Information Security and Network Security

Chapter – 1

Introduction to Information Security

Security frame works

In Software development a framework is defined as a Support structure in which another Software Project can be organized and developed.

Another definition of framework – A fundamental Structure, as for a written work and A set of assumptions concepts, values and practices that Constitutes a way of viewing reality.

Framework is linked to demonstrable work. Frame works set assumptions and practices that are designed to directly impact implementations.

COBIT- Control OBject for Information and related Technology. COBIT is a frame work standard developed in 1996 by the Information System Audit and Control Association (ISACA) and the IT Governance Institute.

1) COBIT provides a framework for users and IT a Security and auditing Managers.

2) It is gaining acceptance as a good practice for controlling data, systems and related risks.

3) The framework includes tools to measure a company's capabilities IT process / high level control objectives

4) It addresses a lot of elements of security and it focuses on Infosec

5) Experts and users of COBIT feel that it does not provide details of the 'how' that is it gives detail of controls and objectives of controls but does not explain how to implement them.

The information security framework (ISF) defines the approach, quidding principles, role and responsibilities set forth by the ICRC to manage an information Security risk, in order to protect ICRC information and information systems against loss of confidentiality, integrity and availability. (ICRC – International committee of the Red Cross)

All technical, organizational and legal rules and measures aiming to ensure the security of information and information systems shall be guided by the information security framework.

The information security framework applies to all information systems managed or approved by ICRC and used by internal staff, partners, and beneficiaries.

It does not apply to the use by beneficiaries or partners of systems that are neither managed, nor approved by the ICRC.

All internal staff should familiarize themselves with, and must respect the information security framework and principles and other relevant information security policies and guidelines enabling them to meet their obligations, under the ICRC's code of conduct signed all staff.

The information security framework, the ICRC rules on personal Data protection, the framework for the management of documents and information at the ICRC the information

handling Typology Rules and other Specific guidelines on the security of ICRC information and information systems are mandatory as well.

Steps in a continuous process and any information systems management process

1.Identify

- Asset management
- Business Environment.
- Governance
- Risk management
- Risk Management Strategy

2.Protect

- Access control
- Awareness and training
- Data security
- Information protection process and procedures
- Maintenance
- Protective technology

3.Defect

- Anomalies (denotes) & Events
- Security Conations monic turns
- Detection processes

4.Respond

- Response Planning
- Communication
- Analysis
- Mitigation- Dotson to reduce severity / Seriousness
- Improvements

5.Recover

- Recovery planning
- Improvements
- Communications