ISO 27000 Series Standards

Risk Assessment	Determining the risks to organizational assets. The degree of risk is based on the impact to the asset and the likelihood of occurrence.
Security Policy	Formal statements defining the organization's security expectations.
Asset Management	Inventory and classification of information assets.
Human Resources Security	Security aspects for employees joining, moving within or for those leaving an organization.
Physical & Environmental Security	Physical systems used to protect systems and data such as alarm systems, guards, office layout, locked doors, keypads, cameras, etc.
Communications and Operations Management	Management of technical security controls in systems and networks.
Access Control	Restriction of access rights to networks, systems, applications, functions and data; maintaining the confidentiality of access credentials and the integrity of access control systems.
Information Systems Acquisition, Development and Maintenance	Building security into applications when they are designed or purchased.
Information Security Incident Management	Planning and responding appropriately to information security breaches.
Business Continuity Management	Protecting, maintaining and recovering business.

CANAUDIT
Information Security & IT Audit Consultants