1. General Data Protection Regulation (GDPR) Overview:

Is the EU law that deals with the use of personal data, its protection, and the security of the same.
Implications: Imposes encryption, breach notifications, and privacy by design; failure to which attracts huge penalties.
2. The Health Insurance Portability and Accountability Act or HIPAA Overview:
Safeguards the health information of patients in the United States.
Implications:
This is done through setting up of measures and precautionary measures, risk evaluation and staff education; failure to adhere to these would attract penalties as well as harm to the reputation.
3. Sarbanes-Oxley Act (SOX) Overview:
Focuses on finance data protection and business reporting of US companies.
Implications:
IT controls and audits are necessary; penalties for violation include fines and heads of offending organizations.
4. Computer Fraud And Abuse Act Overview:
Makes it a criminal offense to access computer systems in the United States without an authorization.
Implications:
Regulates the monitoring, access control and handling of incidents; offenders, subject to fines and imprisonment.

5. Physical Security Standards (ISO/IEC 27001 & CPTED)

Overview:

ISO/IEC 27001: Focuses on information security management.

CPTED: Reduces crime through secure facility design.

Implications: Promotes secure physical environments and compliance to safeguard critical assets.

Impact on Organizations

These laws push organizations to adopt robust security measures, train employees, conduct audits, and ensure compliance to avoid penalties, legal action, and reputational damage.