An Information Security Management System (ISMS)

What to know if you're new to ISO 27001

- It is a management *system* with repeatable behaviors, *not* point in time.
- To be ready for an ISO 27001 audit you must complete the 27001 requirements.
- 27002, also known as Annex A, is based on applicability and scope of requirements.
- Plan a phase to design the controls and an implementation phase to start operating the controls.
- The minimum time to operate controls should be no less than 90 day.
- First time audit cycles should be pre-tested with a readiness assessment.
- If the readiness assessment appears to have acceptable findings, schedule an audit.

Establish the Mandatory ISMS Requirements

1. Document and approve the ISMS scope
2. Document and approve the information security risk assessment and management process
3. Conduct remaining risk assessments and produce risk assessment report
4. Document (through internal tools) risk management plan
5. Document and approve an internal audit methodology, plan, report, and non-conformity document, management review procedure, and ISMS measurement practices
6. Document the latest version of the Statement of applicability
7. Conduct internal ISMS audit
8. Conduct management review of ISMS
9. Collect evidence of measurement of the ISMS controls and processes (as much as possible)

Continuous ISMS Operation

- Ensure information security objectives identified because of continuous information security risk assessment process are reported to the highest management level in a timely manner.
- High level information security objectives, if changed, must be reflected in the Information security policy.
- Specific objectives can be defined and monitored about each ISO 27001 Annex A control or control group.
- Ensure each risk treatment activity has clearly allocated resources with responsibilities and timelines.
- Identify the best support tools for efficient execution of approved corrective actions after an internal audit.
- Consider encouraging the employees in proposing ISMS controls and processes improvements through awards, recognition in internal newsletter, presentations, etc.