

## INFORMATION SECURITY

**Information Security.** We are living in an information age. Information is the competitive advantage that an entity has over others. Increasingly it's protection is becoming a regulatory requirement as well. As information takes myriad forms and becomes all pervading, and the world gets ever more connected, the risks associated with this information multiply manifold. All this information brings with it enormous risks in terms of maintaining the confidentiality, integrity and availability of the data, as well as ability to recover in case of any disaster.

How does one manage risks associated with handling all this information? As per a recent survey, 59% of security risks emanate from within the organization by employees or others who are legally within the organizational LAN. How does one protect one's information in such a scenario? With people, process and technology constantly throwing up issues, no information is safe. With daily new threats coming up, how does one minimize the risk to one's business and control the damage? How does one ensure business continuity?

The answer lies in implementing measures for information security. The answer lies in ISO 27001, the de-facto standard today for information security. **Information Security** consists of all the activities we perform to protect the important information assets from loss of confidentiality or integrity or unavailability. This also covers the equipment on which these reside and the people who are critical for running the business from business continuity point of view. The organization needs to ensure business continuity in the event of a disaster. Thus **disaster recovery (DR)** is also a part of information security management.

Central to the implementation of any information security system is the concept of risk management. Risk management contains all the coordinated activities, which an organization performs to manage and control risk.

The traditional steps in risk management are :

- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication

**CampCorp™** provides comprehensive **management and process consulting, learning, audit and implementation facilitation** to its customers in the area of **Information Security, Risk management and Disaster Recovery.**

Area	Modules	Duration (Hours)
Consulting	ISO 27001 (ISMS)	12 - 15 days
Audits / Assessments	ISO 27001 (ISMS)	1-5 days
	Gap Analysis	1 – 2 days
Trainings	Overview of ISO 27001	4 / 8 hrs
	Internal Auditors training	16 hrs
	Information Security Awareness	4 hrs
	Risk Management Workshop	8 hrs
	Business Continuity Planning	4 hrs
	Disaster Recovery	4 hrs