ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Security category – 12.6. Technical vulnerability management

Control – 12.6.1. Management of technical vulnerabilities
The organization should be able to obtain information about vulnerabilities of its information systems, its exposure to such vulnerabilities should be evaluated and appropriate measures should be taken to address the risks.

Technical vulnerabilities being exploited is among the most common type of attacks on organizations' information systems.

ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Guidelines of ISO/IEC 27002 for the management of vulnerabilities:

- defining responsibilities for vulnerability management;
- find a suitable software to identify technical vulnerabilities;
- set timelines to react since being notified about a potential vulnerability;
- once a technical vulnerability has been identified – assess associated risks and decide actions;
- if a patch is available from a legitimate source the risks associated with installing the patch should be assessed and patches should be tested before being installed. There should be a possibility to uninstall a patch and go back to the previous state;
- if no patch is available some other actions should be taken - turning off services related to the vulnerability, changing or adding access controls (like firewalls); increasing monitoring to detect attacks and raising awareness.

ISO/IEC 27001:2013 Information security management systems
-Technical vulnerability management-

Control – 12.6.2. Restrictions on software installation
The organization should establish and implement rules for the installation of software by users.

In most organizations a certain group of users enjoy increased privileges - allowing them to install software.

But uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and security incidents.

Use of least privilege to be applied.

Rules on what types of software installations are permitted and what installations are prohibited.