中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 1
Introduction to Information Security

Web Security: *Principles & Applications*

School of Data & Computer Science, Sun Yat-sen University

Outline

- 1.1 Concept of Information Security
- 1.2 Computer System Security
- **1.3 Information Security Service**
  - Basic Concepts
  - Authentication
  - Access Control
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
- 1.4 Information Security Management, Audit and Protection
- 1.5 Conclusion

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - Information Security Service includes management service, operational service and technical service.
    - ✧ Organizations frequently must evaluate, select, and employ a variety of Information security services in order to maintain and improve their overall Information security programs.
    - ✧ Information security services (e.g., security policy development, intrusion detection support, etc.) may be offered by an information group internal to an organization, or by a growing group of vendors
      - ◌ 信息安全服务可以由机构内部设立的专门信息小组提供，越来越多的供应商也可提供此类服务。

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - Information Security Service Categories

Management Service	Techniques and concerns normally addressed by management in the organization's computer security program. They focus on managing the computer security program and the risk within the organization.
Operational Service	Services focused on controls implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and rely on management activities and technical controls.
Technical Services	Technical services focused on security controls a computer system executes. These services are dependent on the proper function of the system for effectiveness.

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - 信息安全服务
    - ✧ 信息安全服务指适应安全管理的需要，为企业、政府提供全面或部分信息安全解决方案的服务。信息安全服务应当提供包含从宏观的安全体系策略规划到具体的技术解决措施。
    - ✧ 目前，国内机构中的信息安全建设多数处在初级阶段，缺乏合理规划和管理机制。国内的信息安全服务商提供的安全服务体系一般包括信息安全评估、加固、运维、教育培训、风险管理等。用户购买安全服务的直接动机是应付当前的安全事件、满足管理层的意志或减轻来自内外的舆论压力，服务形式内容和现实需求之间存在较大落差。

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - 信息安全服务
    - ✧ 当前的信息安全服务主要在技术方面提供对用户的帮助，对管理机制的影响有限。用户普遍遇到的最大问题是自身资源不足，亦即“安全管理员”的缺位，其次是对基本管理体系探索的需求。
    - ✧ 从用户的角度看，信息安全服务主要用于弥补用户在人力、技术、信息、管理思想等方面上的不足。这些服务内容主要通过安全服务团队特别是一线人员传递到用户的手中，安全服务人员的技术技能和态度将直接决定用户的收益。
    - ✧ 信息安全产品服务包括解决方案设计、安装调试、人员培训、系统升级以及再服务，具有相当长的持续周期。

1.3 Information Security Services

1.3.2 Basic Issues

- **Authentication**
  - What's Authentication
    - ✧ In computing, e-Business and information security is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

1.3 Information Security Services

1.3.2 Basic Issues

- **Authentication**
  - 认证
    - ✧ 认证技术通过某种特征识别方法确认用户 (如雇员、代理、软件过程等) 身份，从而确定其权限和服务。
  - 基本认证方法：

    (1) 双重认证。采用两种 (或以上) 形式的验证方法，如令牌、智能卡和仿生装置 (视网膜或指纹扫描器)。

    (2) 数字证书。用于检验用户身份的电子文件。数字证书通过授权购买，提供更强的访问控制，并具有很高的安全性和可靠性。

    (3) 智能卡。

    (4) 安全电子交易协议 (SET)。

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - What's Access Control
    - ✧ Access control is a system that enables an authority to control access to areas and resources in a given physical facility or computer-based information system.
    - ✧ An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - 访问控制
    - ✧ 访问控制是针对越权使用资源的防御措施，阻止未被授权的人员使用资源。
      - ◌ 硬件资源：处理器、路由器、存储器；
      - ◌ 软件资源：系统软件、应用程序；
      - ◌ 信息资源：数据文档、系统文档；
      - ◌ 网络资源：局域网、因特网；
      - ◌ 服务资源：计算、通信、电源。
  - 访问控制的基本目标
    - ✧ 防止对任何资源进行未授权的访问，从而使计算机系统在合法范围内使用；决定用户被允许的行为，也决定代表一定用户的程序被允许的行为。

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - 访问控制对 CIA 三元组的作用
    - ✧ 访问控制对机密性、完整性起直接的作用。
    - ✧ 访问控制通过对以下信息行为的有效控制来实现可用性：

      (1) 颁发影响网络可用性的网络管理指令。

      (2) 占用资源。

      (3) 获得可以用于拒绝服务攻击的信息。

1.3 Information Security Services

1.3.2 Basic Issues

- **Confidentiality**
  - What's Confidentiality
    - ✧ Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
    - ✧ Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

1.3 Information Security Services

1.3.2 Basic Issues

- **Integrity**
  - What's Integrity
    - ✧ In information security, integrity means that data cannot be modified undetectably.
    - ✧ Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

1.3 Information Security Services

1.3.2 Basic Issues

- **Integrity**
  - 数据完整性
    - ✧ 数据完整性是信息安全的三个基本要点之一，指在传输、存储信息或数据的过程中，确保信息或数据不被未授权篡改或在篡改后能够迅速被发现。在信息安全领域使用过程中，常常和保密性边界混淆。
    - ✧ 以普通 RSA 对数值信息的加密为例，黑客或恶意用户在没有获得密钥破解密文的情况下，可以通过对密文进行线性运算，相应改变数值信息的值。
      - ◌ 例如交易金额为 X 元，通过对密文乘2，可以使交易金额成为2X (也称为可延展性 malleability)。为解决以上问题，通常需要使用数字签名或散列函数对密文进行保护。

1.3 Information Security Services

1.3.2 Basic Issues

- **Availability**
  - What's Availability
    - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

1.3 Information Security Services

1.3.2 Basic Issues

- **Non-repudiation**
  - What's Non-repudiation
    - ✧ In law, non-repudiation implies one's intention to fulfill their obligations (义务) to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
    - ✧ Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

Outline

- 1.1 Concept of Information Security
- 1.2 Computer System Security
- 1.3 Information Security Service
- **1.4 Information Security Management, Audit and Protection**
  - Information Security Management
  - Information Security Audit
  - Levels of Information Security
- 1.5 Conclusion

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Concepts**
  - Information Security (ISec)
    - ✧ describes activities that relate to the protection of information (and information infrastructure) assets against the risks of loss, misuse, disclosure or damage.
  - Information Security Management (ISM)
    - ✧ describes controls that an organization needs to implement to ensure that it is sensibly managing these risks.
  - Information Security Management System (ISMS)
    - ✧ a set of policies concerned with information security management or IT related risks.

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Concepts**
  - 信息安全管理 (ISM)
    - ✧ 信息对于任何组织或机构都是非常有价值的财产 (信息资产)，不管它是打印或写在纸上、存储在电子设备中或通过邮件发送等不同的形式。信息系统是由计算机及其相关和配套的设备、设施构成的系统或者网络，按照一定的应用目标和规则对信息进行存储、传输、处理。如何对信息系统的信息安全问题进行有效的管理就成为了迫在眉睫的问题，也促成了信息安全管理的产生。
    - ✧ 组织或机构为了规避信息所面临的威胁和风险所采取的管理控制行为就是信息安全管理 (ISM)。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Concepts**
  - 信息安全管理体系 (ISMS)
    - ✧ 信息安全管理体系 (ISMS) 遵从 ISO/IEC 27001 标准，是与信息安全管理或者信息技术风险相关的策略的集合，是信息安全管理的方法体系。
  - 国际和国家标准
    - ✧ IEC -International Electrotechnical Commission 国际电工委员会
    - ✧ GB/T22080-2008《信息技术 安全技术 信息安全管理体系要求》
    - ✧ GB/T22081-2008《信息技术 安全技术 信息安全管理实用规则》

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Goals of ISM**
  - 信息安全管理的目标
    - ✧ A basic goal of ISM is to *ensure adequate information security* (确保足够的信息安全). The primary goal of information security, in turn, is to protect information assets against risks, and thus to maintain their value to the organization.
    - ✧ 基本目标是建立、实施、运行、监督、评审、保持和改进信息安全，即保证足够的信息安全。信息安全管理的主要目标则是保护信息资产免受风险，以此来保持它们对于组织机构的价值，即保密性、完整性和有效性。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则
    - ✧ The Principle of ISM is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.
    - ✧ ISO/IEC 27001 is an ISMS standard.

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则
    - ✧ 信息安全管理的总体原则是设计、实施和维护一套连贯的策略、流程和系统来管理信息资产风险，从而保证信息安全风险的可接受水平。
    - ✧ GB/T 20269-2006《信息安全技术 信息系统安全管理要求》规定了信息安全管理的11个原则。

    (1) 基于安全需求原则

      - ◌ 组织机构应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及所面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当平衡安全投入与效果。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则

(2) 主要领导负责原则

- 主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作于各部门工作的关系，并确保其落实、有效。

(3) 全员参与原则

- 信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则

(4) 系统方法原则：

- 安装系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标和有效性和效率。

(5) 持续改进原则：

- 安全管理是一种动态反馈的过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则

(6) 依法管理原则：

- 信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

(7) 分权和授权原则：

- 对特定智能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会，任何实体 (如用户管理员、进程、应用或系统) 仅享有该实体需要完成其任务所必须的权限，不应享有任何多余的权限。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则

(8) 选用成熟技术原则：

- 成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的错误。

(9) 分级保护原则：

- 按等级划分标准确定信息系统的安全等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Principles of ISM**
  - 信息安全管理的原则

(10) 管理与技术并重原则：

- 坚持积极防御和综合规范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

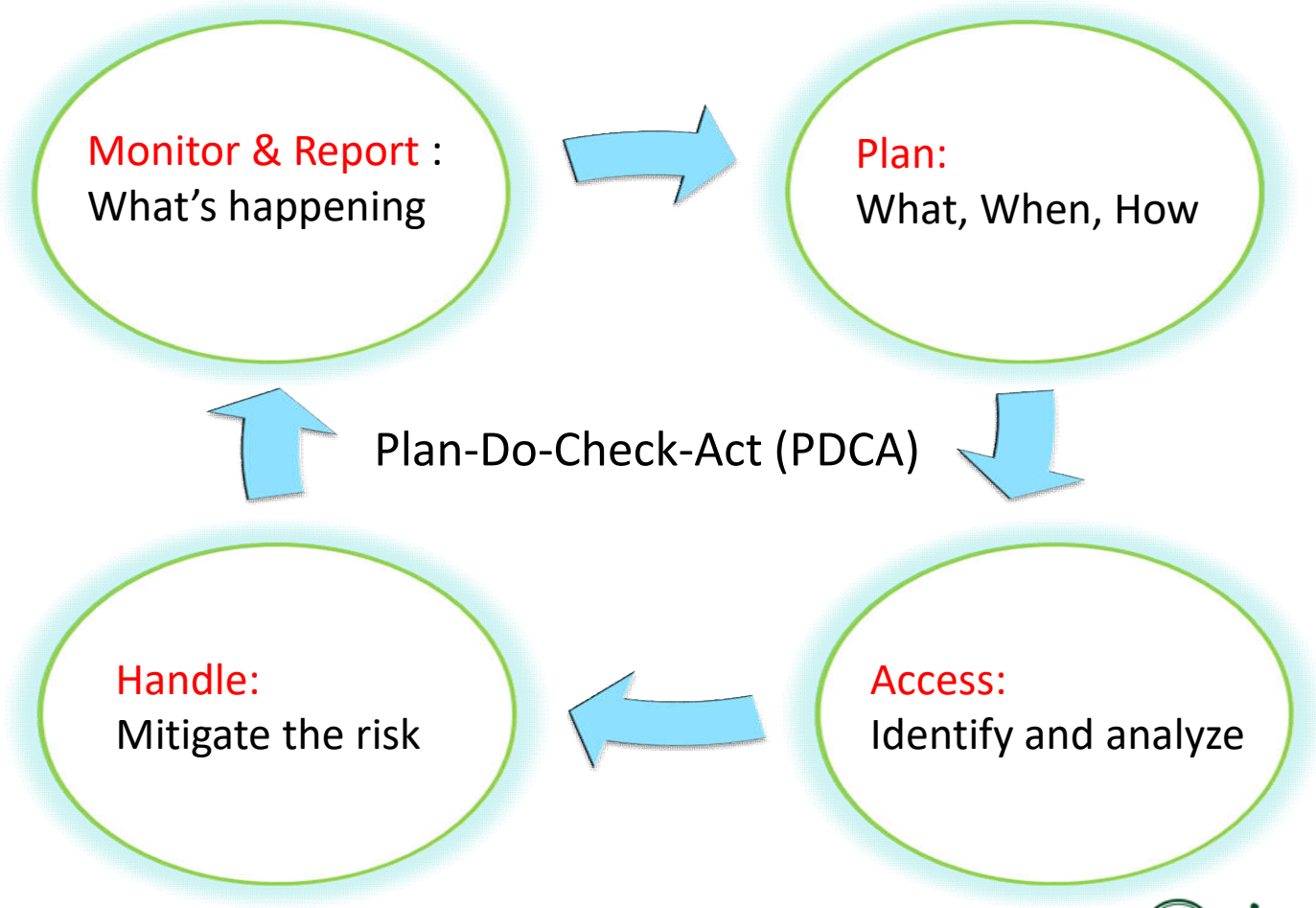
(11) 自保护和国家监管结合原则：

- 组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- **Implementation of ISM**



1.4 Information Security Management and Audit

1.4.1 Information Security Management

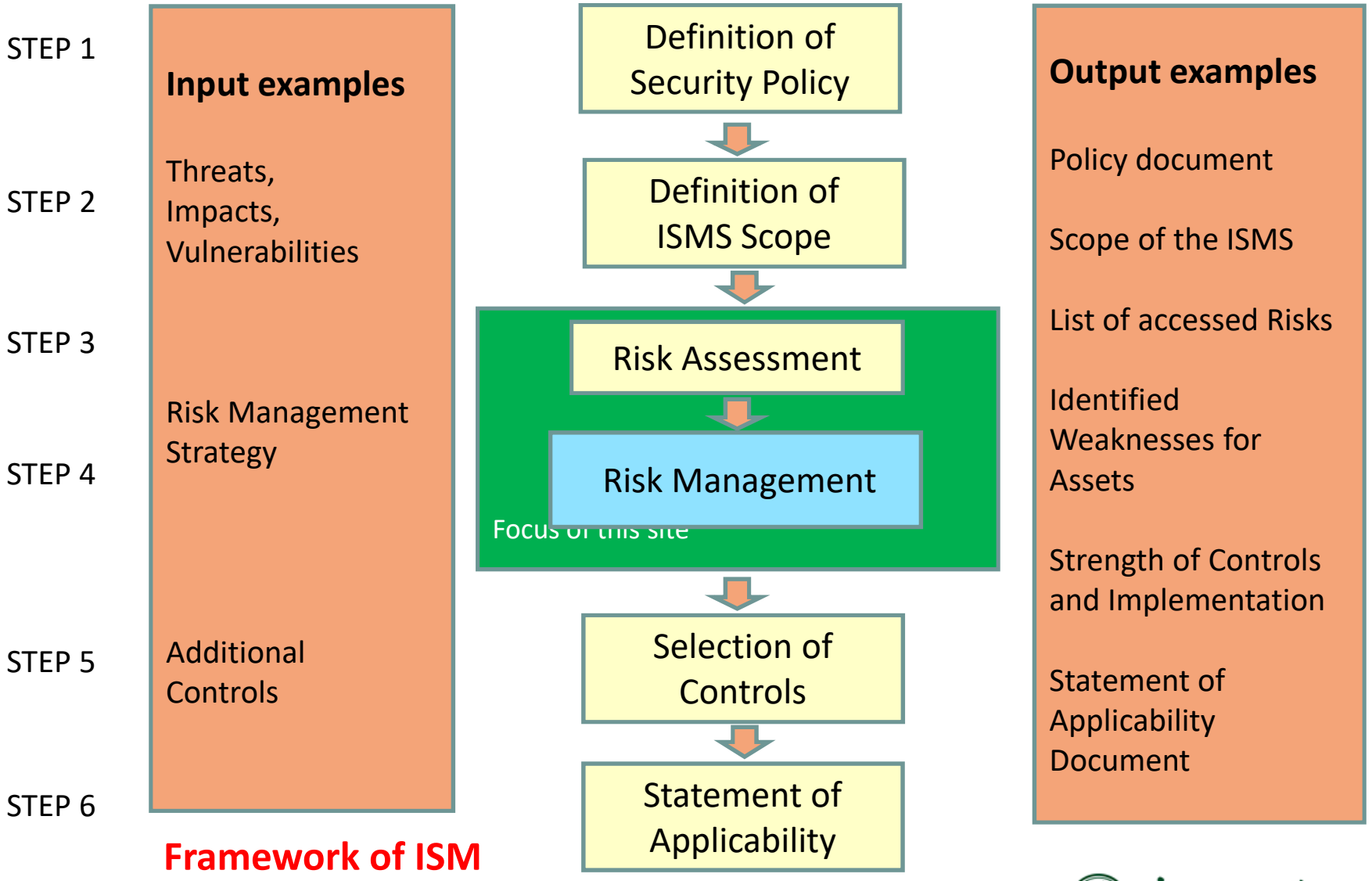
- 信息安全管理体系的实施
  - 戴明环
    - ✧ 实施过程可以用 PDCA (Plan-Do-Check-Act) 循环表示，PDCA 循环又叫戴明环，由美国质量管理专家 *Edwards Deming* 提出 (1950)。

1.4 Information Security Management and Audit

1.4.1 Information Security Management

- 信息安全管理体系的实施
  - 戴明环
    - ✧ Plan：确定范围、风险分析、控制目标与控制方式、实用性声明、业务持续计划；
    - ✧ Do：组织安全、资产分类与控制、人员安全、实物与环境安全、重要作业的保护 (包括保护的资料)；
    - ✧ Check：法律法规的符合性、安全方针的符合性、安全技术的符合性；
    - ✧ Act：管理评审。
    - ✧ 以上四个步骤循环执行，使信息系统的安全管理得到持续改善。

1.4 Information Security Management and Audit



Framework of ISM

中山大學 SUN YAT-SEN UNIVERSITY

1.4 Information Security Management and Audit

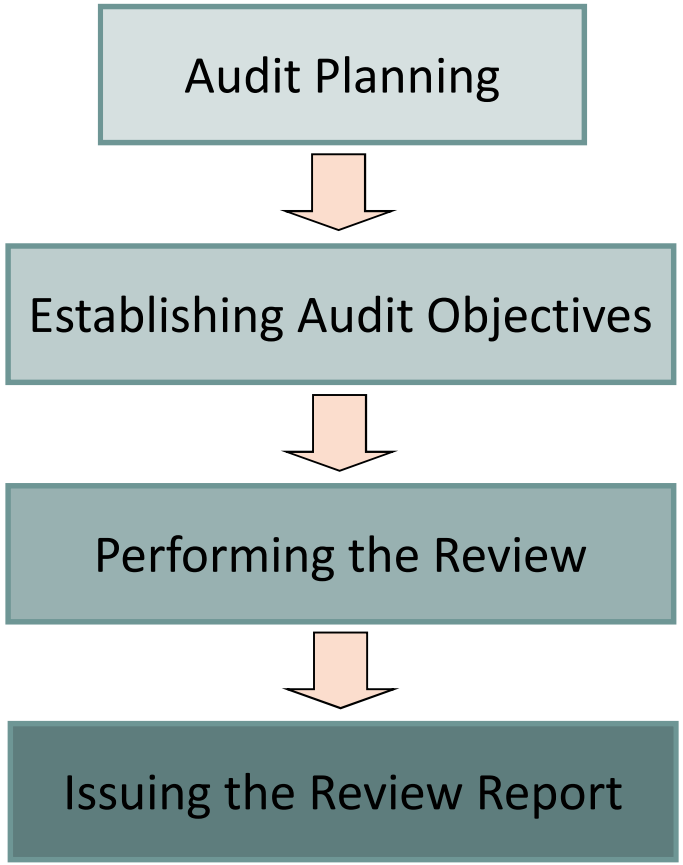
1.4.2 Information Security Audit

- 信息安全审计
  - What's Information Security Audit
    - ✧ An information security audit is an audit *on the level of* information security in an organization.
    - ✧ An evaluation (assessment) of a person, organization, system, process, enterprise, project or product. (Wikipedia)

1.4 Information Security Management and Audit

1.4.2 Information Security Audit

- 信息安全审计
  - Process



1.4 Information Security Management and Audit

1.4.2 Information Security Audit

- 信息安全审计
  - 信息安全审计的概念
    - ✧ 信息安全审计对机构或组织中的信息安全水平进行审查和评价，检验信息系统是否达到相关标准的相应安全等级。信息安全审计已经成为企业内控、信息系统治理、安全风险控制等的不可或缺的关键手段。信息安全审计的范围很广，有多种类型的审计和多个不同的审计目标。最常见的审计可分为技术的、物理的、行政的。
    - ✧ 信息安全审计“收集并评估证据以决定一个计算机系统是否有效做到保护资产、维护数据完整、完成目标，同时最经济地使用资源。”

— Ron Weber

1.4 Information Security Management and Audit

1.4.2 Information Security Audit

- 信息安全审计步骤

(1) 审计准备

✧ 审计人员对审计的组织或机构进行必要的了解调查。

(2) 建立审计目标

✧ 审计人员需要考虑与信息系统相关的多种安全因素，确定运行环境的风险并且评估所采取的降低风险的控制措施，能够充分确定信息系统是否保持了合适的控制能力并且能够高效或有效运行。系统采取的控制措施就是审计目标。

(3) 实施审查

✧ 收集相关证据，结合审计目标进行审查和评价。

(4) 发布审计报告

✧ 给出一个审计报告。权威审计报告可被用作第三方证明资料。

1.4.2 Information Security Audit

- 信息安全审计内容

(1) 安全策略的检查

✧ 检查结构上的系统性、内容上的可理解性、技术上的可实现性、管理上的可执行性。

(2) 技术措施的检查

✧ 根据有关技术标准，结合实际情况，分析安全措施的保护能力及能够满足相关标准需求的程度，并进一步研究该项措施在当前环境和将来环境中的作用及可行性。

(3) 管理措施的检查

✧ 主要检查安全管理机构是否健全，管理职能和管理职责是否明确，有关的政策、法规、制度、规定是否完善。

1.4 Information Security Management and Audit

1.4.2 Information Security Audit

- 信息安全审计与信息安全管理的关系
  - The Relationship Between InfoSec Audit and InfoSec Management
    - ✧ InfoSec Audit is mainly based on the standard of InfoSec Management like ISO/IEC 17799, ISO 17799/27001, COSO, COBIT, ITIL, NIST SP800.
    - ✧ These standards constructed mechanisms that can effectively control information security risks, thus we can achieve the purpose of information security audit.

1.4 Information Security Management and Audit

1.4.2 Information Security Audit

- 信息安全审计与信息安全管理的关系
  - 信息安全审计与信息安全管理密切相关。
    - ✧ 信息安全审计的主要依据是信息安全管理相关的标准，例如ISO/IEC 17799、ISO 17799/27001、COSO、COBIT、ITIL、NIST SP800 系列等。
    - ✧ 这些标准实际上是出于不同的角度提出的控制体系，基于这些控制体系可以有效地控制信息安全风险，从而达到信息安全审计的目的，提高信息系统的安全性。

1.4 Information Security Management and Audit

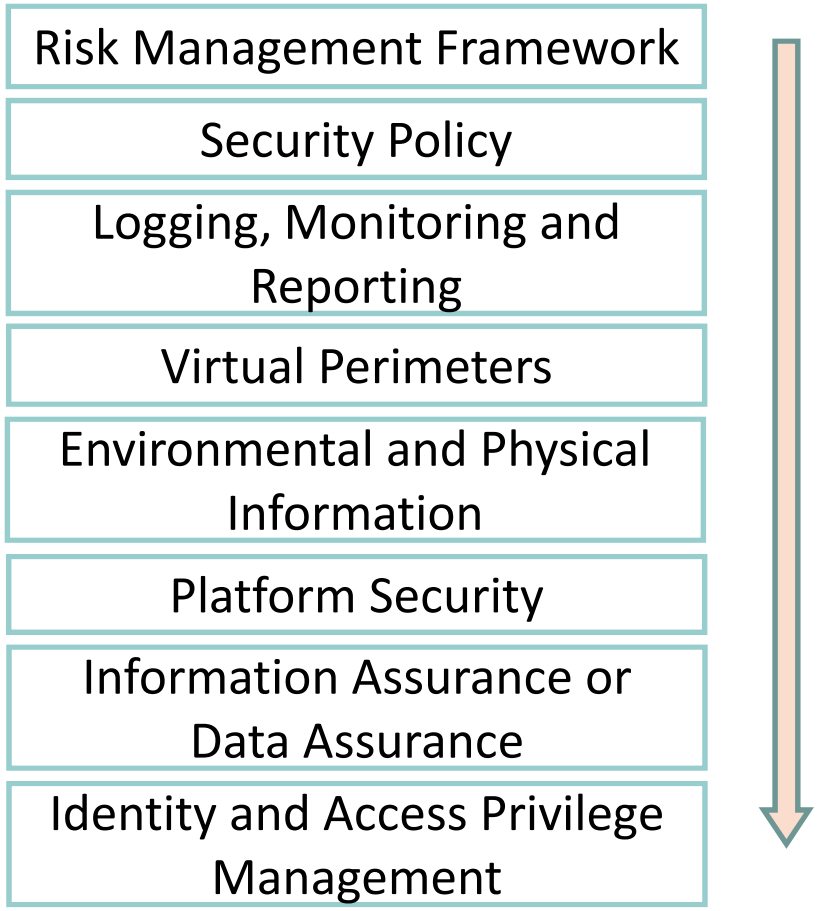
1.4.3 Information Security Levels

- 信息安全分级体系
  - The eight information security levels
  - GB 17859-1999's five levels
    - ✧ GB 17859-1999 计算机信息系统安全保护等级划分准则
      - ◌ Classified criteria for security protection of computer information system
      - ◌ 强制标准
  - Level graph from computer architecture perspective

1.4 Information Security Management and Audit

1.4.3 Information Security Levels

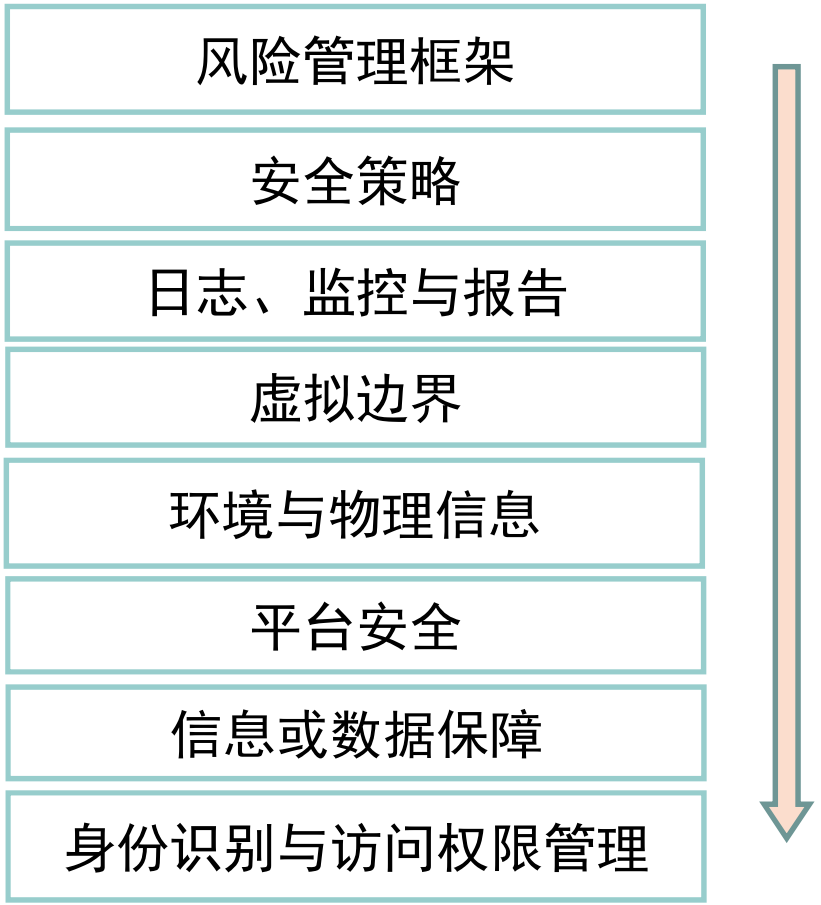
- **The eight information security levels**



1.4 Information Security Management and Audit

1.4.3 Information Security Levels

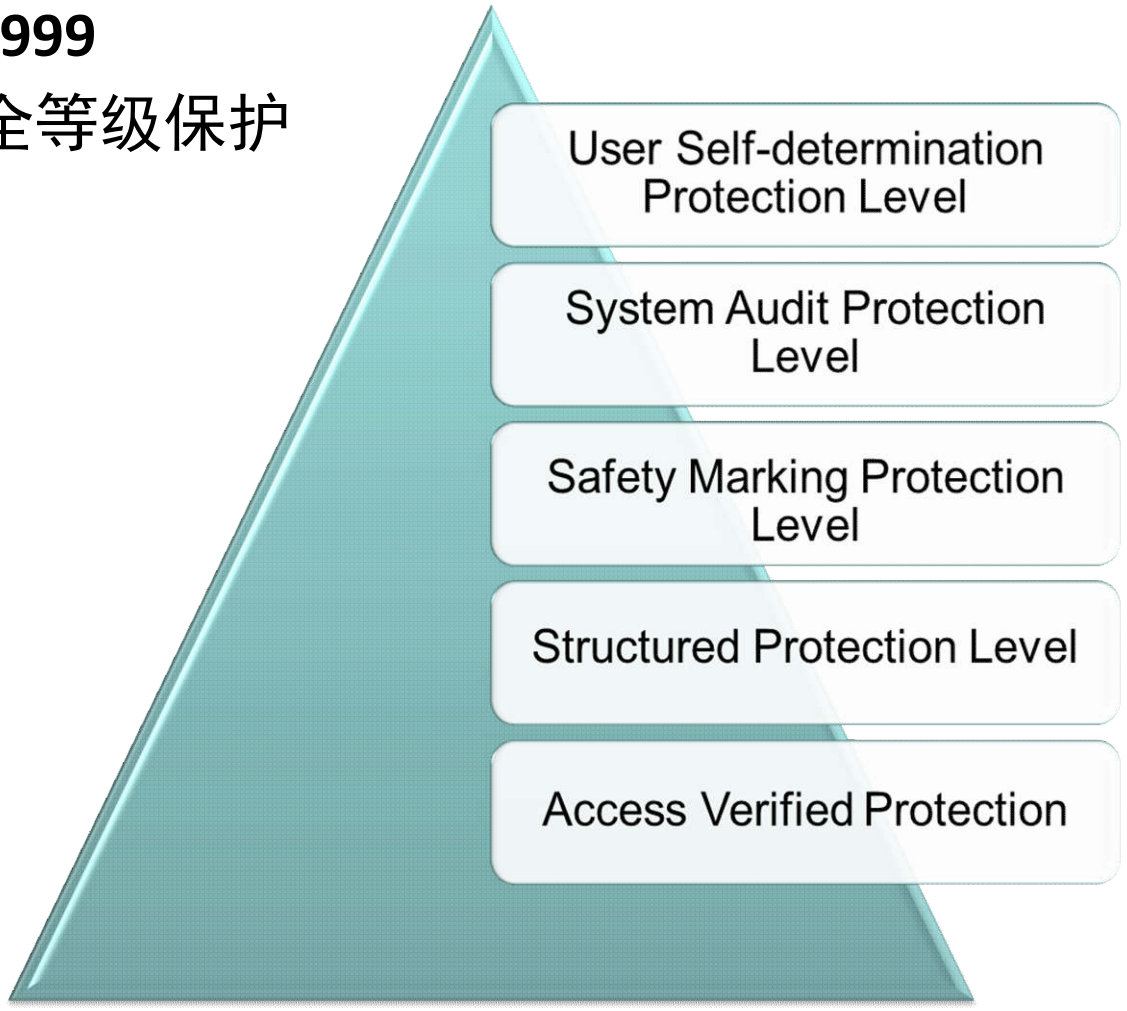
- **The eight information security levels**



1.4 Information Security Management and Audit

1.4.3 Information Security Levels

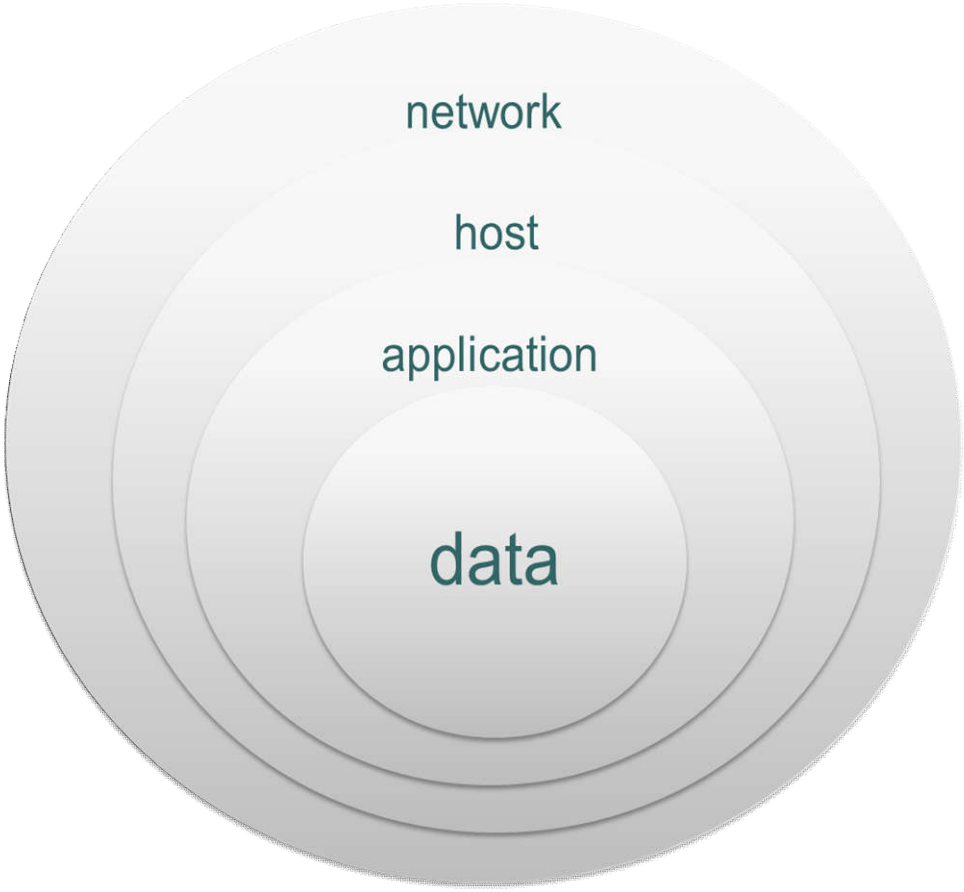
- **GB 17859-1999**
  - 信息安全等级保护



1.4 Information Security Management and Audit

1.4.3 Information Security Levels

- **Level Graph From Computer Architecture Perspective**



1.4 Information Security Management and Audit

1.4.3 Information Security Levels

- GB/T 20269-2006 的信息安全管理五个等级

(1) 用户自主保护级

✧ 本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户信息，避免其他用户对数据的非法读写和破坏。

(2) 系统审计保护级

✧ 与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登陆规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

1.4 Information Security Management and Audit

1.4.3 Information Security Levels

- GB/T 20269-2006 的信息安全管理五个等级

  (3) 安全标记保护级

  ✧ 本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力，消除通过测试发现的任何错误。

1.4.3 Information Security Levels

- GB/T 20269-2006 的信息安全管理五个等级

(4) 结构化保护级

✧ 本级的计算机系统可信计算基建立在一个明确定义的形式安全策略模型之上，要求将第三级系统中的自主和强制访问控制扩展到所有主体和客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

1.4.3 Information Security Levels

- GB/T 20269-2006 的信息安全管理五个等级

(5) 访问验证保护级

✧ 本级的计算机信息系统可信计算基满足访问控制器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

1.4 Information Security Management and Audit

1.4.3 Information Security Levels

- 名词解释
  - 客体 (Object)
    - ✧ 信息的载体。
  - 主体 (Subject)
    - ✧ 引起信息在客体之间流动的人、进程或设备等。
  - 安全策略 (Security Policy)
    - ✧ 有关管理、保护和发布敏感信息的法律、规定和实施细则。
  - 计算机信息系统可信计算基 (Trusted Computing Base of Computer Information System)
    - ✧ 计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体，它建立了一个基本的保护环境并提供一个可信计算系统要求的附加用户服务。

1.4 Information Security Management and Audit

1.4.3 Information Security Levels

- 名词解释
  - 敏感标记 (Sensitivity Label)
    - ✧ 表示客体安全级别并描述客体数据敏感性的一组数据，可信计算基中把敏感标记作为强制访问控制决策的依据。
  - 信道 (Channel)
    - ✧ 系统内的信息传输路径。
  - 隐蔽信道 (Covert Channel)
    - ✧ 运行进程，以危害系统安全策略的方式传输信息的信道。
  - 访问监控器 (Reference Monitor)
    - ✧ 监控主体和客体之间的授权访问关系的部件。

End of Chapter 1.3-1.4