ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Security category – 14.2. Security in development and support processes

Control – 14.2.1. Secure development policy
The organization should develop and apply rules for the development of software and systems.

The secure development policy should address aspects like:

- Security of the development environment;
- Guidelines for secure coding that should be used;
- Security checkpoints within the project milestones;
- Security in the version control.

Unsafe coding may lead to vulnerabilities
(www.securecoding.cert.org)

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.2. System change control procedures
The organization should use a change control procedure to handle changes to systems within the development lifecycle.

A system is more vulnerable whenever it undergoes change.

A risk assessment and analysis on the impact of change should exist along with the specification of security controls needed.

Procedures for change control should address aspects like:
- authorization of changes;
- fallback arrangements;
- reviews and tests;
- version control of all software updates;
- audit trail of all changes;
- Update system documentation on the completion of the change;
- implementing changes so that disturbance to business processes is minimal

ISO/IEC 27001:2013 Information security management systems

-Security in development and support processes (1)-

Control – 14.2.3. Technical review of applications after operating platform changes
Whenever the organization is making changes to its operating platforms, critical applications should be reviewed and tested to ensure there is no adverse impact on operations or security.

Changes to operating system software should be under control.

ISO/IEC 27002 recommends to have a formal process to review the applications and test for possible vulnerabilities that may appear after a new operating system is implemented or the existing one is changed.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.4. Restrictions to changes to software packages
*The organization should discourage modifications to software packages and limit them to necessary changes. All changes should be strictly controlled***.**

Changes to software packages and especially to vendor-supplied software should be made only if there is a really critical business need to do so.

If a software package needs to be modified to suit a business need the following should be considered:
- risk assessment to identify the potential vulnerabilities;
- need for a consent from the vendor for the changes;
- if the changes result in vendor support for the software package to cease.
- retain the original of the software and make changes to a copy;
- test the software after implementing the changes before starting to use it.

ISO/IEC 27001:2013 Information security management systems
-Security in development and support processes (1)-

Control – 14.2.5. Secure system engineering principles
The organization should establish, document, maintain and apply principles for engineering secure systems for all its implementation efforts.

Security engineering focuses on the security aspects in the design of systems that need to be able to deal with possible sources of disruption, ranging from natural disasters to malicious acts.

nist.org - SP 800-160 (Systems security engineering)

Principles for security engineering have to be reviewed periodically to ensure they are still up-to-date.