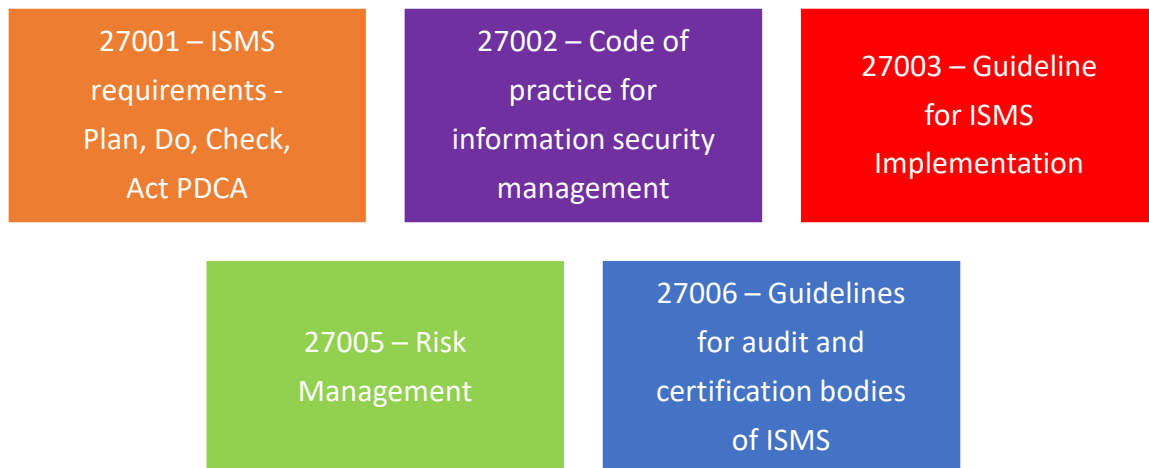


Unit 7: Basic Network Investigation Using Standard Tools

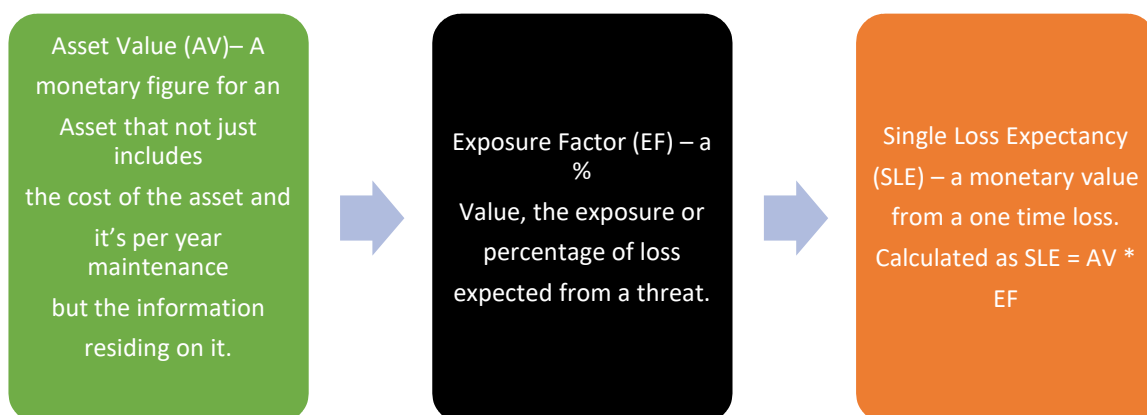
In this unit, we studied and learned about risk management and standards.

A summary of ISO Standards we discussed is as follows:



We also studied and discussed risk management.

Quantitative Risk Analysis - is determined on Single loss and Annual Loss expectations and is derived using a set of formulas.



Risk Choices

Risk Mitigation – Risk reduction or risk mitigation is the implementation of safeguards and countermeasures to eliminate vulnerabilities or block threats. We are lowering the risk to an acceptable level. In some cases, specific risks can be eliminated entirely.

Risk Transfer – Transfer risk to another organization such as insurance or outsourcing.

Risk Avoidance – Eliminating the Risk cause to avoid risk. E.g. System is open to HTTP attacks, if HTTP is not needed, the protocol can simply be disabled to prevent the risk.

We also covered Business Continuity Plan (DRP) and Disaster Recovery (DR)

The difference between BCP and DRP BCP is more high-level than DRP. DRP falls under the umbrella of BCP.

We covered Business Impact Analysis (BCP)

