ISO/IEC 27001:2013 Information security management systems
- Internal audit-

Organizations shall perform internal audits of the ISMS at planned intervals.

Internal audit programme – schedule of internal audits for a period of time.
For the development of internal audit programme the organization should take into consideration:

- importance of activities and processes;
- results of previous audits;
- security incidents;
- security performance.

ISO/IEC 27001:2013 Information security management systems
- Internal audit-

For each internal audit:

- Scope - what activities and locations are to be audited
- Criteria – ISO/IEC 27001, information security policies, internal regulations, legislation requirements, contract requirements, etc.

Auditors have knowledge of:

- information security terminology and principles,
- risk management,
- the security controls and techniques,
- current security threats and vulnerabilities,
- relevant legislation with regards to information security and of course
- the requirements of ISO/IEC 27001 including the controls from Annex A

Auditors should be independent from activities being audited

ISO/IEC 27001:2013 Information security management systems
- Internal audit-

Results of the audit – Audit report – Communicated to top management

Nonconformities should be managed – with corrections and corrective actions.

The organization should retain documented information as evidence of performing internal audits.