same access control procedures for test application systems as for operational systems;
- existence of an authorization each time operational information is used in a test environment;
- After testing is finalized the data no longer needed should be securely erased from the test system;
- Logging the use of operational information for testing purposes.