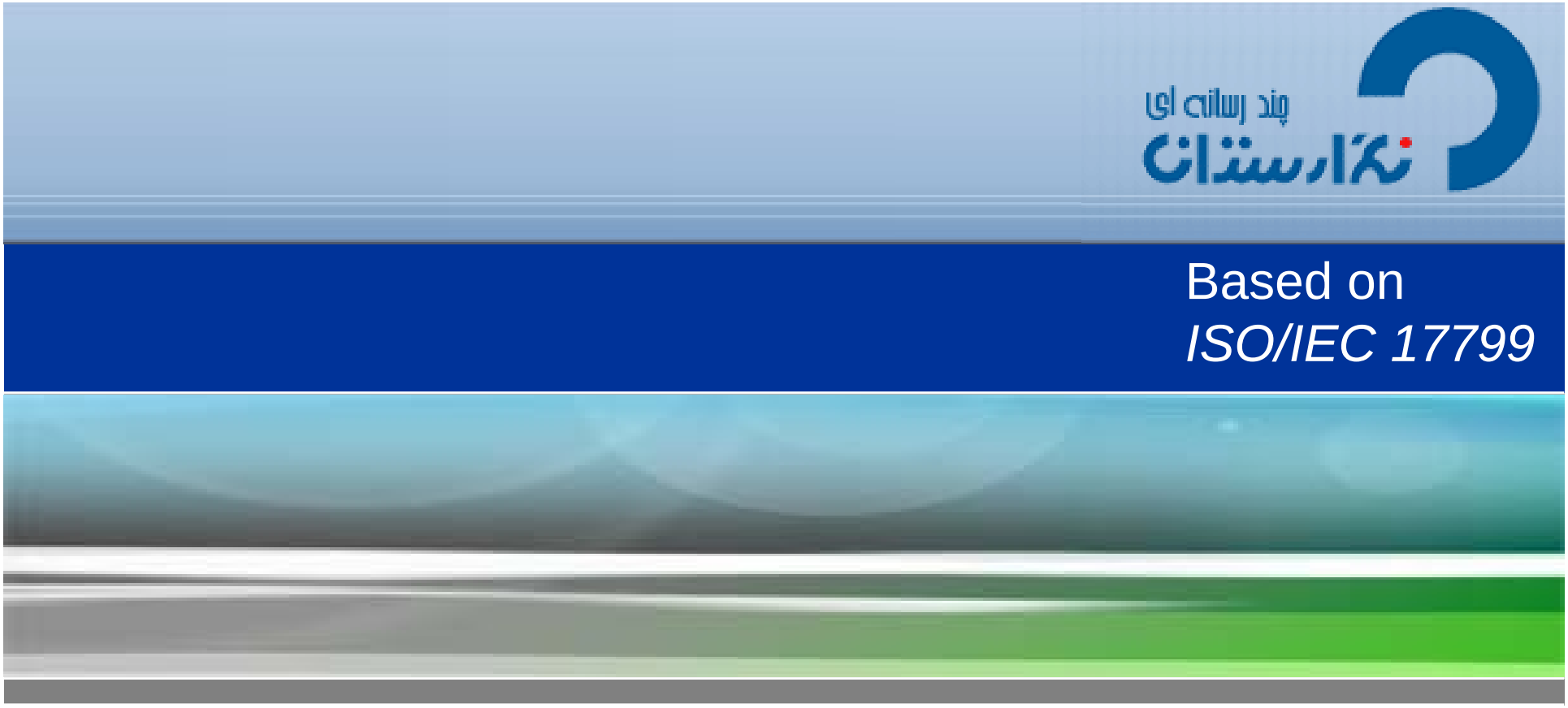
Information Security Management System

Based on
ISO/IEC 17799

Houman Sadeghi Kaji
Spread Spectrum Communication System PhD. ,
Cisco Certified Network Professional Security Specialist
BS7799 LA
info@houmankaji.net

Agenda

- What is Information and Information Security?
- BS 7799/ ISO 17799 Overview
- BS 7799-2 Controls
- Implementation Methodology
- IT Security
- The Internet threat
- Setting the IT security policy framework with BS 7799
- Defining the security requirement
- Designing the security architecture
- Security Project Lifecycle



What is Information and Information Security?

What is Information and Information Security?

“Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected.”

Types of Information

- Printed or written on paper
- Stored electronically
- Transmitted by mail or electronic means
- Shown on corporate videos
- Spoken in conversations

Examples of Threats to Information

- Employees
- Low awareness of security issues
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Email
- Fire, Flood, Earthquake

What is Information Security?

- ISO 17799:2000 defines information security as the preservation of:
  - Confidentiality
    - Ensuring that information is accessible only to those authorized to have access
  - Integrity
    - Safeguarding the accuracy and completeness of information and processing methods
  - Availability
    - Ensuring that authorized users have access to information and associated assets when required

Achieving Information Security

- Implementing a suitable set of controls
  - Policies
  - Practices
  - Procedures
- Controls need to be established to ensure that the specific security objectives of the organization are met

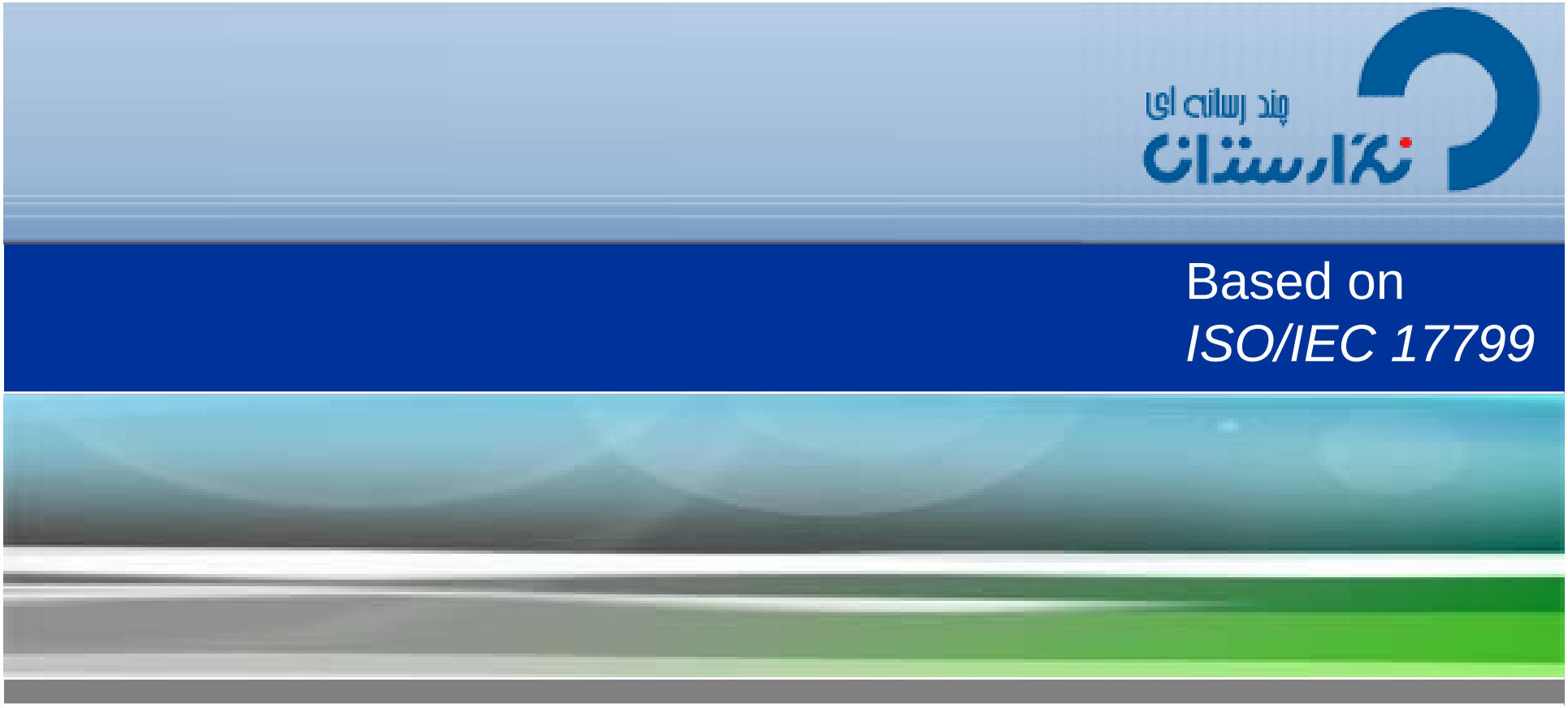
چند رسانه ای
نگارستان

Based on
ISO/IEC 17799

What is a Management System?

Elements of a Management System

- Policy (demonstration of commitment and principles for action)
- Planning (identification of needs, resources, structure, responsibilities)
- Implementation and operation (awareness building and training)
- Performance assessment (monitoring and measuring, handling non-conformities, audits)
- Improvement (corrective and preventive action, continual improvement)
- Management review

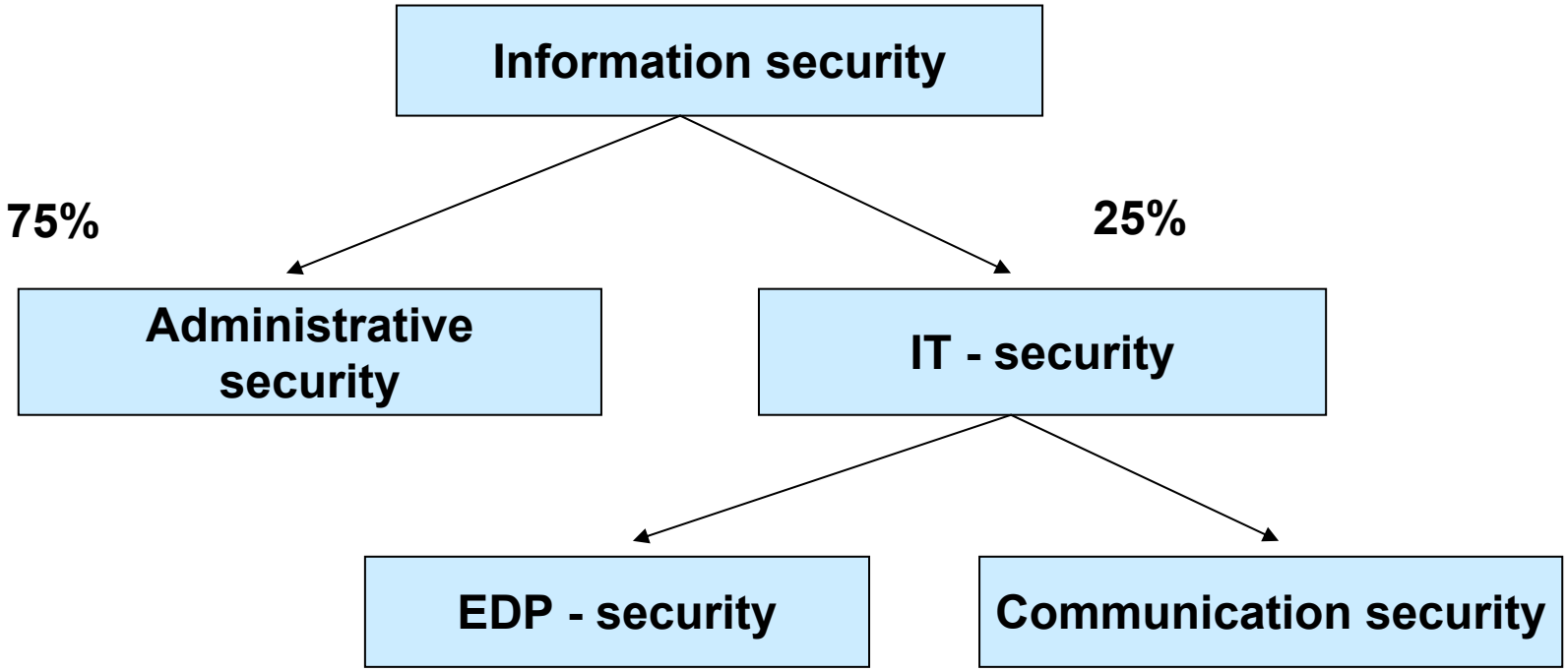


BS 7799/ ISO 17799 Overview

The ISO 17799 Way

Safeguarding the confidentiality, integrity, and availability of written, spoken, and computer information

Information Security - Structure



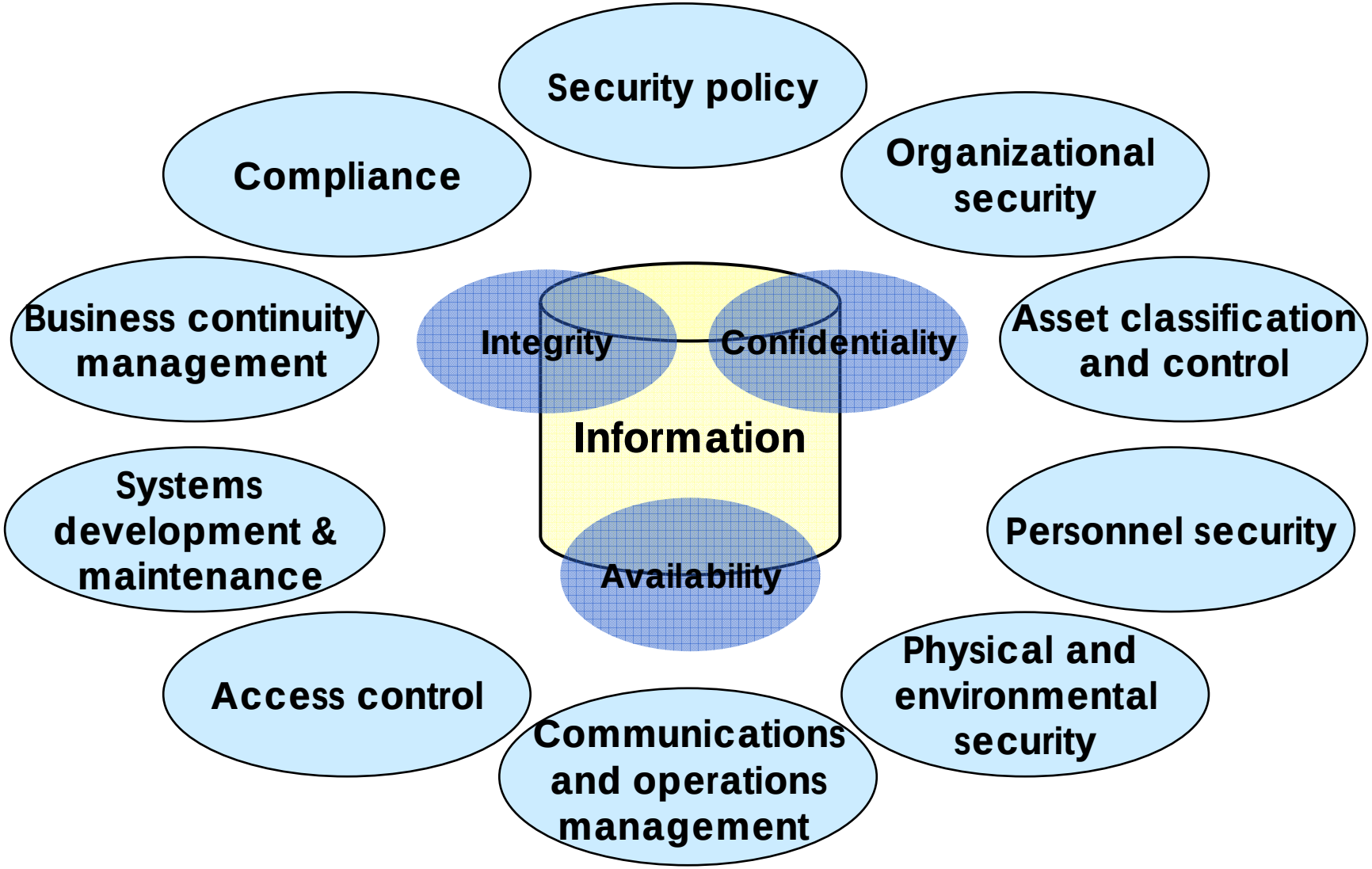
ISO 17799 Is

- An internationally recognized structured methodology dedicated to information security
- A defined process to evaluate, implement, maintain, and manage information security
- A comprehensive set of controls comprised of best practices in information security
- Developed by industry for industry

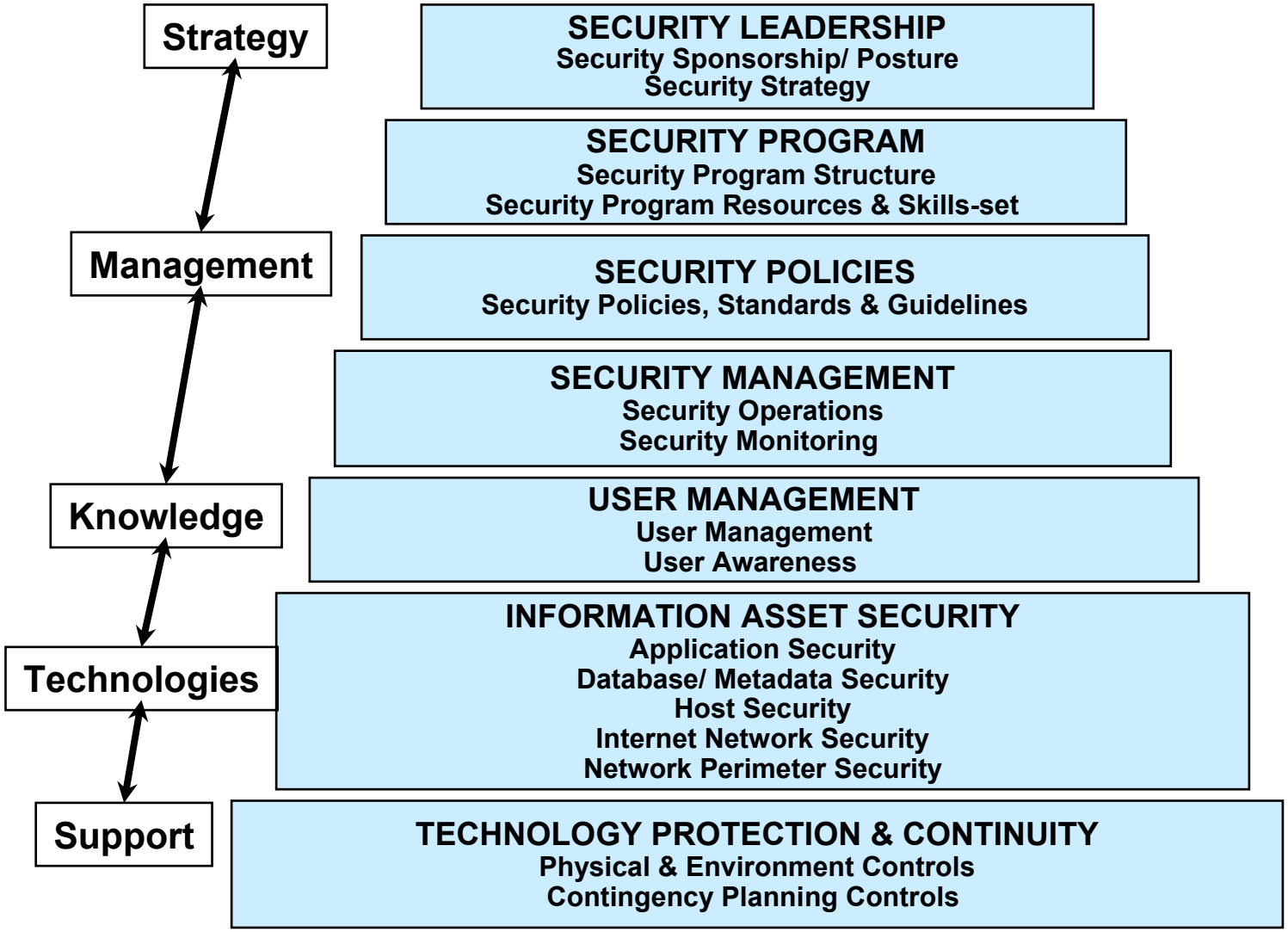
ISO 17799 Is Not

- A technical standard
- Product or technology driven
- An equipment evaluation methodology such as the Common Criteria/ISO 15408
- Related to the "Generally Accepted System Security Principles," or GASSP

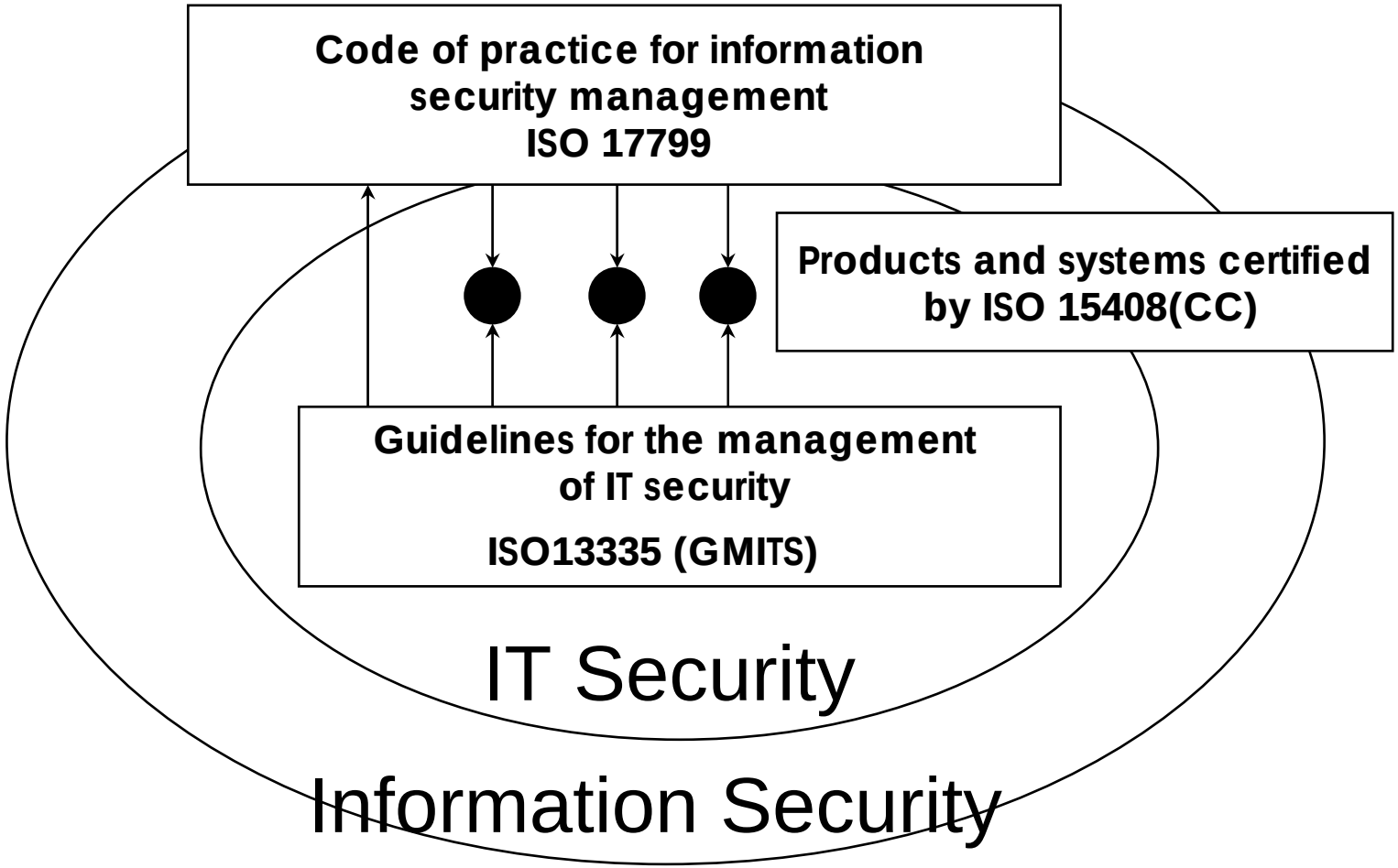
BS 7799 –10 Domains of Information Management

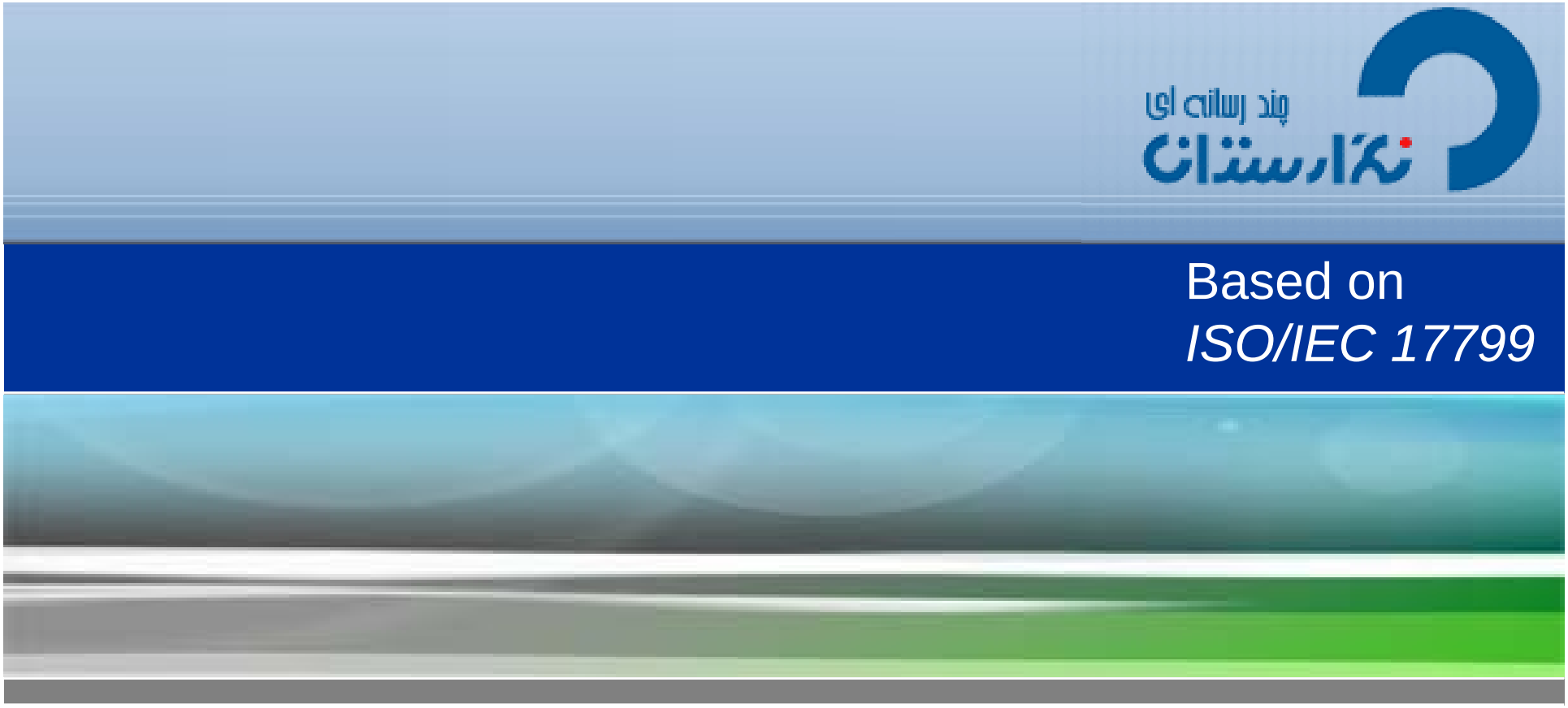


The 10 Sections of ISO 17799



Complementarity with Other ISO Standards





BS 7799-2 Controls

Control Objectives and Controls

- BS 7799-2 ISO 17799 contains:
  - 10 control clauses, 36 control objectives, and 127 controls
- “Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required.”
- “They are either based on essential legislative requirements or considered to be common best practice for information security.”
- “…guiding principles providing a good starting point for implementing information security.”

Main Information Security Issues

- Only 40% of organizations are confident they would detect a systems attack
  - A.9.7 Monitoring system access and use
  - Objective: To detect unauthorized activities
    - A.9.7.1 Event logging
    - A.9.7.2 Monitoring system use
    - A.9.7.3 Clock synchronization

Main Information Security Issues

- 40% of organizations do not investigate information security incidents
  - A.6.3 Responding to security incidents and malfunctions
  - Objective: To minimize the damage from incidents or malfunctions and to monitor and learn from such incidents
    - A.6.3.1 Reporting security incidents
    - A.6.3.4 Learning from incidents

Main Information Security Issues

- Critical business systems are increasingly interrupted - over 75% of organizations experienced unexpected unavailability
  - A.8.2 System planning and acceptance
  - Objective: To minimize the risk of systems failures
    - A.8.2.1 Capacity planning
    - A.8.2.2 System acceptance

Main Information Security Issues

- Business continuity plans exist in only 53% of organizations
  - A.11 Business continuity management
  - Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
    - A.11.1.1 Business continuity management process
    - A.11.1.3 Writing and implementing continuity plans
    - A.11.1.5 Testing, maintaining, and re-assessing business continuity plans

Main Information Security Issues

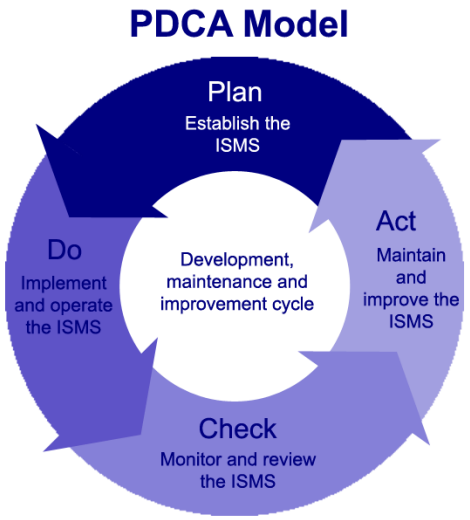
- Only 41% of organizations are concerned about internal attacks on systems, despite overwhelming evidence of the high number of attacks from within organizations
  - A.6 Personnel Security
    - Objective: To reduce the risks of human error, theft, fraud, or misuse of facilities
  - A.7 Physical and environmental security
    - Objective: To prevent unauthorized access, damage, and interference to business premises and information

Main Information Security Issues

- Less than 50% of organizations have information security training and awareness programs
  - A.6.2 User Training
  - Objective: To ensure that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work

4 Information Security Management System

- 4.1 General requirements
- 4.2 Establishing and managing the ISMS
  - Refer to the PDCA model



- 4.3 Documentation Requirements

5 Management Responsibility

- 5.1 Management commitment
- 5.2 Resource management

تشکیلات تامین امنیت شبکه

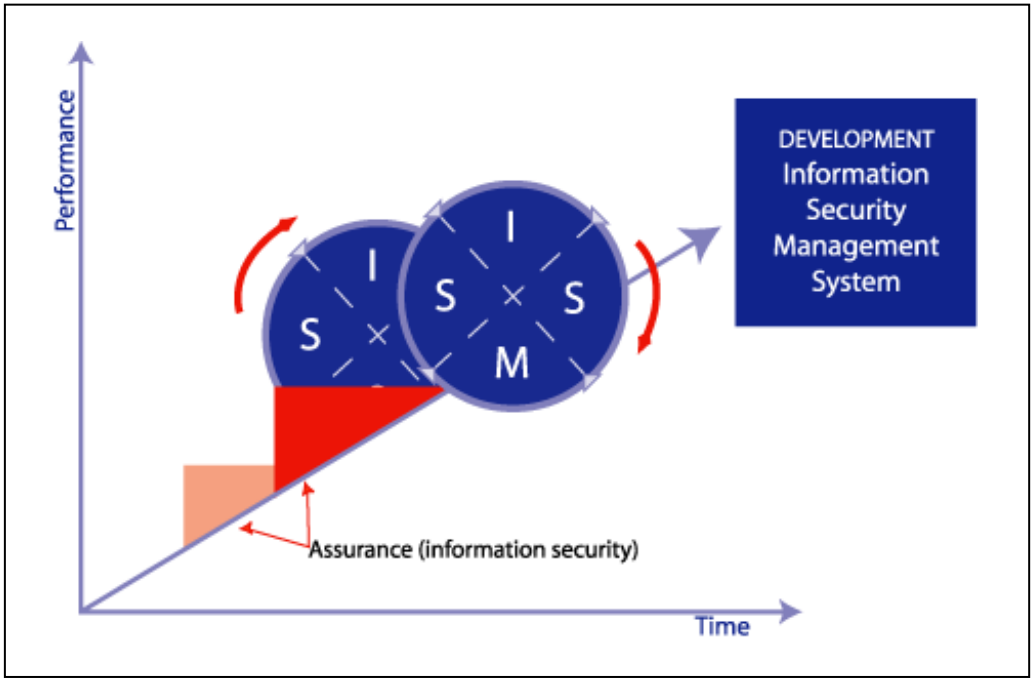
A1.pdf

6 Management Review of the ISMS

- 6.1 General
- 6.2 Review input
- 6.3 Review output
- 6.4 Internal ISMS audits

7 ISMS Improvement

- 7.1 Continual improvement
- 7.2 Corrective action
- 7.3 Preventive action



BS 7799-2 Control Sections

- A.3 Security policy
- A.4 Organizational security
- A.5 Asset classification and control
- A.6 Personnel security
- A.7 Physical and environmental security

سیاست‌های امنیتی کاربران شبکه
A2.pdf

BS 7799-2 Control Sections

- A.8 Communications and operations management
- A.9 Access control
- A.10 System development and maintenance
- A.11 Business continuity management
- A.12 Compliance

چارچوب پیشنهادی برای طرح پشتیبانی حوادث شبکه
A3.pdf

چند رسانه ای
نگارستان

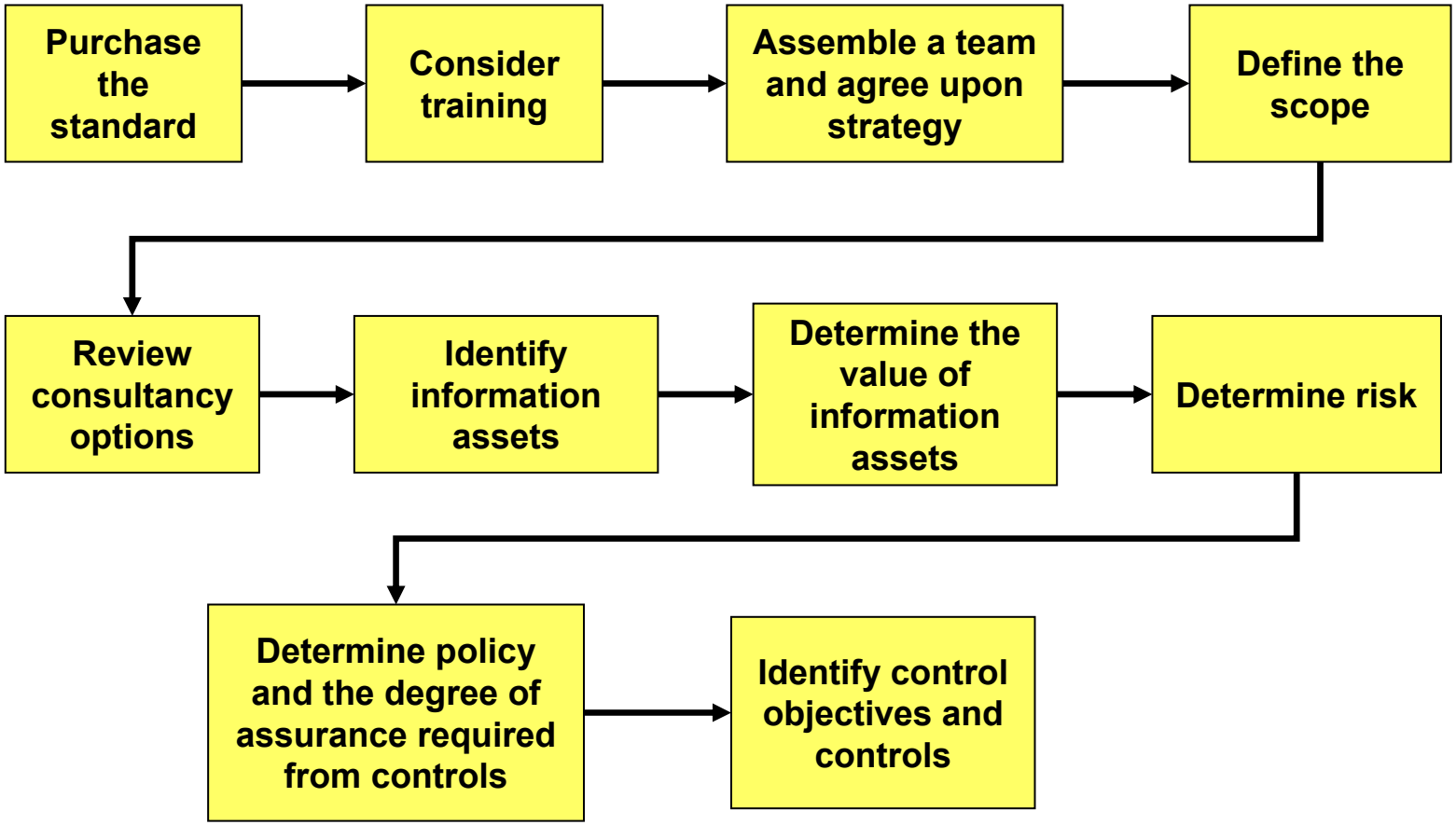
Based on
ISO/IEC 17799

Implementation Methodology

Establishing Security Requirements

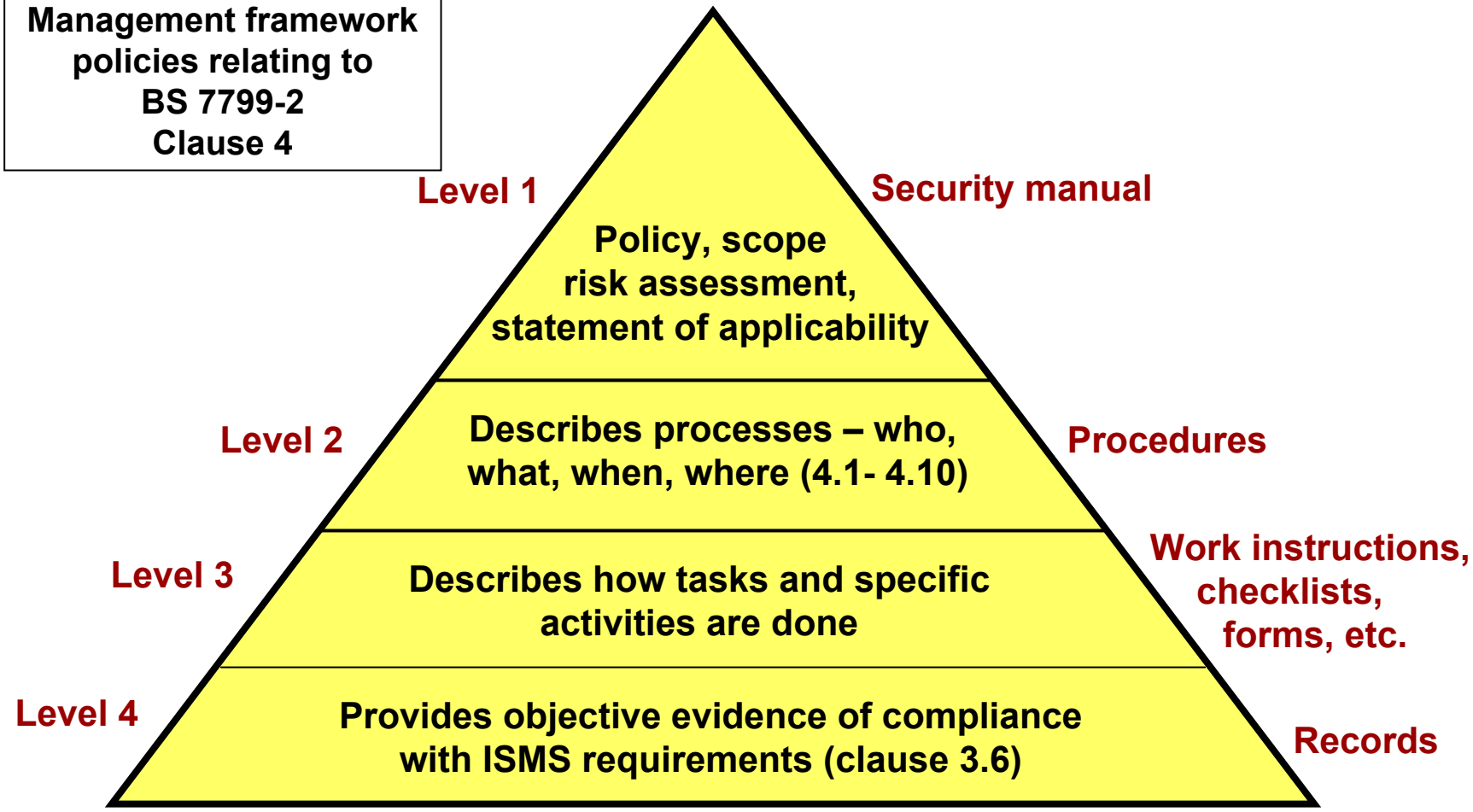
- Assessment of risks to the organization
  - Identify threats to assets, vulnerability to and likelihood of occurrence, potential impact
- Legal, statutory, regulatory, contractual requirements
  - These requirements must be met by the organization, trading partners, contractors, and service providers
- Set of principles, objectives, and requirements for information processing developed by the organization in order to support its operations

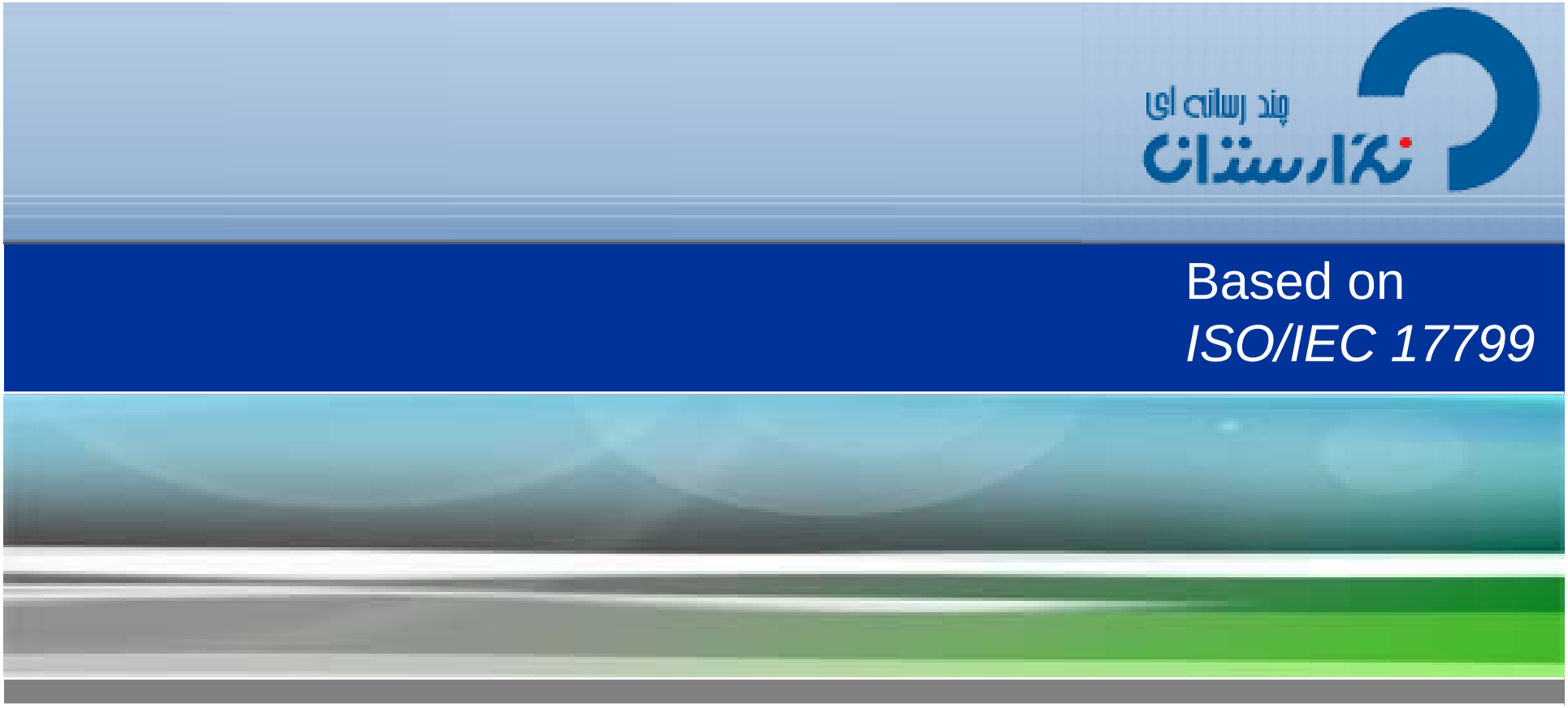
Implementation Process



ISMS Documentation

Management framework policies relating to BS 7799-2 Clause 4

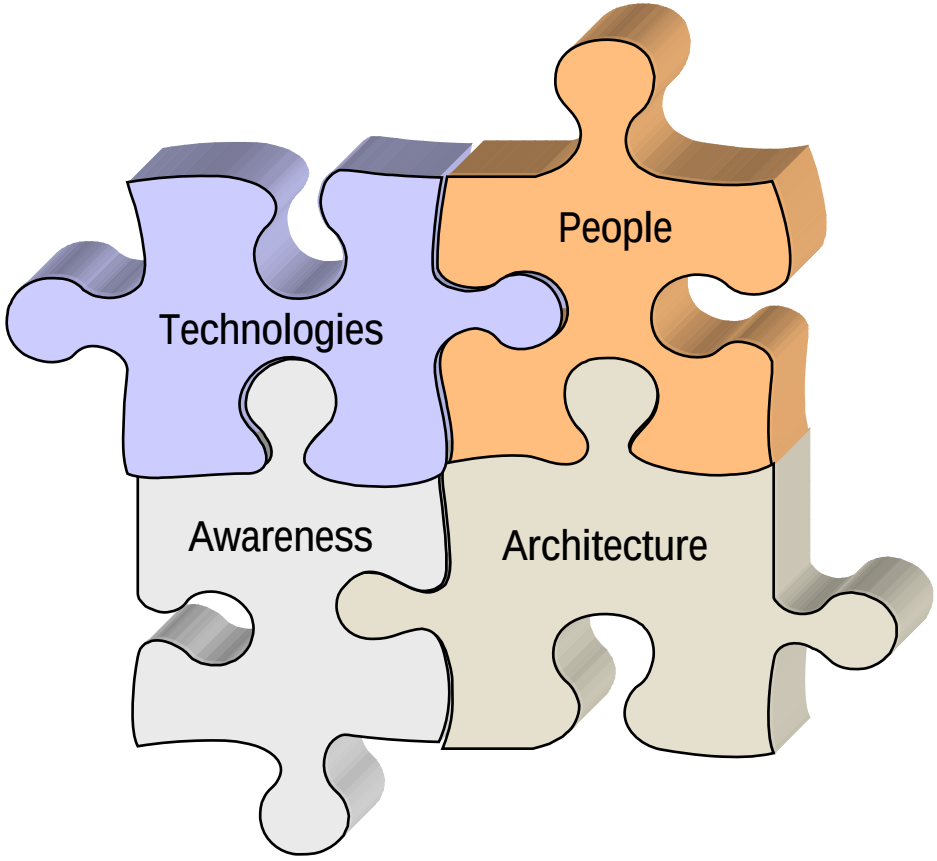




IT Security

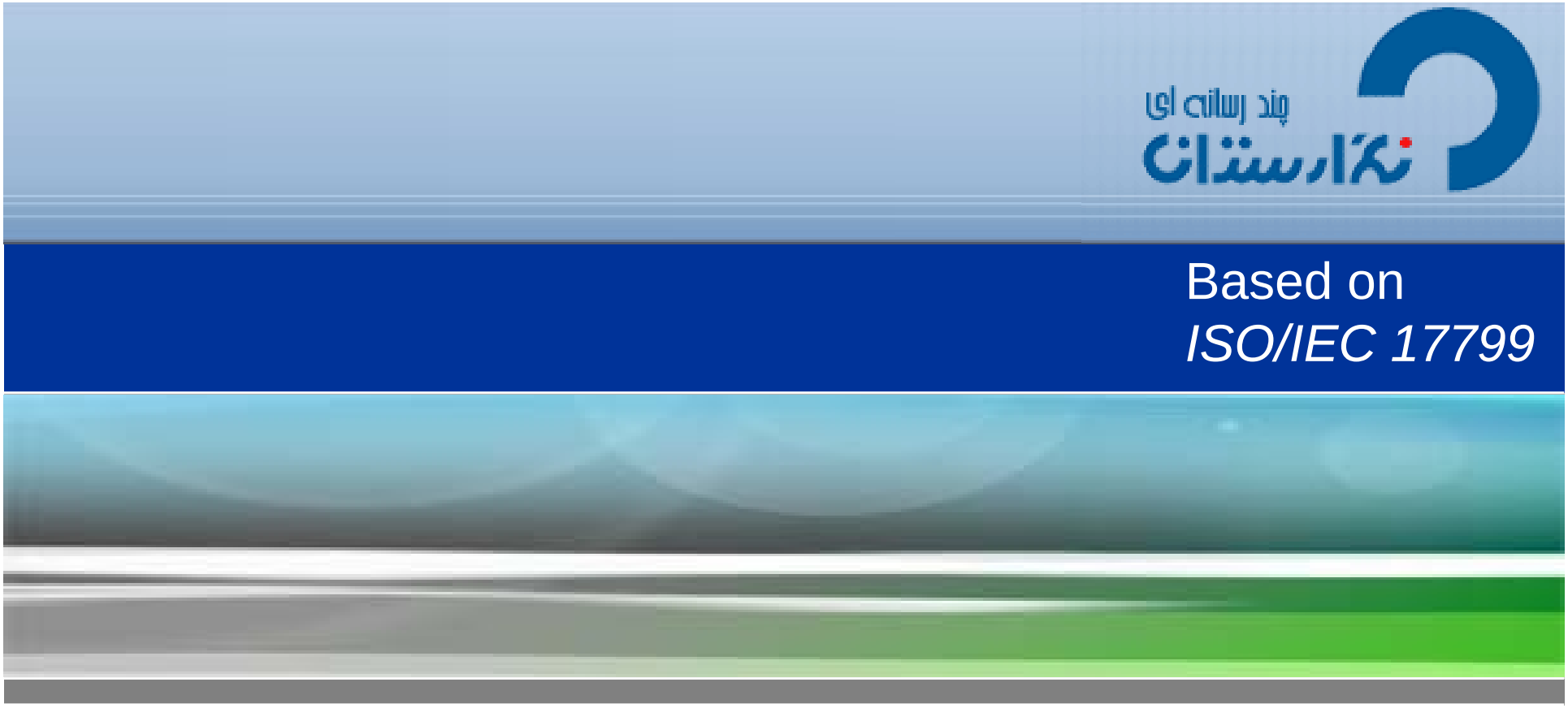
Process View of Security

- People: **Everyone has a role in information security.**
- Architecture: **Aligns security with business, sets management expectations.**
- Awareness: **For expectations to be adhered to they have to be communicated.**
- Technologies: **Security is enforced through selection of products that support the architecture requirements.**



Secure Computing in the Internet age

- The Internet threat
- Setting the IT security policy framework with BS 7799
- Assessing and managing risks
- Defining the security requirement
- Designing the security architecture
- Enabling secure e-business
- Implementing and managing secure e-business solutions
- Security Lifecycle



The Internet Threat

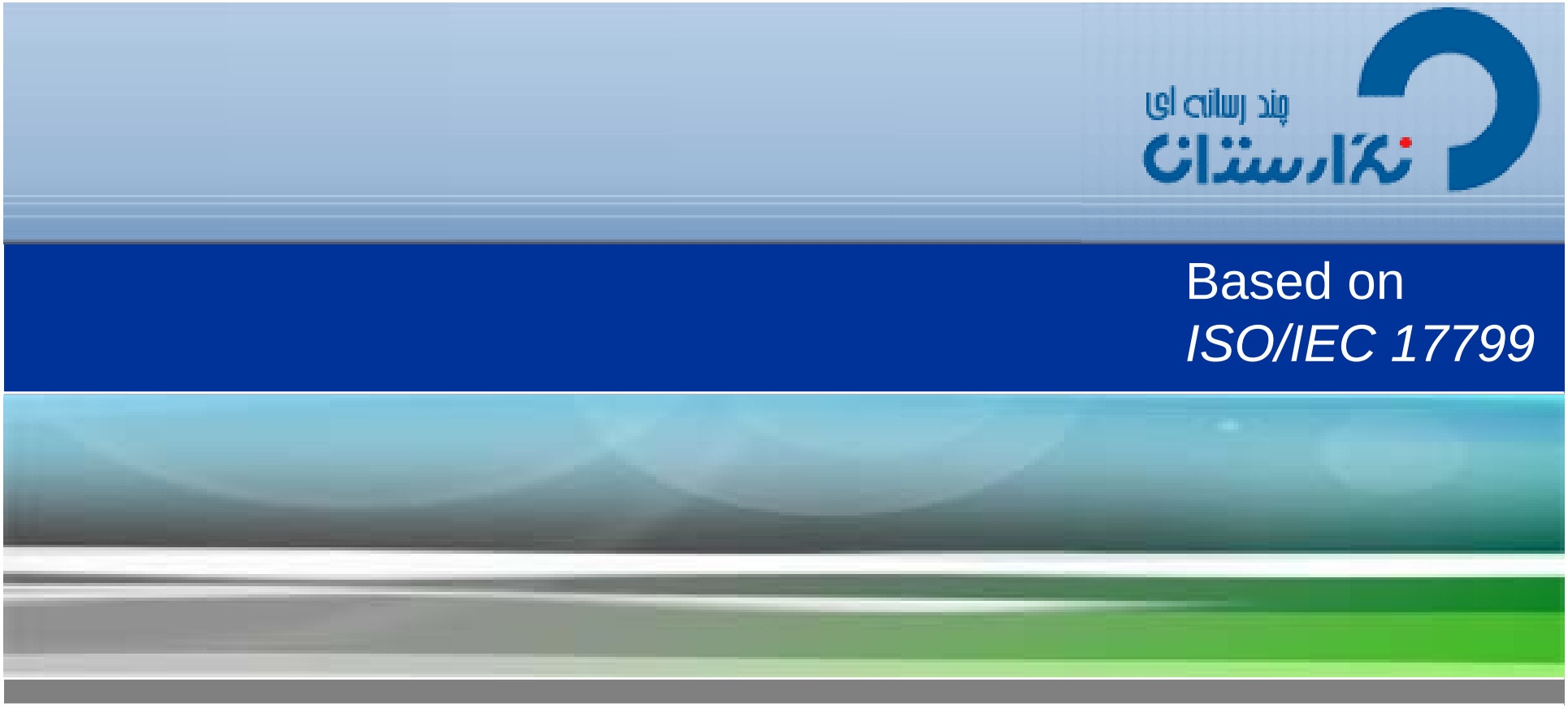
Security Breaches

- **All Systems**
  - **Viruses** **85%**
  - **Insider abuse of Internet Access** **79%**
  - **Denial of Service** **27%**

- **Web sites**
  - **Vandalism** **64%**
  - **Denial of Service** **60%**
  - **Theft of transactional information** **8%**
  - **Financial Fraud** **3%**

Challenges

- **Internet transactions need to achieve**
- **Privacy**
- **Maintainability**
  - Requires constant changing
  - Standards and Technologies Evolving
  - Intruders becoming more sophisticated
- **Security**
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudation



Setting the IT security policy framework

BS7799 (ISO 17799)

- Define Security Policy
- Define Scope of Information Security Management System
- Conduct Risk Assessment
- Select controls form section 4 of BS7799 part 2
- Prepare statement of applicability

BS7799 (ISO 17799)

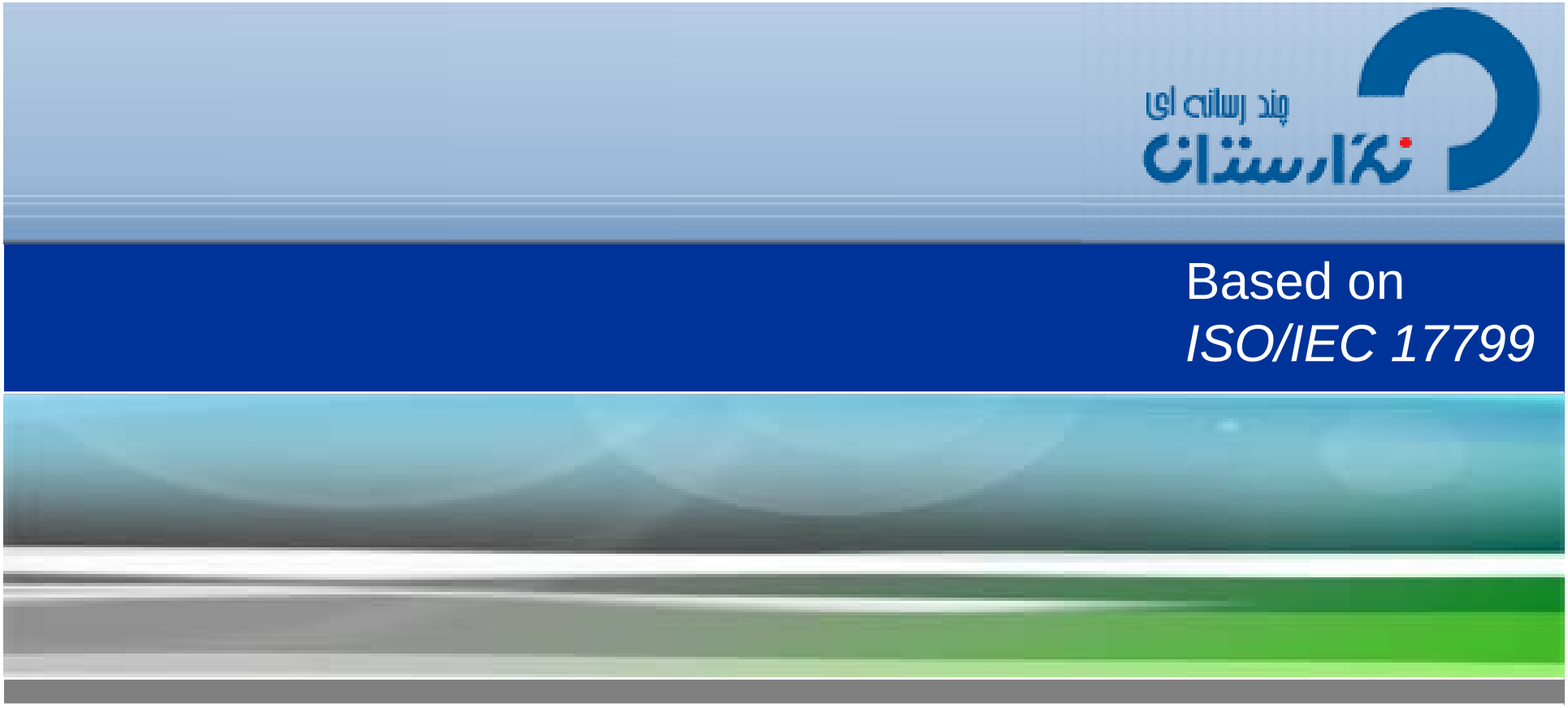
- Information security policy
- Information security Infrastructure
- Information classification & Control
- Personnel Security
- Policy for physical and environmental security
- Responding to security incidents and malfunctions
- Operational procedures and responsibilities

Case Study

Policy : B1.pdf

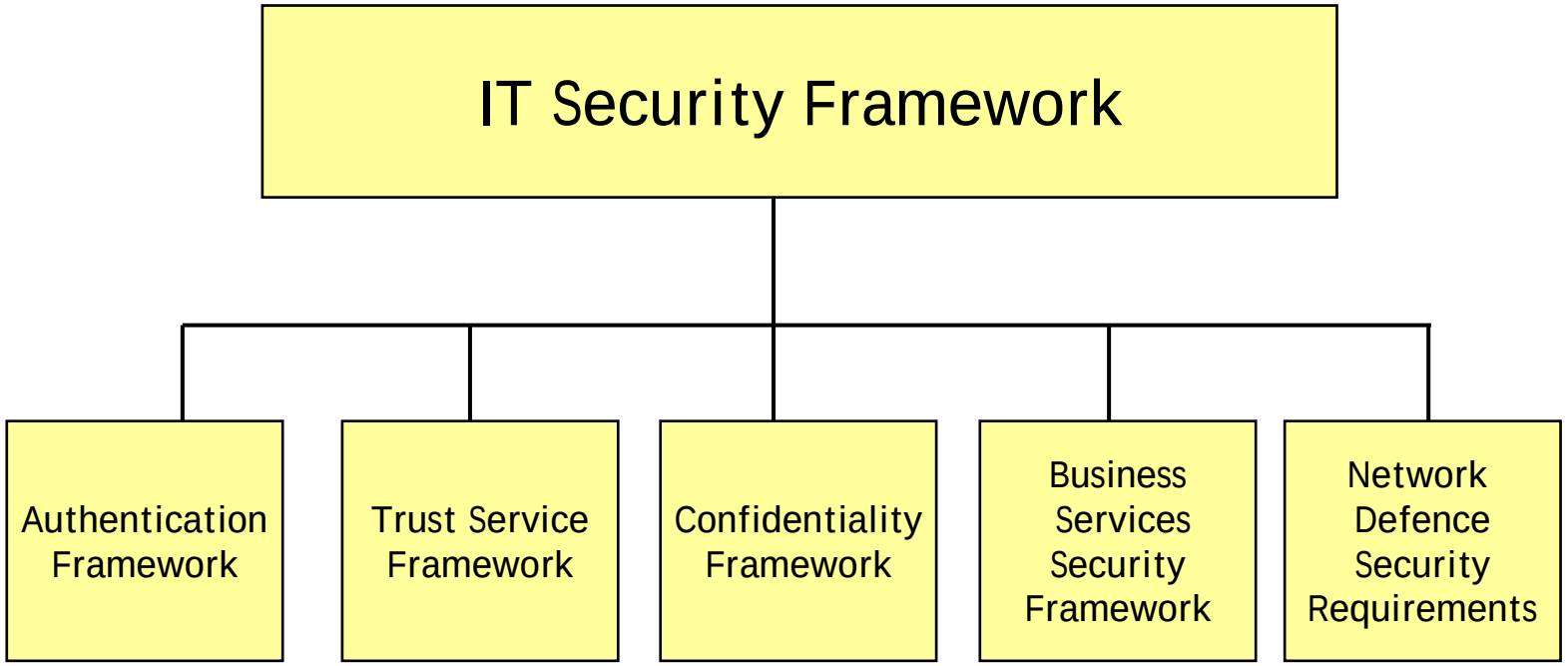
Procedure : B2.pdf

Form : B3.pdf



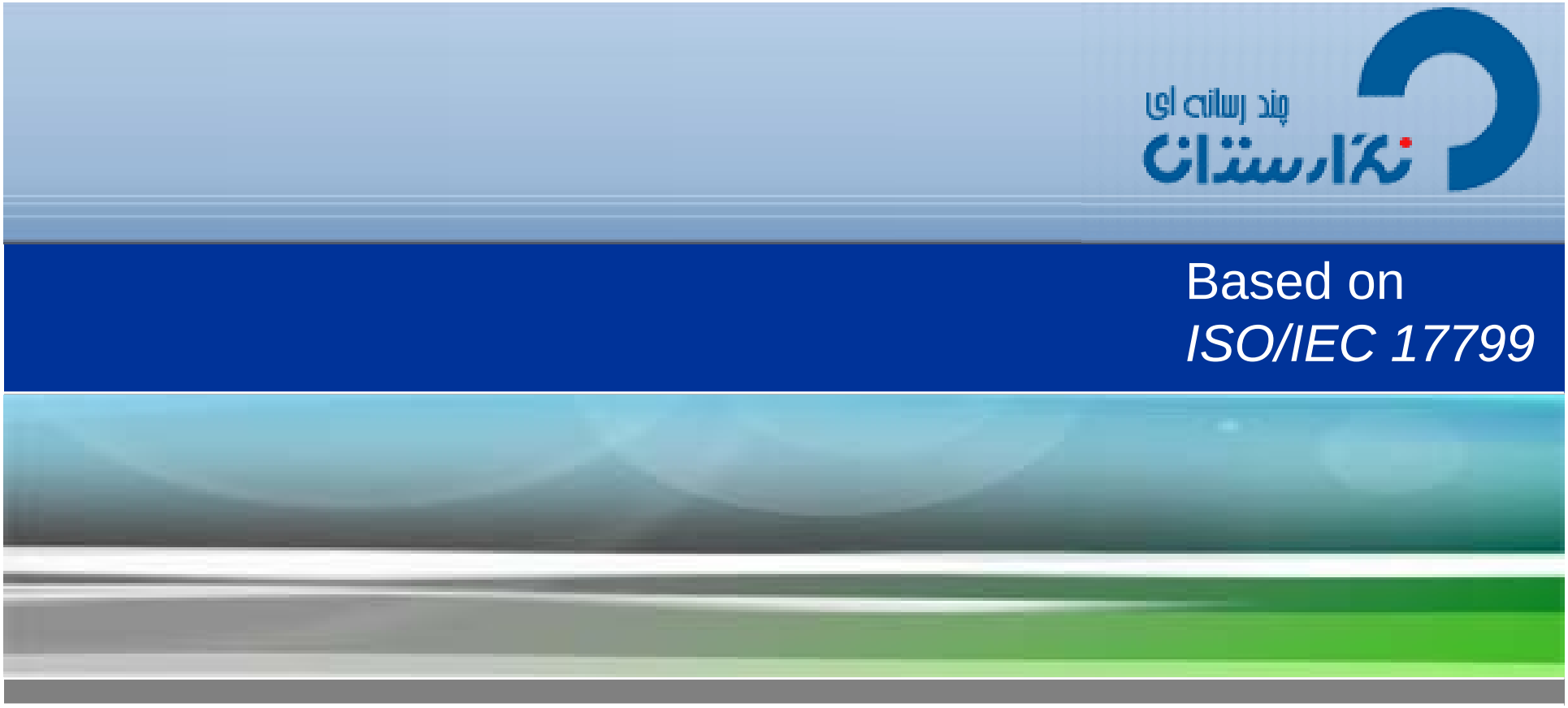
Defining the security requirement

Defining the security requirement



IT Security Framework

- **Authentication Framework**
  - Users Uniquely and unambiguously identified and granted access only when authorisation granted
- **Trust Services Framework**
  - Transactions traceable and accountable to authenticated individuals
- **Confidentiality Framework**
  - Information stored and transferred safely
- **Business Services Security Framework**
  - Applications should be designed, and operated in a secure manner and their information assets properly protected. Business applications should include the web servers which host them.
- **Network Defence**
  - Computer equipment and data are protected against malicious attack and non malicious failures.



Designing the security architecture

Designing the security architecture

- Firewalls
- Virus protection
- Security standards
- Access controls
- Audit & monitoring

- Secure sockets layer
- Digital signatures
- X509 certificates
- Certificate management
- Intranets
- Extranets (VPN)

Organisations consider the following

1. Security policies must be in place
2. Conducted risk analysis
3. The system must be accredited !!
4. Authentication & access controls implemented
5. Regular accounting & auditing (internally & mailguards/firewalls)
6. Strictly controlled external connections to other systems/ organisations

چند رسانه ای
نگارستان

Based on
ISO/IEC 17799

Security Project Life Cycle

Security Project Life Cycle

Require-ments Analysis	Technical Options	Design	Develop	Test	Implement	Live System
Risk Assessment	Identify Security Products	Design Security Services	Integrate Security	Test Security	Set-up Security	Manage Security
Security Policy & Procedures						

The Secure IT Business