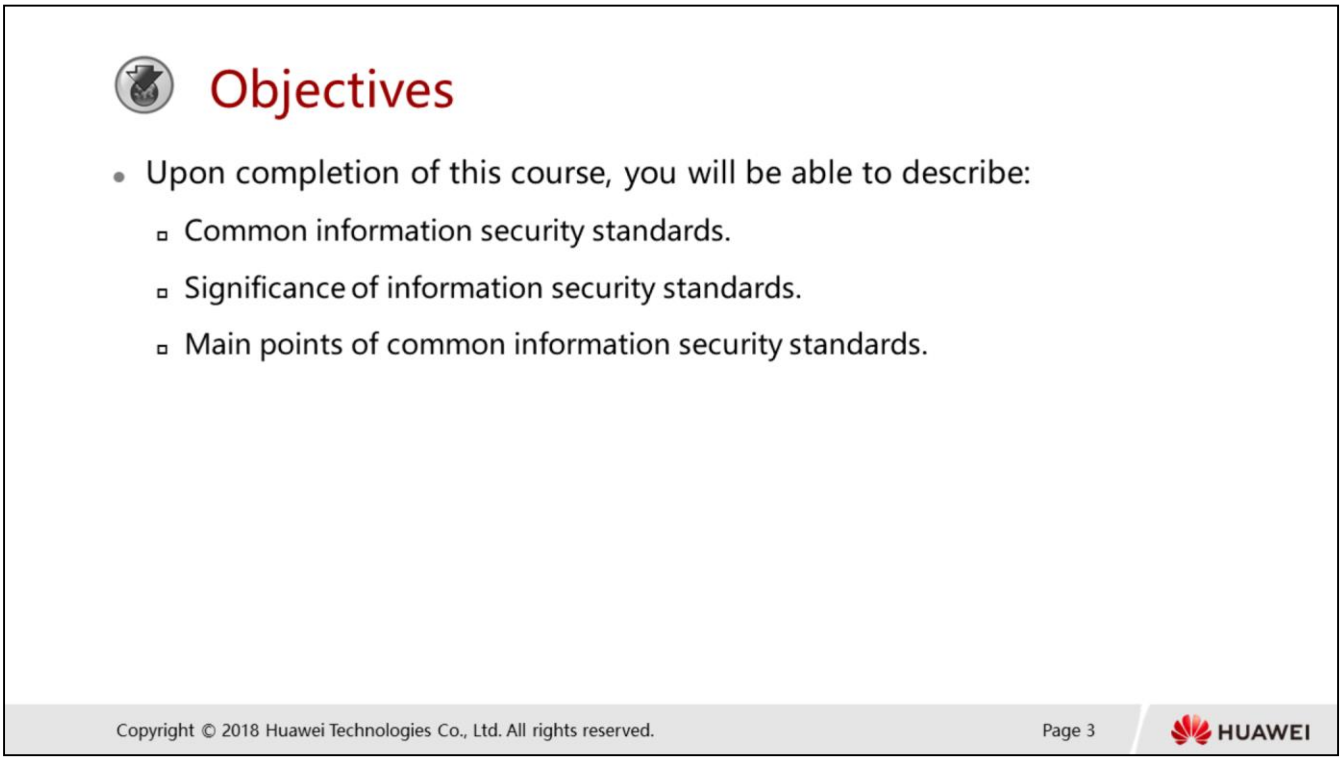
Information Security Standards and Specifications

www.huawei.com

HUAWEI

Foreword

- In the process of information security system construction, enterprises comply with international standards and specifications to develop their own information security specifications and improve operations.
- This document describes and analyzes several international information security standards to help better understand information security.



Objectives

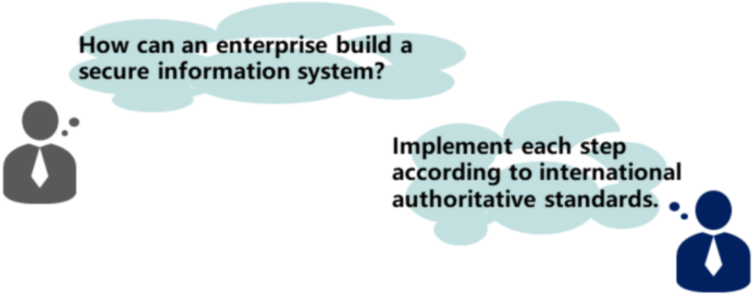
- Upon completion of this course, you will be able to describe:
  - Common information security standards.
  - Significance of information security standards.
  - Main points of common information security standards.

Contents

1. **Information Security Standards and Specifications**
2. ISO 27001 ISMS
3. Graded Protection of Information Security
4. Other Standards

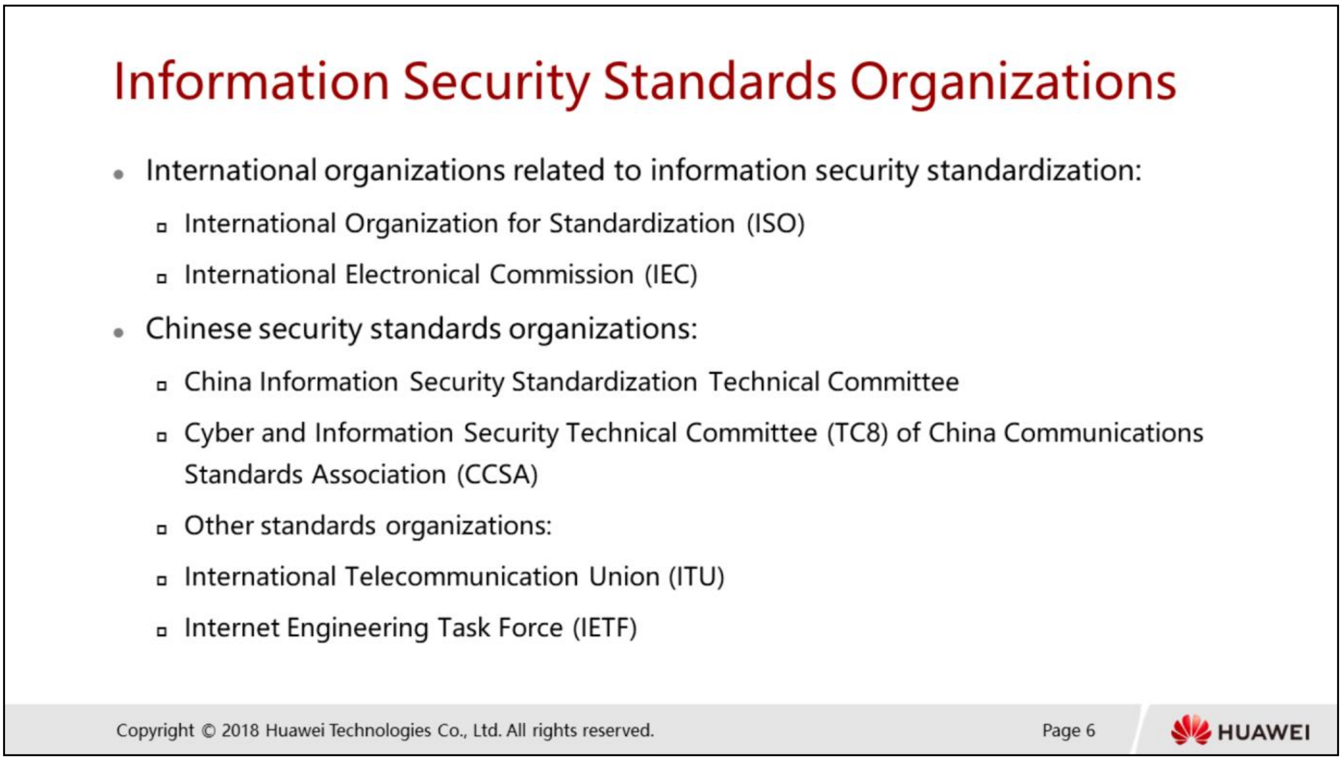
Significance of Information Security Standards

- Standards are normative documents that are jointly formulated, approved by recognized authorities, and used throughout the industry to achieve the best security.



How can an enterprise build a secure information system?

Implement each step according to international authoritative standards.



Information Security Standards Organizations

- International organizations related to information security standardization:
  - International Organization for Standardization (ISO)
  - International Electronical Commission (IEC)
- Chinese security standards organizations:
  - China Information Security Standardization Technical Committee
  - Cyber and Information Security Technical Committee (TC8) of China Communications Standards Association (CCSA)
  - Other standards organizations:
  - International Telecommunication Union (ITU)
  - Internet Engineering Task Force (IETF)

- International information security standardization began in the middle of the 1970s, rapidly developed in the 1980s, and drew global attention in the 1990s. At present, there are nearly 300 international and regional organizations establishing standards or technical rules.
- ISO is a global non-governmental organization and plays a crucial role in international standardization. It has published international standards and related documents for most fields (including monopolized industries such as military, oil, and shipping).
- IEC was the first international organization established for the preparation and publication of international standards for all electrical, electronic and related technologies.
- ITU is the United Nations specialized agency for information and communication technologies. It allocates global radio spectrum and satellite orbits, develops global telecommunication standards, works to improve telecommunication infrastructure in the developing world, and promotes global telecommunication development.
- IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Common Information Security Standards and Specifications

China: Graded Protection of Information Security (GB)

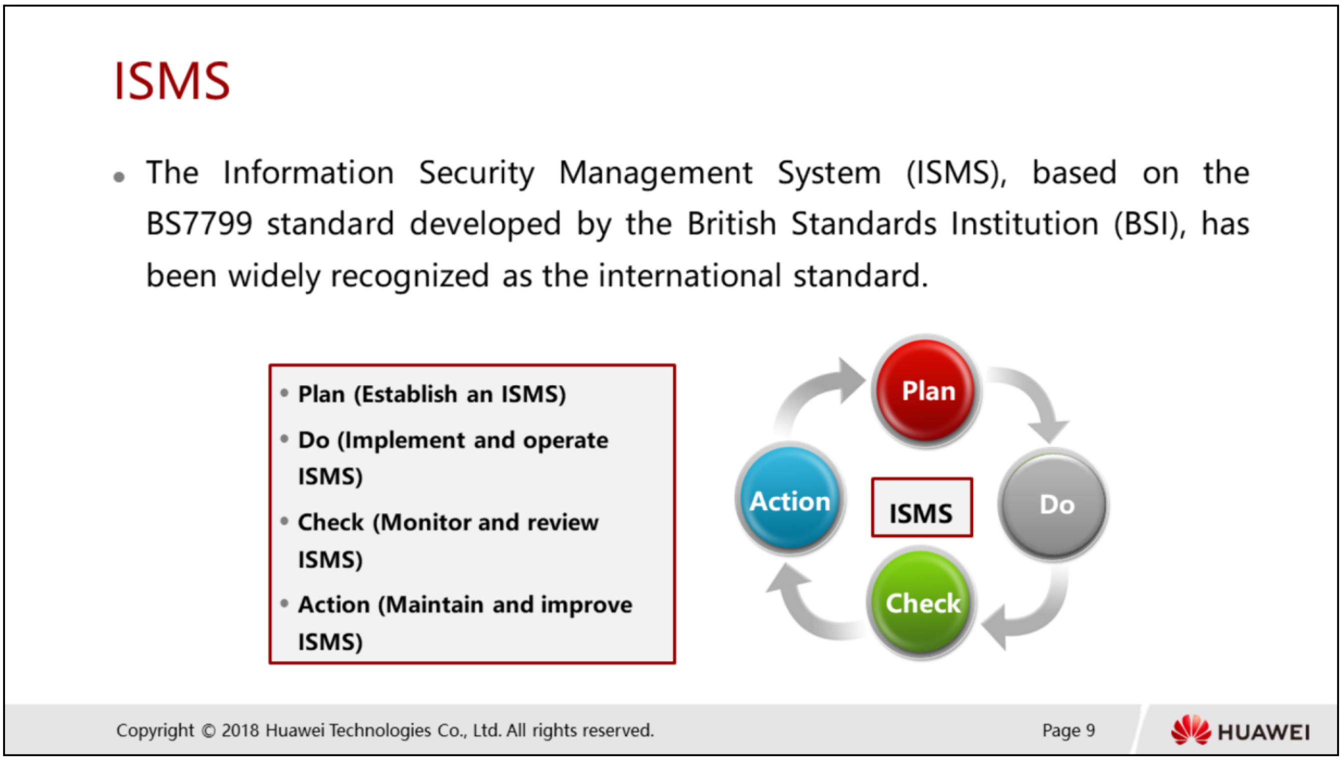
ISO 27001

US: Trusted Computer System Evaluation Criteria (TCSEC)

EU: Information Technology Security Evaluation Criteria (ITSEC)

Contents

1. Information Security Standards and Specifications
2. **ISO 27001 ISMS**
3. Graded Protection of Information Security
4. Other Standards



ISMS

- The Information Security Management System (ISMS), based on the BS7799 standard developed by the British Standards Institution (BSI), has been widely recognized as the international standard.

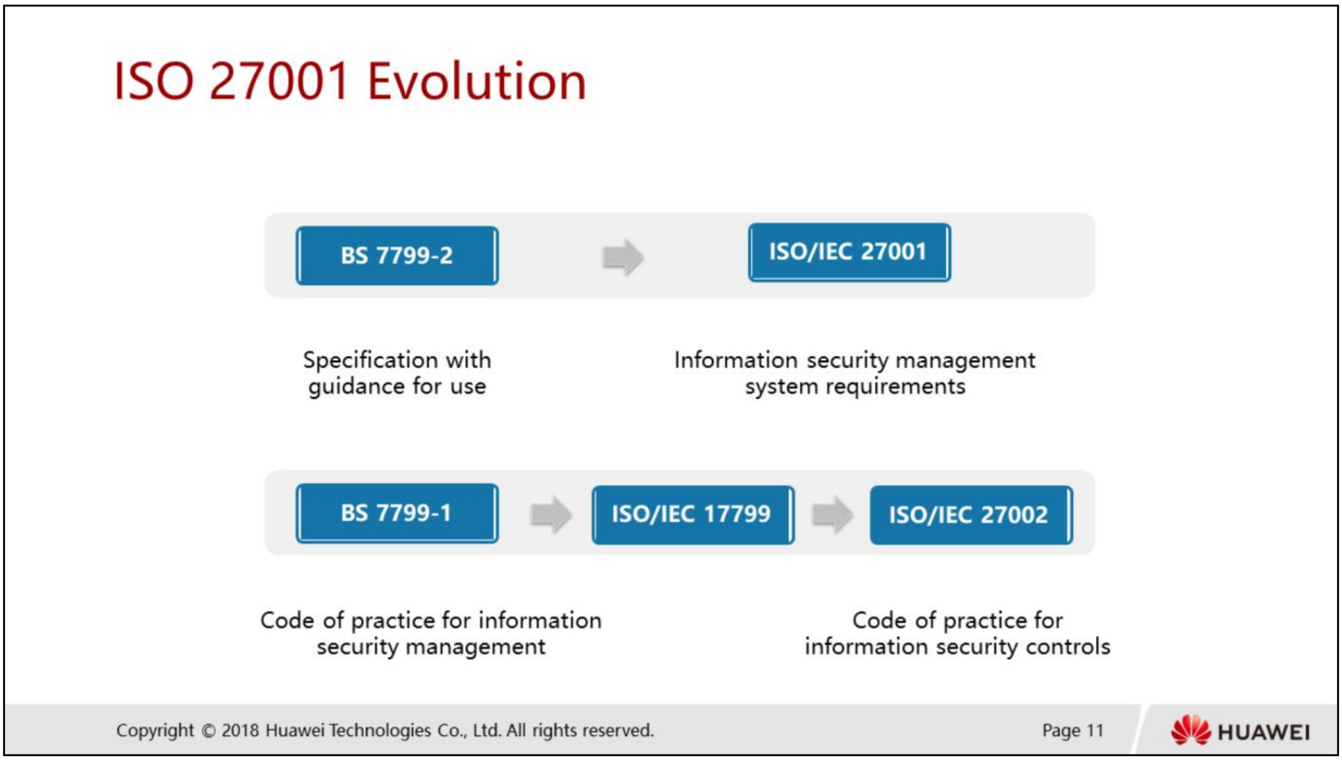
- Plan (Establish an ISMS)
- Do (Implement and operate ISMS)
- Check (Monitor and review ISMS)
- Action (Maintain and improve ISMS)

Plan
Action
ISMS
Do
Check

- Plan: ISMS planning and preparation
  - Establish security policy, objectives, processes and procedures relevant to managing risks and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do: ISMS document development
- Implement and operate the ISMS policy, controls, processes and procedures.
- Check: ISMS operation
- Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Action: ISMS examination, review, and continuous improvement
- Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

ISO 27000 ISMS Family of Standards

I	II	III	IV
Requirements and supporting guidelines	Audit and certification guidelines	Industry information security management requirements	Health information security management standards
ISO/IEC 27000 ISO/IEC 27001	ISO/IEC 27006	Finance	ISO 27799
ISO/IEC 27002 ISO/IEC 27003	ISO/IEC 27007	Telecommunication	Projects that are in the research phase. For example, medicine supply chain and storage security.
ISO/IEC 27004 ISO/IEC 27005	ISO/IEC 27008	Other specific security domains	



ISO 27001 Evolution

BS 7799-2 → ISO/IEC 27001

Specification with guidance for use

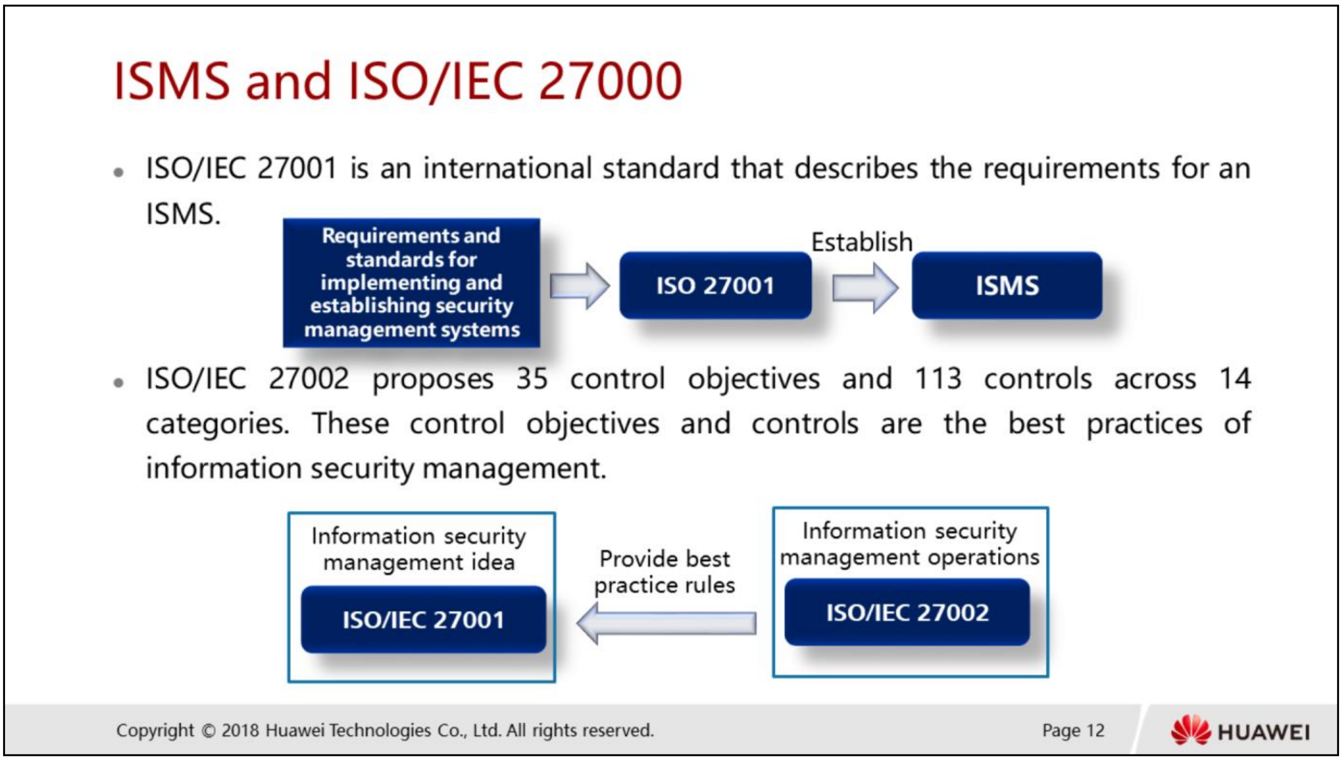
Information security management system requirements

BS 7799-1 → ISO/IEC 17799 → ISO/IEC 27002

Code of practice for information security management

Code of practice for information security controls

- ISO/IEC 27001 and ISO/IEC 27002, released in 2013, are the currently used standards.



ISMS and ISO/IEC 27000

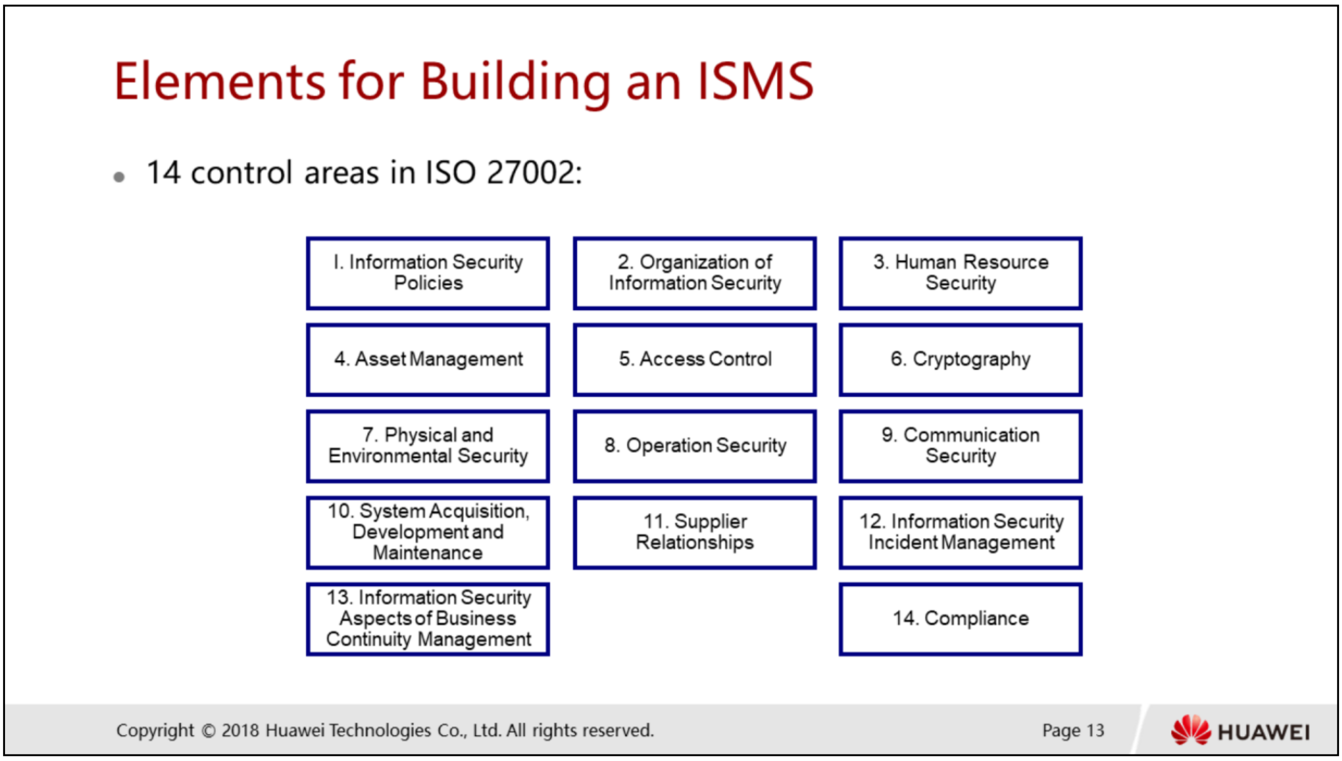
- ISO/IEC 27001 is an international standard that describes the requirements for an ISMS.

Requirements and standards for implementing and establishing security management systems → ISO 27001 → Establish → ISMS

- ISO/IEC 27002 proposes 35 control objectives and 113 controls across 14 categories. These control objectives and controls are the best practices of information security management.

Information security management idea: ISO/IEC 27001 ← Provide best practice rules ← Information security management operations: ISO/IEC 27002

- Any company can implement an ISMS, but how? What requirements must be met? ISO 27000 provides detailed requirements which organizations can use to establish ISMSs.
- ISO 27001 is to manage information security risks based on risk assessments and to comprehensively, systematically, and continuously improve information security management using the Plan, Do, Check, Action (PDCA) cycle. It can be used to establish and implement ISMSs and ensure information security of organizations.
- ISO 27001, an overall information security management framework based on the PDCA cycle, focuses on the establishment of a continuous-cyclic long-term management mechanism. Only certification to ISO/IEC 27001 is possible. Other ISO/IEC standards are the specific clauses and operation guides for the certification. For example, ISO 27002 defines a specific information security management process under the guidance of ISO 27001.



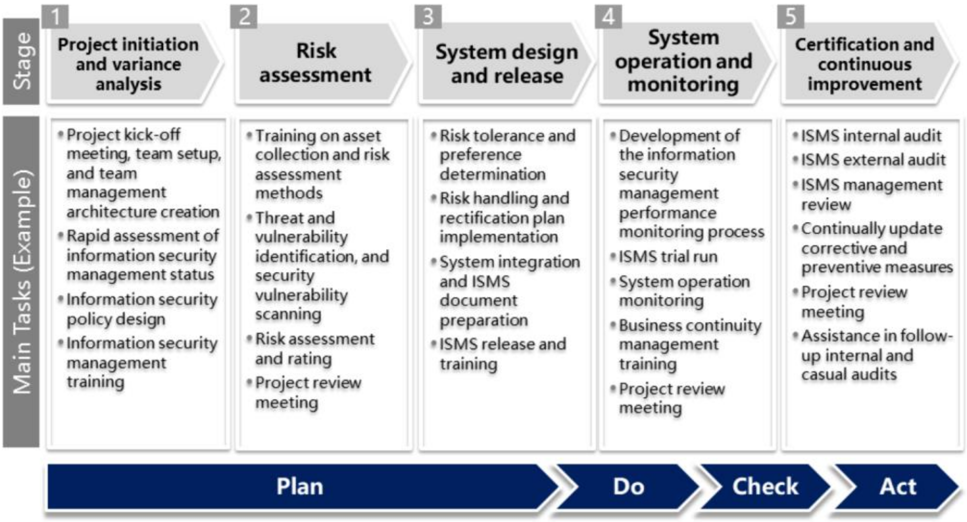
Elements for Building an ISMS

- 14 control areas in ISO 27002:

I. Information Security Policies	2. Organization of Information Security	3. Human Resource Security
4. Asset Management	5. Access Control	6. Cryptography
7. Physical and Environmental Security	8. Operation Security	9. Communication Security
10. System Acquisition, Development and Maintenance	11. Supplier Relationships	12. Information Security Incident Management
13. Information Security Aspects of Business Continuity Management		14. Compliance

- The key check points in the ISO 27001 certification process are as follows:
- Document review:
  - Risk assessment reports
  - Security principles
  - Statement of Applicability (SoA)
  - Other ISMS documents
- Formal review:
  - Check records, including account and permission assignment, training, business continuity drill, access control, and media usage records.
  - Check the information asset identification and processing, and risk assessment and handling forms.
  - Perform terminal security check, including the screen saver, screen lock, and antivirus software installation and upgrade status.
  - Carry out the physical environment survey, including the field observation and inquiry of equipment rooms and office environments.

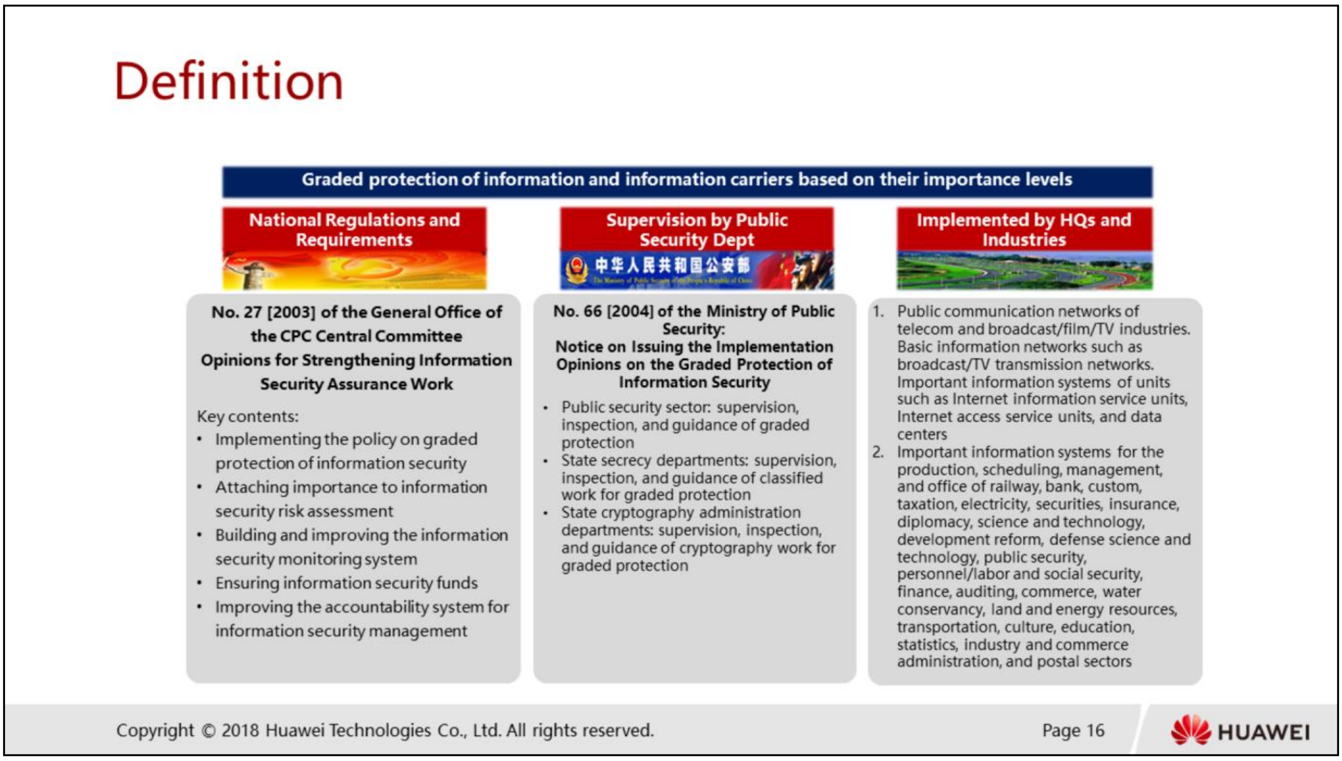
ISO 27001 Project Implementation Methodology and Steps



	1	2	3	4	5
Stage	Project initiation and variance analysis	Risk assessment	System design and release	System operation and monitoring	Certification and continuous improvement
Main Tasks (Example)	• Project kick-off meeting, team setup, and team management architecture creation • Rapid assessment of information security management status • Information security policy design • Information security management training	• Training on asset collection and risk assessment methods • Threat and vulnerability identification, and security vulnerability scanning • Risk assessment and rating • Project review meeting	• Risk tolerance and preference determination • Risk handling and rectification plan implementation • System integration and ISMS document preparation • ISMS release and training	• Development of the information security management performance monitoring process • ISMS trial run • System operation monitoring • Business continuity management training • Project review meeting	• ISMS internal audit • ISMS external audit • ISMS management review • Continually update corrective and preventive measures • Project review meeting • Assistance in follow-up internal and casual audits

Contents

1. Information Security Standards and Specifications
2. ISO 27001 ISMS
3. **Graded Protection of Information Security**
4. Other Standards



Definition

Graded protection of information and information carriers based on their importance levels

National Regulations and Requirements

No. 27 [2003] of the General Office of the CPC Central Committee
Opinions for Strengthening Information Security Assurance Work

Key contents:

- Implementing the policy on graded protection of information security
- Attaching importance to information security risk assessment
- Building and improving the information security monitoring system
- Ensuring information security funds
- Improving the accountability system for information security management

Supervision by Public Security Dept

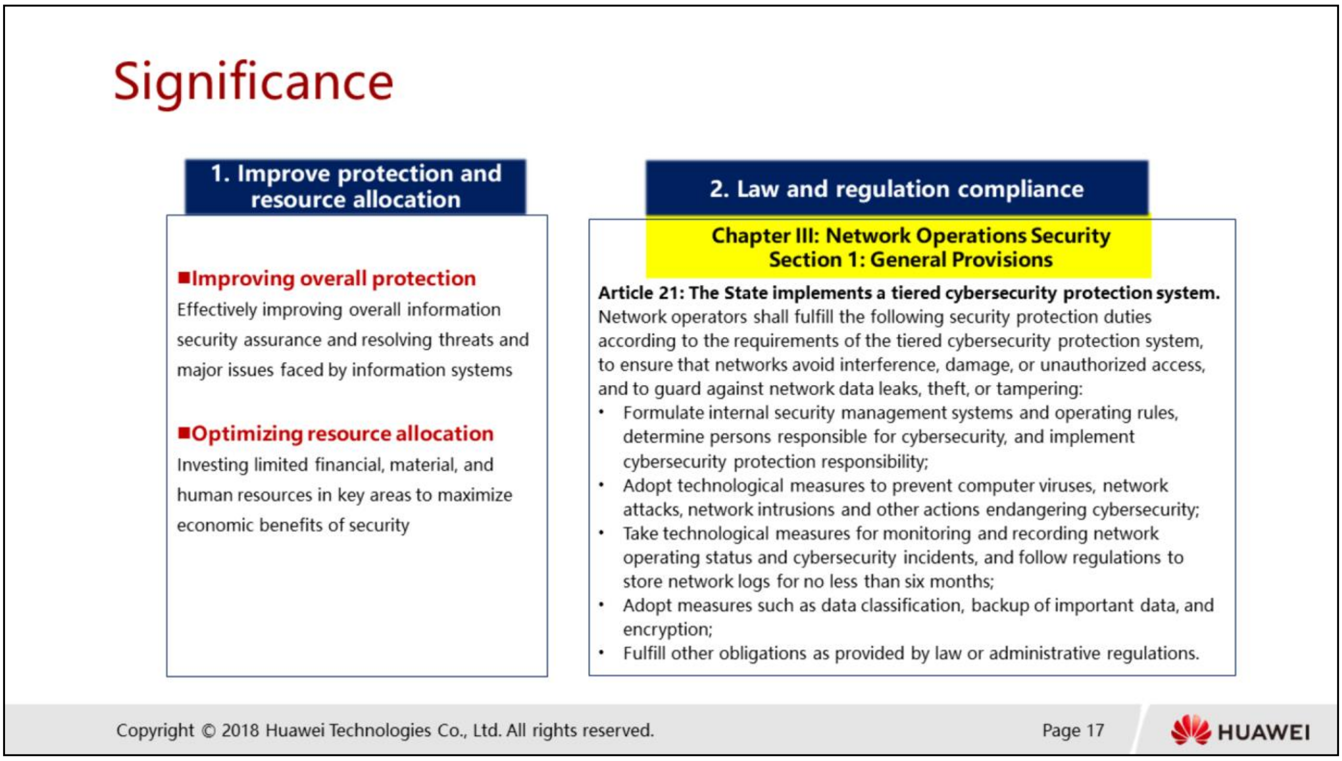
No. 66 [2004] of the Ministry of Public Security:
Notice on Issuing the Implementation Opinions on the Graded Protection of Information Security

- Public security sector: supervision, inspection, and guidance of graded protection
- State secrecy departments: supervision, inspection, and guidance of classified work for graded protection
- State cryptography administration departments: supervision, inspection, and guidance of cryptography work for graded protection

Implemented by HQs and Industries

1. Public communication networks of telecom and broadcast/film/TV industries. Basic information networks such as broadcast/TV transmission networks. Important information systems of units such as Internet information service units, Internet access service units, and data centers
2. Important information systems for the production, scheduling, management, and office of railway, bank, custom, taxation, electricity, securities, insurance, diplomacy, science and technology, development reform, defense science and technology, public security, personnel/labor and social security, finance, auditing, commerce, water conservancy, land and energy resources, transportation, culture, education, statistics, industry and commerce administration, and postal sectors

- Graded protection of information security refers to: graded security protection of crucial government information, private and public information of legal persons/organizations/citizens, and information systems that store, transmit, and process the information; graded management of information security products in information systems; graded response to and handling of information security incidents in information systems.



Significance

1. Improve protection and resource allocation

■**Improving overall protection**

Effectively improving overall information security assurance and resolving threats and major issues faced by information systems

■**Optimizing resource allocation**

Investing limited financial, material, and human resources in key areas to maximize economic benefits of security

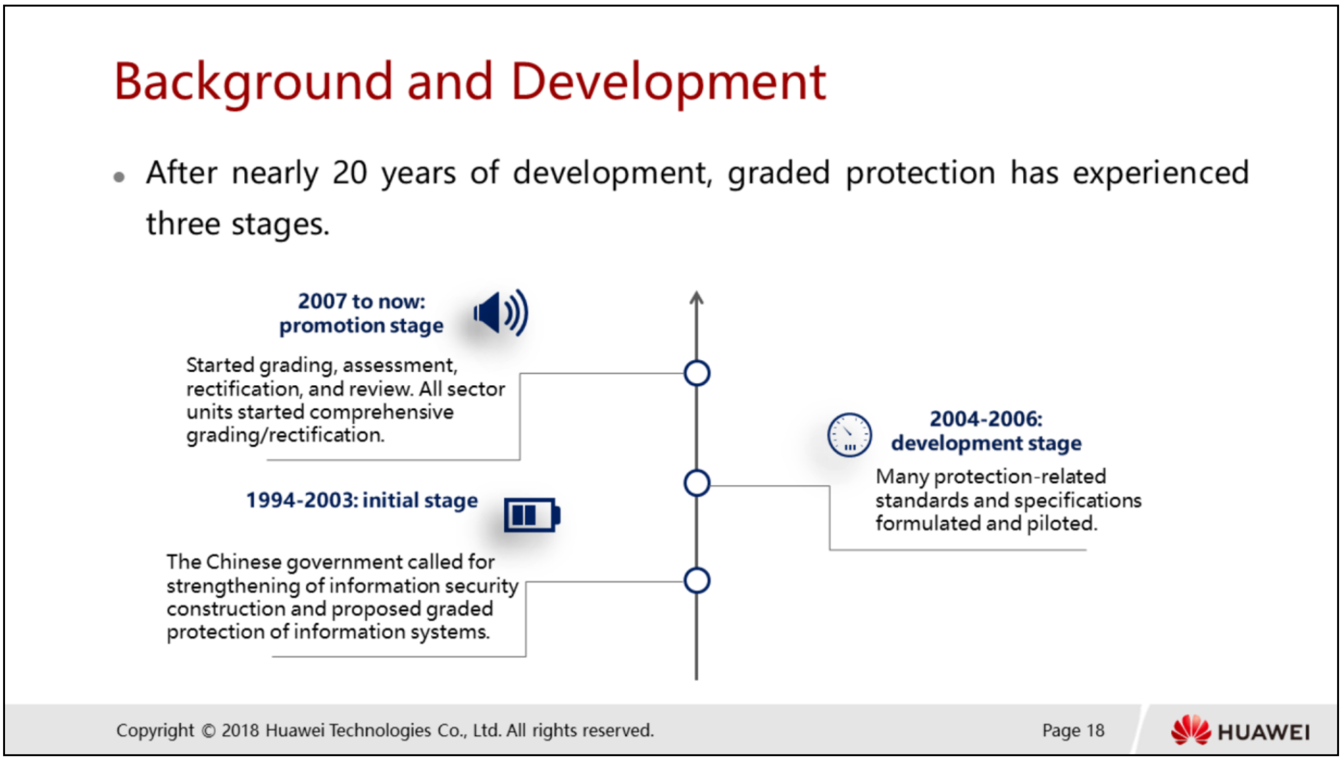
2. Law and regulation compliance

Chapter III: Network Operations Security
Section 1: General Provisions

Article 21: The State implements a tiered cybersecurity protection system. Network operators shall fulfill the following security protection duties according to the requirements of the tiered cybersecurity protection system, to ensure that networks avoid interference, damage, or unauthorized access, and to guard against network data leaks, theft, or tampering:

- Formulate internal security management systems and operating rules, determine persons responsible for cybersecurity, and implement cybersecurity protection responsibility;
- Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cybersecurity;
- Take technological measures for monitoring and recording network operating status and cybersecurity incidents, and follow regulations to store network logs for no less than six months;
- Adopt measures such as data classification, backup of important data, and encryption;
- Fulfill other obligations as provided by law or administrative regulations.

- Legal liabilities of graded protection:
  - A corporate sector that does not carry out assessment for graded protection will be rectified according to relevant regulations. If it violates the provisions of China's Cybersecurity Law enforced in June 2017, it will be punished according to relevant laws and regulations. Article 21 of the Cybersecurity Law: The State implements a tiered cybersecurity protection system. Article 59: Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the administrative department shall order corrections and give warnings; where corrections are refused or it leads to endangerment of cybersecurity or other such consequences, a fine of between 10,000RMB and 100,000RMB shall be imposed, and persons who are directly in charge shall be fined between RMB 5,000RMB and 50,000RMB.



Background and Development

- After nearly 20 years of development, graded protection has experienced three stages.

2007 to now: promotion stage

Started grading, assessment, rectification, and review. All sector units started comprehensive grading/rectification.

2004-2006: development stage

Many protection-related standards and specifications formulated and piloted.

1994-2003: initial stage

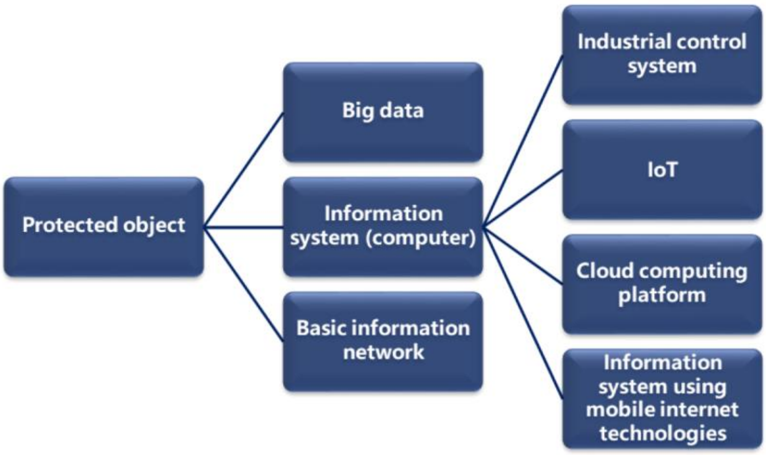
The Chinese government called for strengthening of information security construction and proposed graded protection of information systems.

HUAWEI

- Development timeline:
  - February 18, 1994, Decree No. 147 of the State Council, Regulations of the People's Republic of China for Safety Protection of Computer Information Systems
  - September 2003, No. 27 [2003] of the General Office of the CPC Central Committee, Opinions for Strengthening Information Security Assurance Work
  - November 2004, No. 66 [2004] of the Ministry of Public Security, Notice of the Ministry of Public Security, the State Secrecy Bureau, the State Cipher Code Administration and the Information Office of the State Council on Issuing the Implementation Opinions on the Graded Protection of Information Security
  - September 2005, No. 25 [2004] of the State Council Information Office, Notice on Forwarding the Guide for Implementing Graded Protection of e-Government Information Security
  - January 2006, No. 7 [2006] of the Ministry of Public Security, Notice of the Ministry of Public Security, the State Secrecy Bureau, the State Cipher Code Administration and the Information Office of the State Council on Issuing the Administrative Measures for the Graded Protection of Information Security (for Trial Implementation)

- June 2007, No. 43 [2007] of the Ministry of Public Security, Notice of the Ministry of Public Security, the State Secrecy Bureau, the State Cipher Code Administration and the Information Office of the State Council on Issuing the Administrative Measures for the Graded Protection of Information Security
- 2008, GB/T 22239-2008 Baseline for classified protection of information system security and GB/T 22240-2008 Classification guide for classified protection of information system security
- 2009, No. 1429 [2009] of the Ministry of Public Security, Guiding Opinions on the Building and Improvement of Graded Protection of Information Systems
- March 2010, No. 303 [2010] of the Ministry of Public Security, Notice on Promoting the Assessment System Construction and Grade Assessment for Graded Protection of Information Security

Scope



Protected object

Big data

Information system (computer)

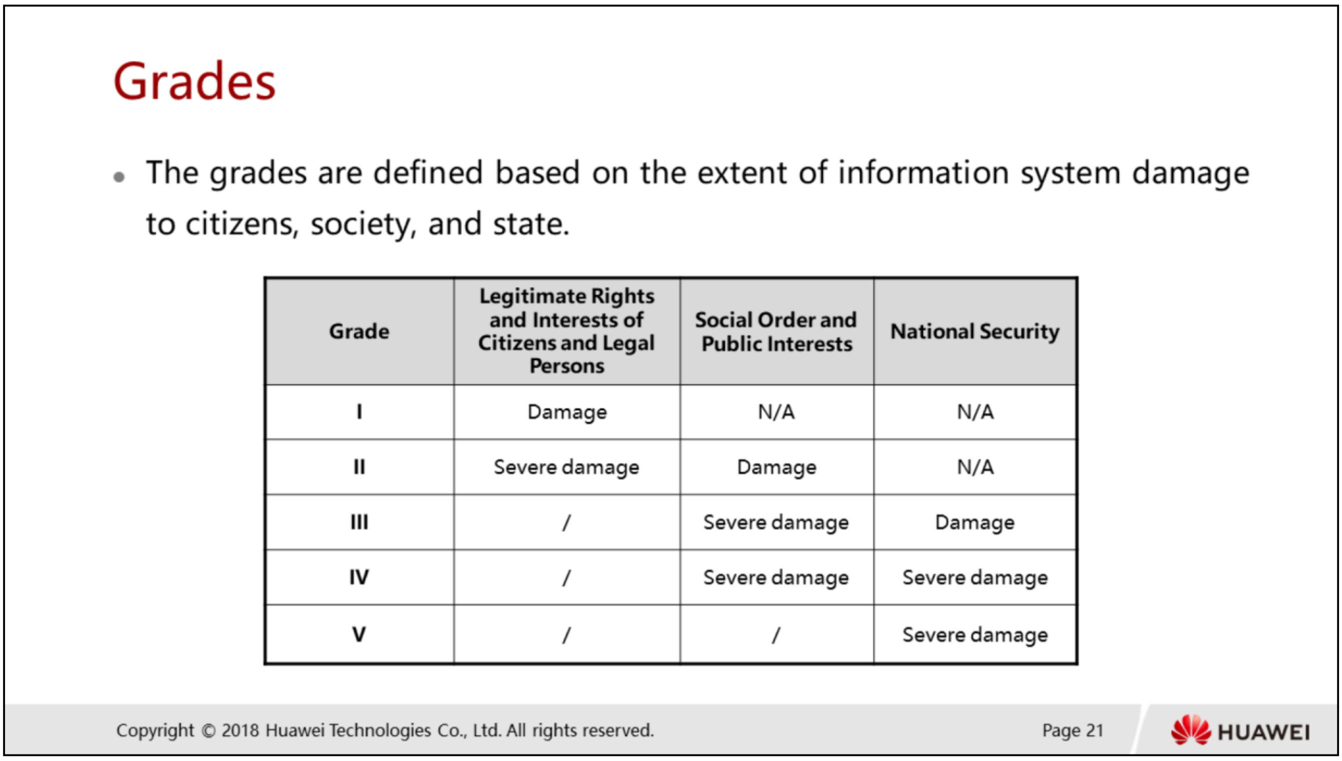
Basic information network

Industrial control system

IoT

Cloud computing platform

Information system using mobile internet technologies



Grades

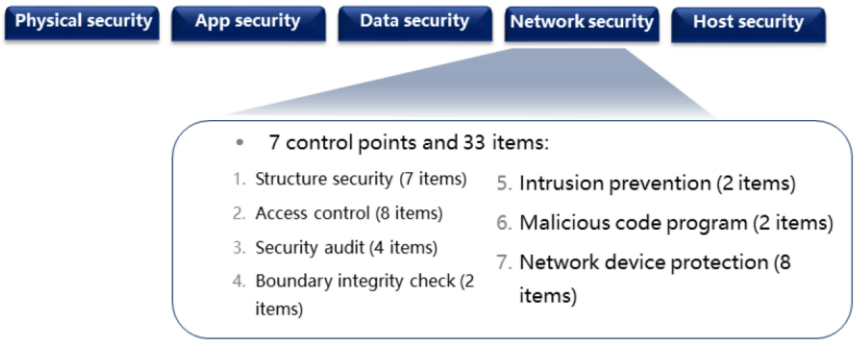
- The grades are defined based on the extent of information system damage to citizens, society, and state.

Grade	Legitimate Rights and Interests of Citizens and Legal Persons	Social Order and Public Interests	National Security
I	Damage	N/A	N/A
II	Severe damage	Damage	N/A
III	/	Severe damage	Damage
IV	/	Severe damage	Severe damage
V	/	/	Severe damage

- Grade I: Destruction of the information system would cause damage to the legitimate rights and interests of citizens, legal persons and other organizations, but would cause no damage to national security, social order or public interests.
- Grade II: Destruction of the information system would cause severe damage to the legitimate rights and interests of citizens, legal persons and other organizations or cause damage to social order and public interests, but would not damage national security.
- Grade III: Destruction of the information system would cause severe damage to social order and public interests or would cause damage to national security.
- Grade IV: Destruction of the information system would cause particularly severe damage to social order and public interests or would cause severe damage to national security.
- Grade V: Destruction of the information system would cause particularly severe damage to national security.

Basic Technical Requirements

- Each grade of protection has corresponding technical requirements. For example, the technical requirements for Grade III cover 5 aspects:



Physical security

App security

Data security

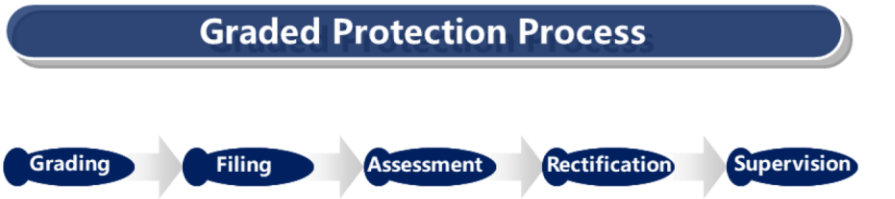
Network security

Host security

- 7 control points and 33 items:

1. Structure security (7 items)
2. Access control (8 items)
3. Security audit (4 items)
4. Boundary integrity check (2 items)
5. Intrusion prevention (2 items)
6. Malicious code program (2 items)
7. Network device protection (8 items)

Process



Graded Protection Process

Grading
- Primary step of graded protection

Filing
- Mandatory procedure for notifying the supervision department of graded protection construction

Assessment
- Method to assess the status of security protection

Rectification
- Key to the implementation of graded protection

Supervision
- External management of graded protection

Contents

1. Information Security Standards and Specifications
2. ISO 27001 ISMS
3. Graded Protection of Information Security
4. **Other Standards**

Other Standards - US - TCSEC

- Trusted Computer System Evaluation Criteria (TCSEC)
- First formal standard for computer system security evaluation
- Proposed by the Defense Science Board in 1970 and released by the United States Department of Defense in December 1985

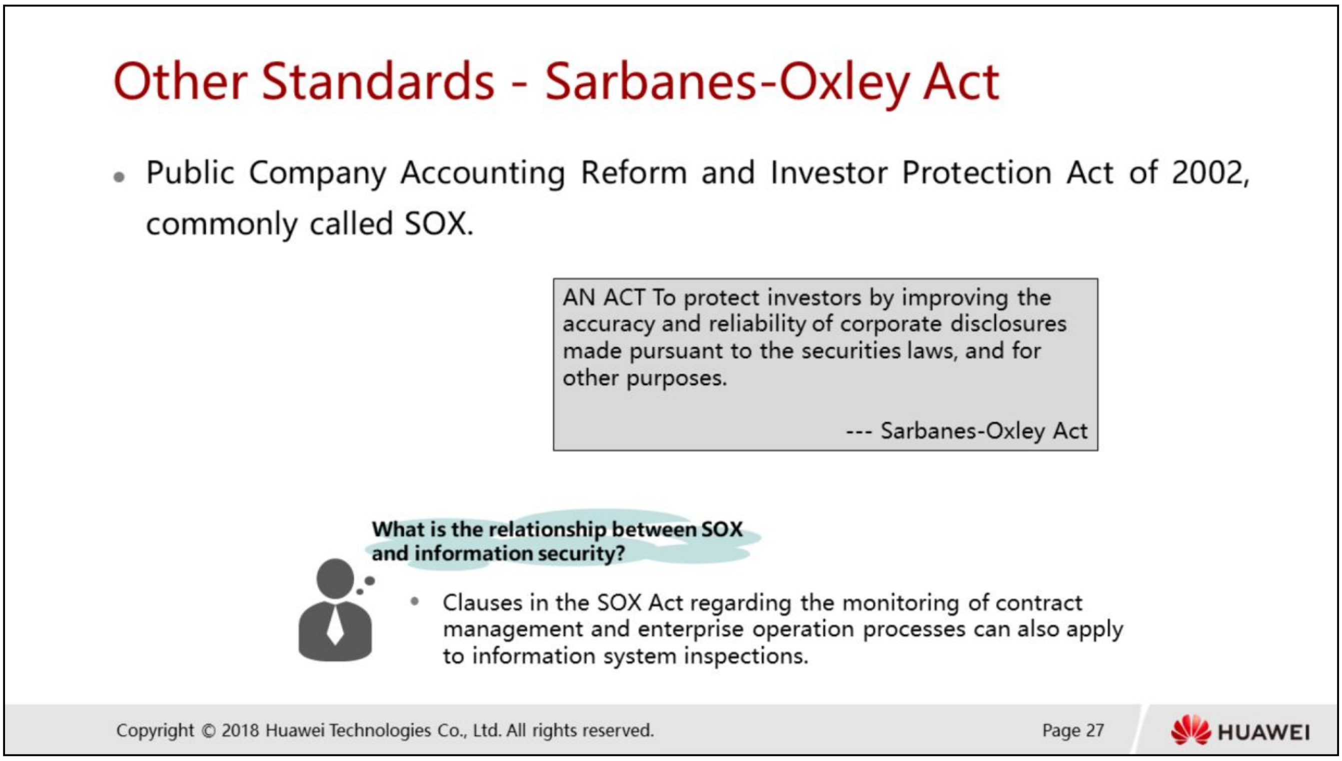
A: Verified protection	A1	The system administrator must receive a formal security policy model from the developer. All installation operations must be performed by the system administrator. Formal documents must be available for all of these operations.
B: Mandatory protection	B1	Class-B systems are protected against access from users without security levels.
	B2	
	B3	
C: Discretionary protection	C1	Audit protection is available, and users' actions and responsibilities can be audited.
	C2	
D: Minimal protection	D1	Security protection is provided only for files and users. The most common D1 system is a local operating system or a completely unprotected network.

Other Standards - Europe - ITSEC

- Information Technology Security Evaluation Criteria (ITSEC)
- Formulated by the UK, France, Germany, and the Netherlands, the ITSEC makes better progress in function flexibility and related evaluation technologies than TCSEC; applied in the military, government, and business sectors

Function	
Level	**Description**
F1-F5	TCSEC D-A
F6	Data and program integrity
F7	System availability
F8	Data communication integrity
F9	Data communication confidentiality
F10	Network security including confidentiality and integrity

Evaluation	
Level	**Description**
E0	Inadequate assurance
E1	At this level there shall be a security target and an informal description of the architectural design of the Target of Evaluation (TOE). Functional testing shall indicate that the TOE satisfies its security target.
E2	In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.
E3	In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
E4	In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semi-formal style.
E5	In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.
E6	In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.



Other Standards - Sarbanes-Oxley Act

- Public Company Accounting Reform and Investor Protection Act of 2002, commonly called SOX.

> AN ACT To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.
>
> --- Sarbanes-Oxley Act

What is the relationship between SOX and information security?

- Clauses in the SOX Act regarding the monitoring of contract management and enterprise operation processes can also apply to information system inspections.

- The legislation in the Sarbanes-Oxley Act (SOX) stems from a December 2001 securities scandal involving Enron, then one of the largest energy companies in the United States. The company hid massive debts that, when revealed, sent stock prices tumbling. With investor confidence "thoroughly destroyed", the United States Congress and government rapidly introduced the SOX Act. The act promised "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."
- The act contains the following:
  - Setting up the Public Company Accounting Oversight Board (PCAOB) to supervise registered public accounting firms
  - Strengthening auditor independence
  - Increasing the corporate responsibility for financial reports
  - Enhancing financial disclosures
  - Increasing criminal penalties

- SOX ACT’s impact on corporate governance:
    - Responsibilities of board members: The board members and audit commission must undertake self-assessment and follow-up education.
    - Professional ethics and corporate law-abiding: The act requires companies to develop written provisions on employees' professional ethics and the audit committee to establish an internal report incentive mechanism.
    - Transparency and information disclosure: The Securities & Exchange Commission recommended the establishment of the Information Disclosure Committee to strengthen the responsibilities of internal audit departments.
    - Risk management and control: Establish an internal control system and process.