ISO/IEC 27001:2013 Information security management systems
-Information security reviews-

Security category – 18.2. Information security reviews

Control – 18.2.1. Independent review of information security
An independent review of the implementation of information security should be performed from time to time and also whenever significant changes occur.

An independent review is useful to ensure that the approach taken by the organization on information security is suitable and also to find opportunities for improvement.

The review should be done by individuals that are independent from the area under review.

Results of the review should be communicated to management

ISO/IEC 27001:2013 Information security management systems
-Information security reviews-

Control – 18.2.2. Technical compliance review
The managers of the organization are required to review compliance of procedures applied in their area or responsibility with the appropriate security policies, standards and requirements.

Technical compliance review requires skilled personnel and the help of automated tools:
- Penetration tests
- Vulnerability assessments.

Technical reviews have to be done with proper planning, have to be authorized and documented