Implementation of Information Security Management System in Government & Critical Sectors as per ISO 27001 : Progressive Steps

- Identification of a Point-of-Contact (POC) / Chief Information Security Officer (CISO) for coordinating information security policy implementation efforts and communication with CERT-In
- Information Security Awareness Programme
- Determination of general Risk environment of the organization (low / medium / High) depending on the nature of web & networking environment, criticality of business functions and impact of information security incidents on the organization, business activities, assets / resources and individuals
- *Status appraisal and gap analysis against ISO 27001 based best information security practices*
- *Risk assessment covering evaluation of threat perception and technical & operational vulnerabilities*
- Comprehensive risk mitigation plan including selection of appropriate information security controls as per ISO 27001 based best information security practices
- Documentation of agreed information security control measures in the form of information security policy manual, procedure manual and work instructions
- Implementation of information security control measures (Managerial, Technical & operational)
- Testing & evaluation of technical information security control measures for their adequacy & effectiveness and audit of IT applications / systems / networks by an independent information security auditing organization (penetration testing, vulnerability assessment, application security testing, web security testing, LAN audits, etc)
- Information Security Management assessment and certification against ISO 27001 standard, preferably by an independent & accredited organization