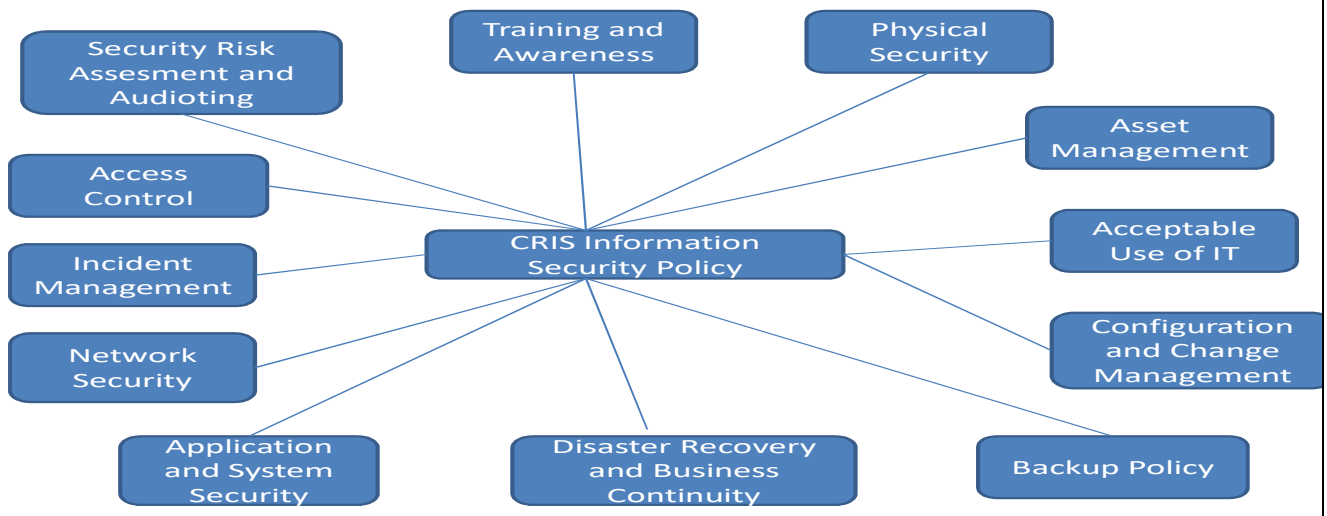
Information Security



IS Audit of **all Applications and ICT Infrastructure** (HW, SW, NW), Compliance checks for these IS Audits. Users **Awareness**, Training, Self-Audits (by Tools);	for Indian Railways
Audits **periodicity**, Internal and External;	at least Yearly
Incident Monitoring, **Reporting**, Drills, **Alerts**, Advise;	RB, CERT-In, NCIIPC

Scope : Systems under management of CRIS

Timelines : Security is not an one-time Project, its an '<u>on-going Process</u>' in /for the Organisation.

Security Tools implemented /In Use

: HP-Fortify (Source Code Analyser), Web-Inspect (Dynamic Application Security Testing), NESSUS and Nipper (Configuration Audit Tools), Metasploit (Penetration Testing Tool), N-Map, ZAP, Vega, Paros etc.

Information Security Group (Roles)	Benefits (CRIS & IR)
CRIS had an approved Info-Sec Policy (v6.2), far more specific & stringent than the IR Info-Sec Policy (2007), for all Systems, Application and Network under its purview. Control processes for Physical, HR, SW, HW, NW security, their Implementation to ensure Confidentiality + Integrity + Availability (CIA) is done & Audited, with ISO-27001 Certification in mind. Periodic Security Risk Assessment, Auditing & Compliances are done for all Projects & Groups, by Internal & External Auditors.	• Ensure Info-Sec preparedness /postures. • Enhance Info-Sec awareness in CRIS. • Compliance to various Govt. Regulations. • Safety of Customer Data /Info. • Max. availability of Systems to IR Users. • Protection from Internal and External Risks /Threats to Information.