ISO/IEC 27001:2013 Information security management systems
- Monitoring, measurement, analysis and evaluation-

The organization has to evaluate its information security performance and the effectiveness of the ISMS.
(*it is completely up to the organization to decide what it chooses to monitor and measure*)

Examples of what can be monitored and measured:

- information security events and out of them how many have been information security incidents;
- accomplishment of information security objectives;
- reported security vulnerabilities.

ISO/IEC 27001:2013 Information security management systems
- Monitoring, measurement, analysis and evaluation-

The information collected through monitoring and measurement has to be analyzed and evaluated to see what can be improved.

The organization shall retain documented information as evidence of monitoring, measuring, analysis and evaluation.

ISO/IEC 27004 - guidelines in evaluating the information security performance and the effectiveness of an ISMS.