

IT RISK MANAGEMENT

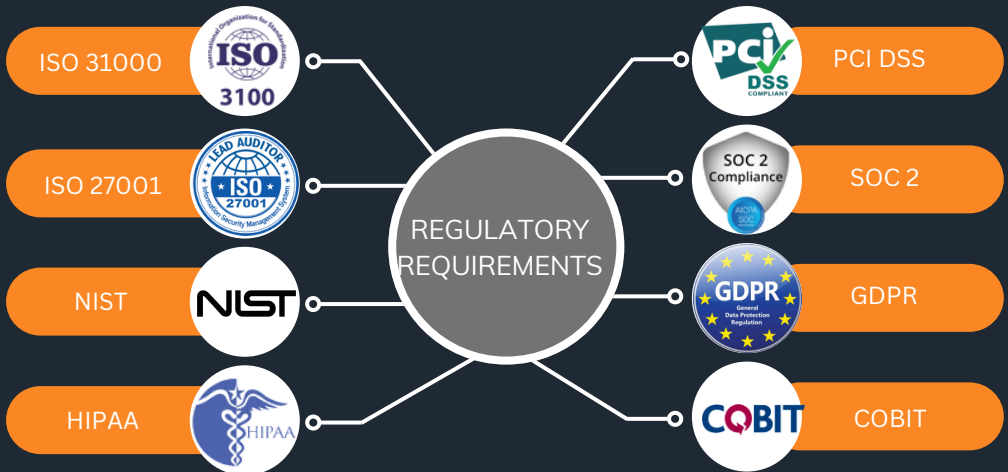
Information systems are subjected to serious threats which have adverse effect on organizations. An incident can drastically impact an organization's business with enormous regulatory fines, reputation loss and customer trust issues.

Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk.

IT risk management entails a process for the organization of identifying, monitoring and managing potential information security or technology risks with the goal of mitigating or minimizing the negative impact.

OBJECTIVES

- 1.To identify and monitor relevant threats to the organization.
- 2.Manage complex structures of compliance requirements for standards such as ISO 27001, NIST, HIPAA, PCI DSS, SOC 2 and GDPR.
- 3.Integrate with mitigation actions and remediation controls with organizational IT and security systems.
- 4.Helps in managing the level of cyber security incidents.
- 5.Formalize the organization in preparing strategic security roadmap.



GET IN TOUCH



+918800377255

info@cybersrcc.com

www.cybersrcc.com

DOMAINS

- Physical and Environmental controls
- Logical access Controls
- Operating System/database review including Vulnerability
- IT Governance
- IT Policy
- Information & Cyber Security
- IT Operations
- Internal Audit
- BCP
- IT Services Outsourcing
- Reporting Cyber Incidents
- Third-party/ vendor risk assessment

METHODOLOGY



Scope
Identification



Risk
assessment



Risk
treatment



Recording &
Reporting



Maintenance

SERVICE OFFERING



GET IN TOUCH



+918800377255

info@cybersrcc.com

www.cybersrcc.com