ISMS Implementation plan/activites
Kick-off meeting x 1
Form an "ISMS committee"
Awareness x 4
What is ISMS (ISO/IEC 27001)?
What is the applicable legislation?
WHY ISMS related to you?
IT Assets management x 10
"All" assets should be identified
Asset classification guideline
Labeling and handling procedures
Asset inventory (for important assets)
with "Owner" information
Risk Assessment x 20 on :
Business process (IT)
Business impact analysis
BCM framework
IT assets
Risk assessment methodology
Identify the possible threat and vulnerabilities
Decide the risk acceptable level
Risk assessment report
Statement of Applicability (SoA)
Risk treatment plan
Preparation of ISMS documentation (around 30 documents) x 15
Control of documents and records
Organizational security and 3rd-party related policy and procedure
Human resources security related policy and procedures
Physical and Environmental security related policy and procedure
Communications and Operations management related procedures
Access control related policy and procedures
Information system acquisition, development and maintenance related procedures
Training x 4
ISMS Policies and Procedures
Control objectives and Controls
Technical related (Competence)
IT - networking, system, application and Database
Internal Auditor
Information Security Incident management x 4
Reporting on information security event
Reporting on weakness
Collection of incident records
Learning form incident
Business continuity management x 4
BCPs and test
Internal Audit x 4
Audit team competence and selection
Audit programme
ISMS internal audit(s)
Continual improvement x 4
Corrective actions
Preventive actions
Management review
Pre-Audit x 2
Certification process