layer. Each shaded band is a layer of protection and control.

4. Discuss in detail about NIST security models publications. (NOV/DEC 2014)

NIST Security Models

NIST refers to "The National Security Telecommunications and Information systems Security Committee" document. This document presents a comprehensive model for information security. Another possible approach available is described in the many documents available from the Computer Security Resource Center of the National Institute

for Standards and technology. NIST documents are publicly available at no charge and have been available for some time, they have been broadly reviewed by government and industry professionals, and are among the references cited by the federal government when it decided not to select the ISO/IEC 17799 standards.

The following NIST documents can assist in the design of a security framework:

- **NIST SP 800-12 :** An Introduction to Computer Security: The NIST Handbook
- **NIST SP 800-14 :** Generally Accepted Security Principles and Practices for Securing IT Systems
- **NIST SP 800-18** : The Guide for Developing Security Plans for IT Systems
- **NIST SP 800-26**: Security Self-Assessment Guide for IT systems.
- **NIST SP 800-30**: Risk Management for IT systems.

NIST Special Publication SP 800-12

SP 800-12 is an excellent reference and guide for the security manager or administrator in the routine management of information security. It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

NIST Special Publication SP 800-14

. It provides best practices and security principles that can direct the security team in the development of **Security Blue Print**. The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail:

Security Supports the Mission of the organization

Failure to develop an information security system based on the organization's mission, vision, and culture guarantees the failure of the information security program.

Security is an integral element of Sound Management

Effective management includes planning, organizing, leading, and controlling. Security enhances management functions by providing input during the planning process for organizational initiatives. Information security controls support sound management via the enforcement of both managerial and security policies.

Security should be cost-effective

The costs of information security should be considered part of the cost of doing business, much like the cost of the computers, networks, and voice communications systems. These are not profit-generating areas of the organization and may not lead to competitive advantages. Information security should justify its own costs. The use of security measures that do not justify their cost must have a strong business justification (such as a legal requirement).

Systems Owners have security responsibilities outside their own organizations

Whenever systems store and use information from customers, patients, clients, partners, or others, the security of this information becomes the responsibility of the owner of the systems. Each system's owners are expected to diligently work with those who have systems that are interconnected with their own to assure the confidentiality, integrity, and availability of the entire value chain of interconnected systems.

Security Responsibilities and Accountability Should Be Made Explicit

Policy documents should clearly identify the security responsibilities of users, administrators, and managers. To be legally binding, the policies must be documented, disseminated, read, understood,
and agreed to by all involved members of the organization.

Security Requires a Comprehensive and Integrated approach

Security personnel alone cannot effectively implement security. Security is everyone's responsibility. The three communities of interest (information technology management and professionals, information security management and professionals, and users,managers, administrators, and other stakeholders) should participate in the process of developing a comprehensive information security program.

Security Should Be Periodically Reassessed

Information security that is implemented and then ignored is considered negligent, the organization having not demonstrated due diligence. Security is an ongoing process. To be effective against a constantly shifting set of threats and a changing user base, the security process must be periodically repeated. Continuous analyses of threats, assets, and controls must be conducted and new blueprints developed. Only thorough the preparation, design, implementation, eternal vigilance, and ongoing maintenance can secure the organization's information assets.

Security is constrained by Societal Factors

There are a number of factors that influence in the implementation and maintenance of security. Legal demands, shareholder requirements, even business practices affect the implementation of security controls and safeguards. For example, security professionals

generally prefer to isolate information assets from the Internet, which is the leading avenue of threats to the assets, but the business requirements of the organization may preclude this control measure.

NIST SP 800-18

The Guide for developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework. It provides detailed methods for assessing, and implementing controls and plans for applications of varying size. It can serve as a useful guide to the activities and as an aid in the planning process. It also includes templates for major application security plans

System Analysis

- System Boundaries
- Multiple similar systems
- System Categories

Plan Development All Systems

- Plan control
- System identification
- System Operational status
- System Interconnection/ Information Sharing
- Sensitivity of information handled
- Laws, regulations and policies affecting the system

Management Controls

- Risk Assessment and Management
- Review of Security Controls
- Rules of behavior
- Planning for security in the life cycle
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

Operational Controls

- Personnel Security
- Physical Security
- Production, Input/Output Controls
- Contingency Planning
- Hardware and Systems Software

- Data Integrity
- Documentation
- Security Awareness, Training, and Education
- Incident Response Capability

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

Management controls

It addresses the design and implementation of the security planning process and security program management. They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

Operational controls

It deals with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning. They also address personnel security, physical security, and the protection of production inputs and outputs.

They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls

It address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information. They address the specifics of technology selection and the acquisition of certain technical components.

They also include logical access controls, such as identification, authentication, authorization, and accountability. They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed. Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.