NFbraska CERT Conference 2006
Computer Security and Information Assurance

The Information Security Management Process based on ISO 27001

Ing. Leonardo García Rojas

CISSP, CISM, CISA, ISO9000LA, ISMS IRCA LA, BS7799LA, PMP

leonardo_garciar@yahoo.com

lgarcia@intelematica.com.mx

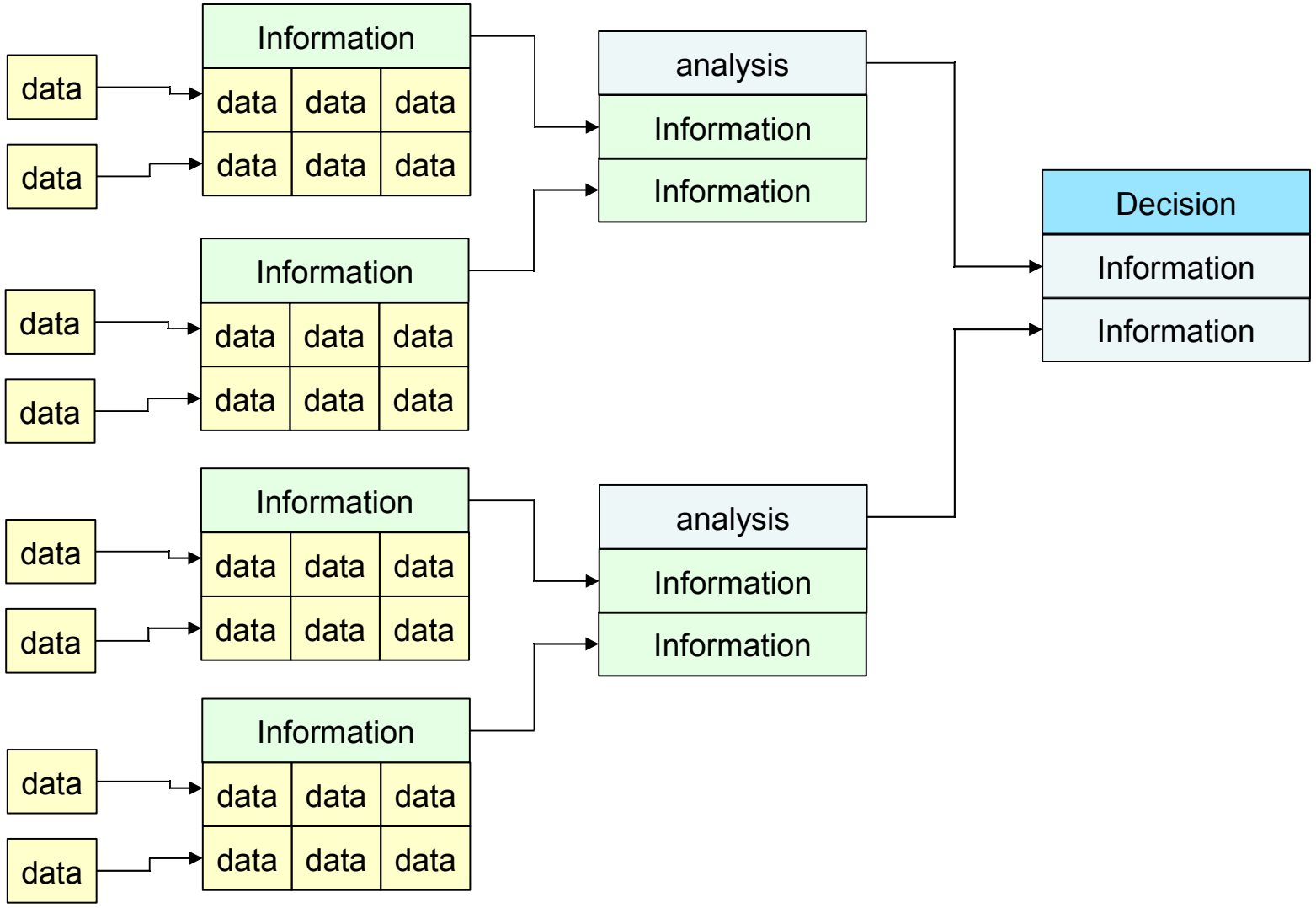
What is Data, Information and Information Security?

“Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.”

ISO/IEC 17799

Data is a bunch of registers that has value if they are interpreted in the way to take a decision

From data to decisions



Types of information

- On paper
- Stored electronically
- Transmitted by regular mail or e-mail
- Videos
- Spoken in conversations

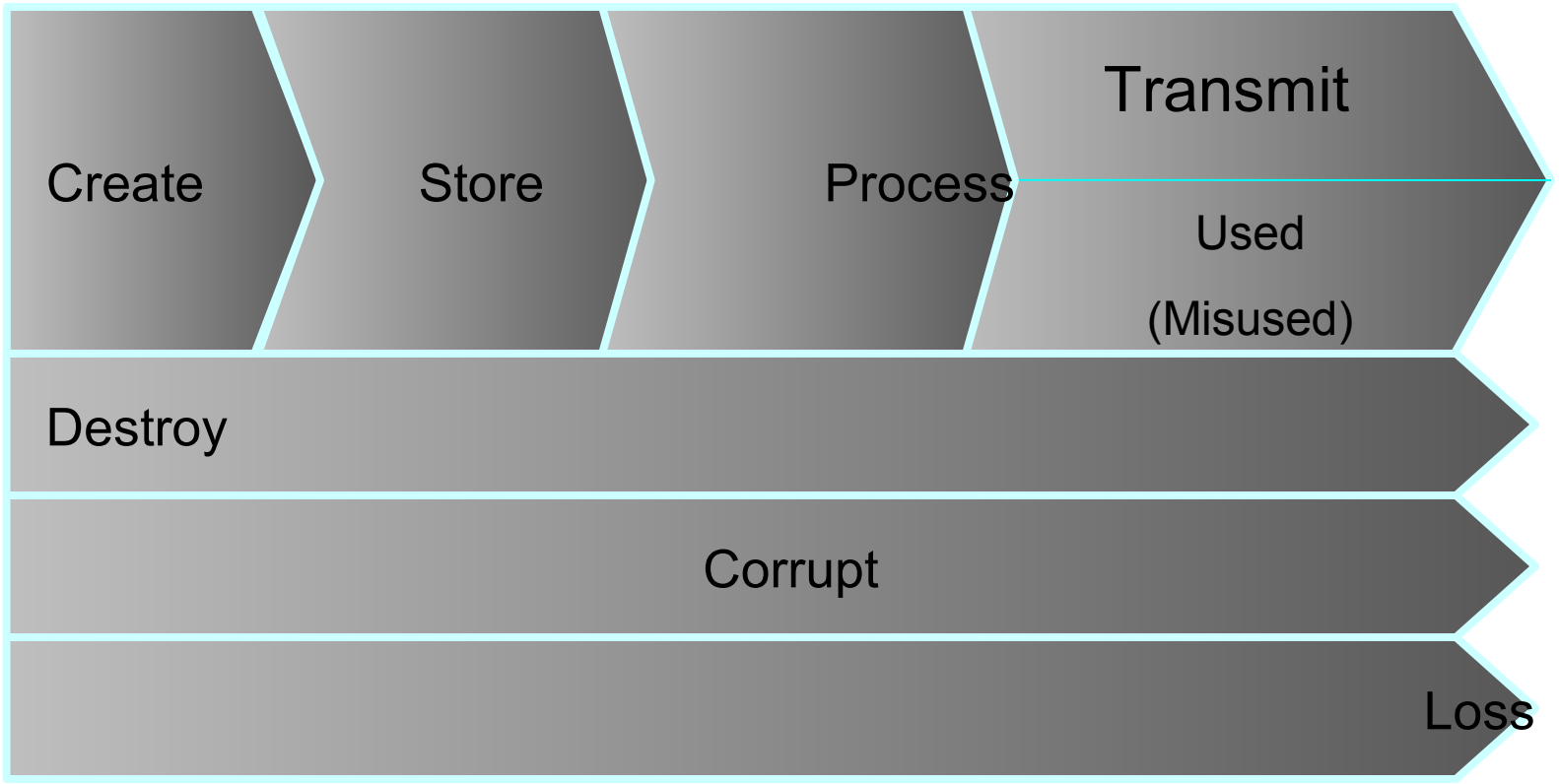
Information used and risk level by sector

- Agriculture
- Construction & real state
- Food & Tobaco
- Industrial equipment
- Mining

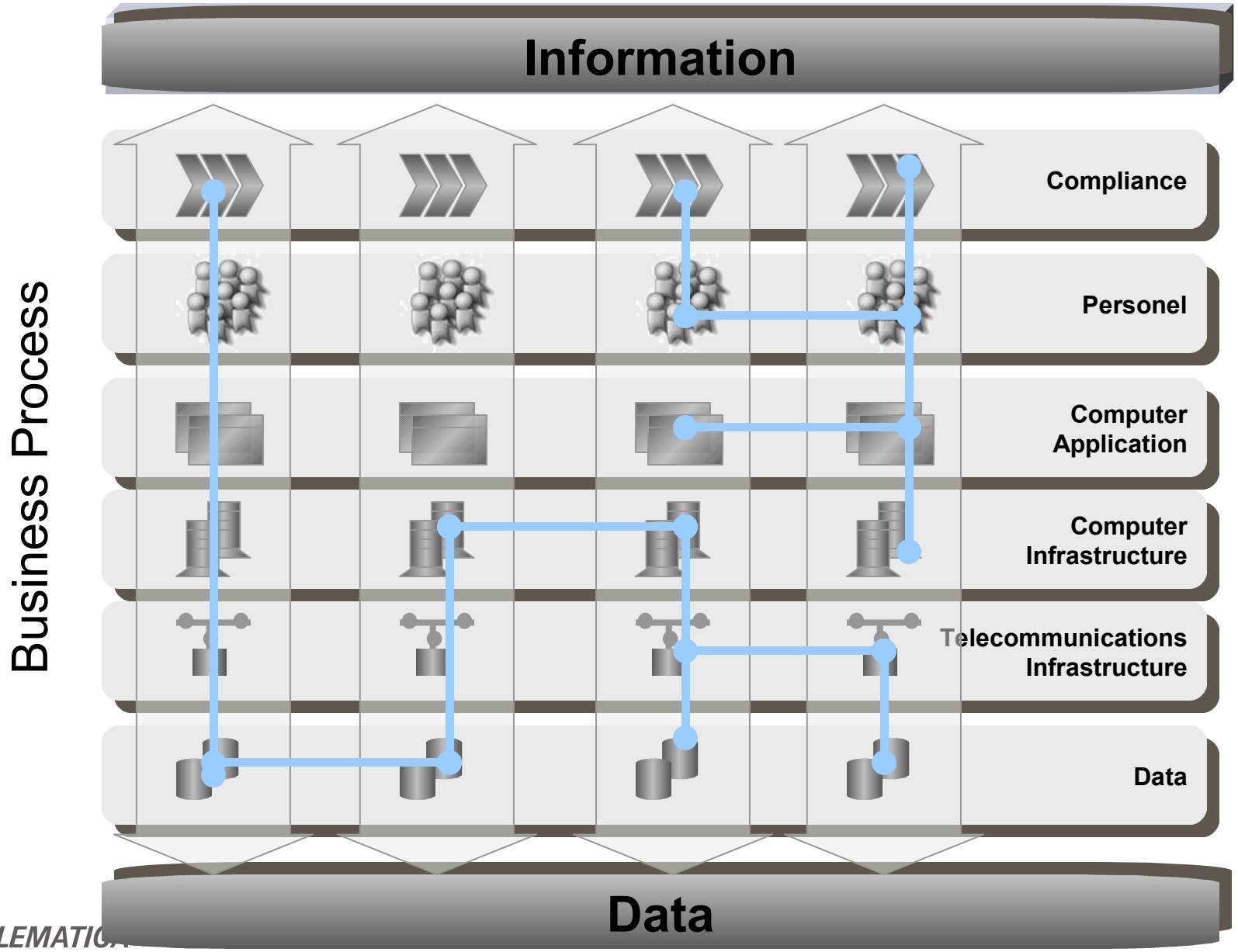
- Automitive
- Chemical
- Energy (Oil & Gas)
- Transportation

- Pharmaceutical
- Telecommunications
- Government
- Aerospace
- Defense
- Biomedic
- Electronics
- Finacial Services
- Health
- Information Services
- Retail

Information life cycle



Data and information



Threats to Information

- **Examples**
  - **Employees**
  - **Low awareness about information security**
  - **Growth in networking and distributed computing**
  - **Hacking tools and viruses**
  - **E-Mail**
  - **Naturals - Fire, flood, earthquake**

What is Information Security

- **Confidentiality**
  - the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**
  - the property of safeguarding the accuracy and completeness of assets
- **Availability**
  - the property of being accessible and usable upon demand by an authorized entity

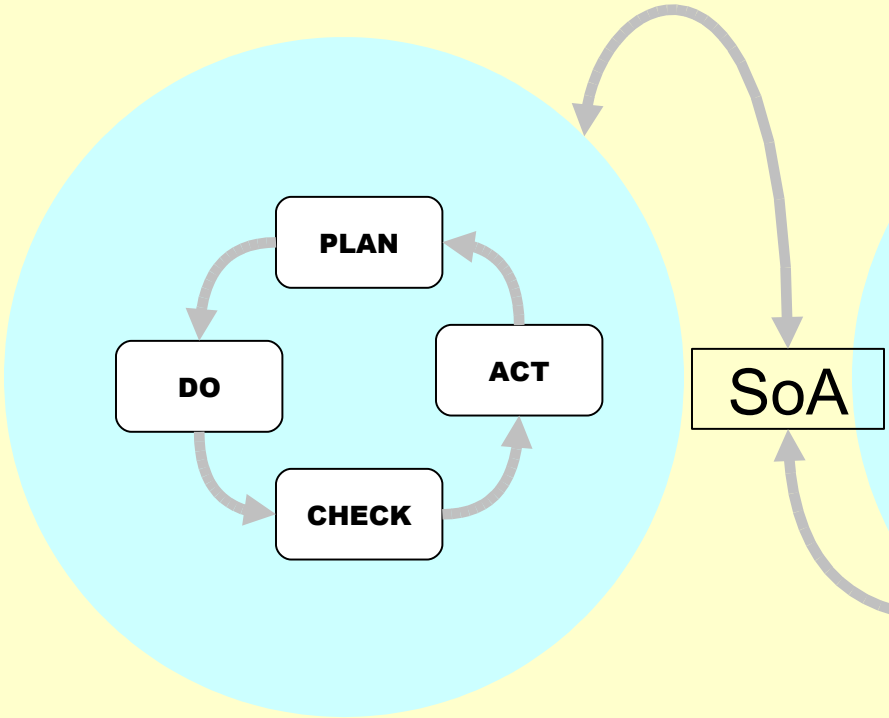
Achieving Information Security

- **Implementing a set of controls**
  - **Policies**
  - **Practices**
  - **Procedures**
  - Organizational structures
  - Software functions
- **Controls are selected based on a Risk Assessment**

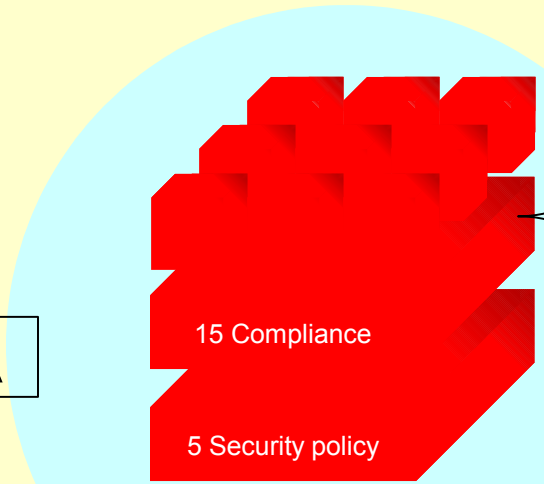
What is an Information Security Management System?

ISMS

ISMS Scope and boundary



SoA



6 Organization of information security

7 Asset management

8 Human resources security

9 Physical and environmental security

10 Communications and operations management

11 Access control

12 Information systems acquisition, development and maintenance

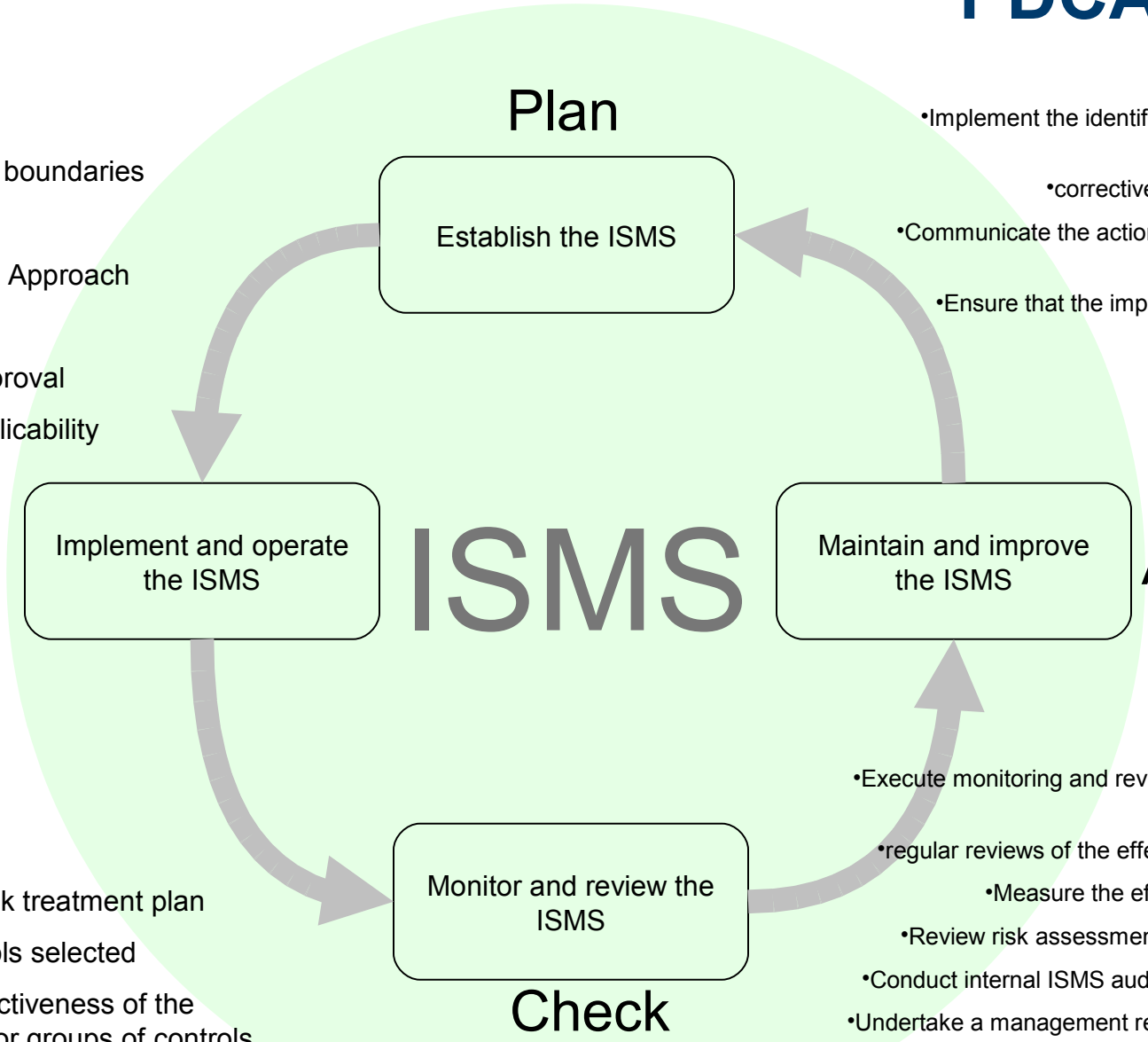
13 Information security incident management

14 Business continuity management

ISMS

Information Security Architecture

PDCA Model



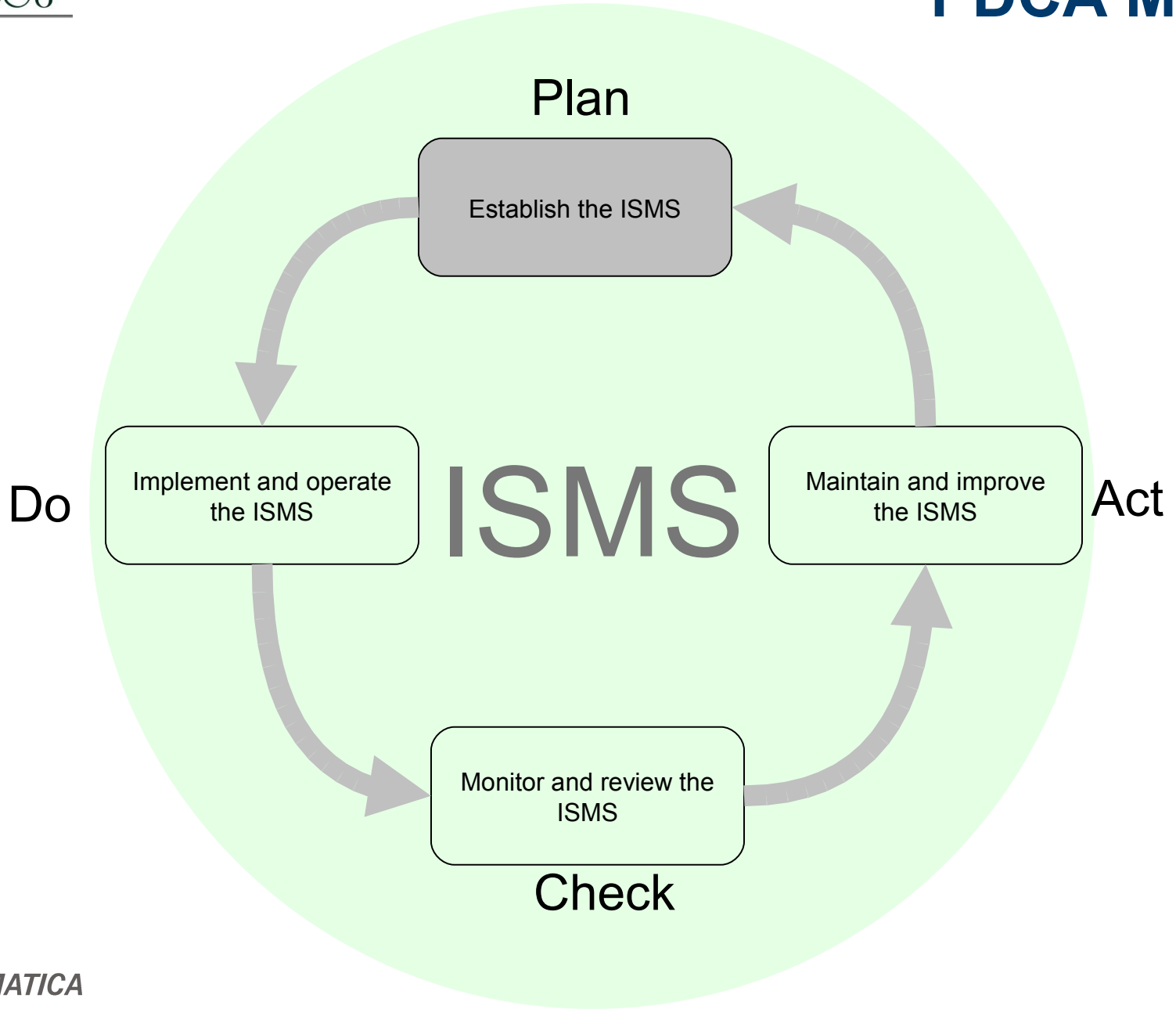
- ISMS Scope and boundaries
- ISMS Policy
- Risk Assessment Approach
- Risk treatment
- Management approval
- Statement of applicability

- Implement the identified improvements in the ISMS.
- corrective and preventive actions
- Communicate the actions and improvements to all interested parties
- Ensure that the improvements achieve their intended objectives.

- Implement the risk treatment plan
- Implement controls selected
- measure the effectiveness of the selected controls or groups of controls

- Execute monitoring and reviewing procedures and other controls
- regular reviews of the effectiveness of the ISMS
- Measure the effectiveness of controls
- Review risk assessments at planned intervals
- Conduct internal ISMS audits at planned intervals
- Undertake a management review of the ISMS on a regular basis
- Update security plans

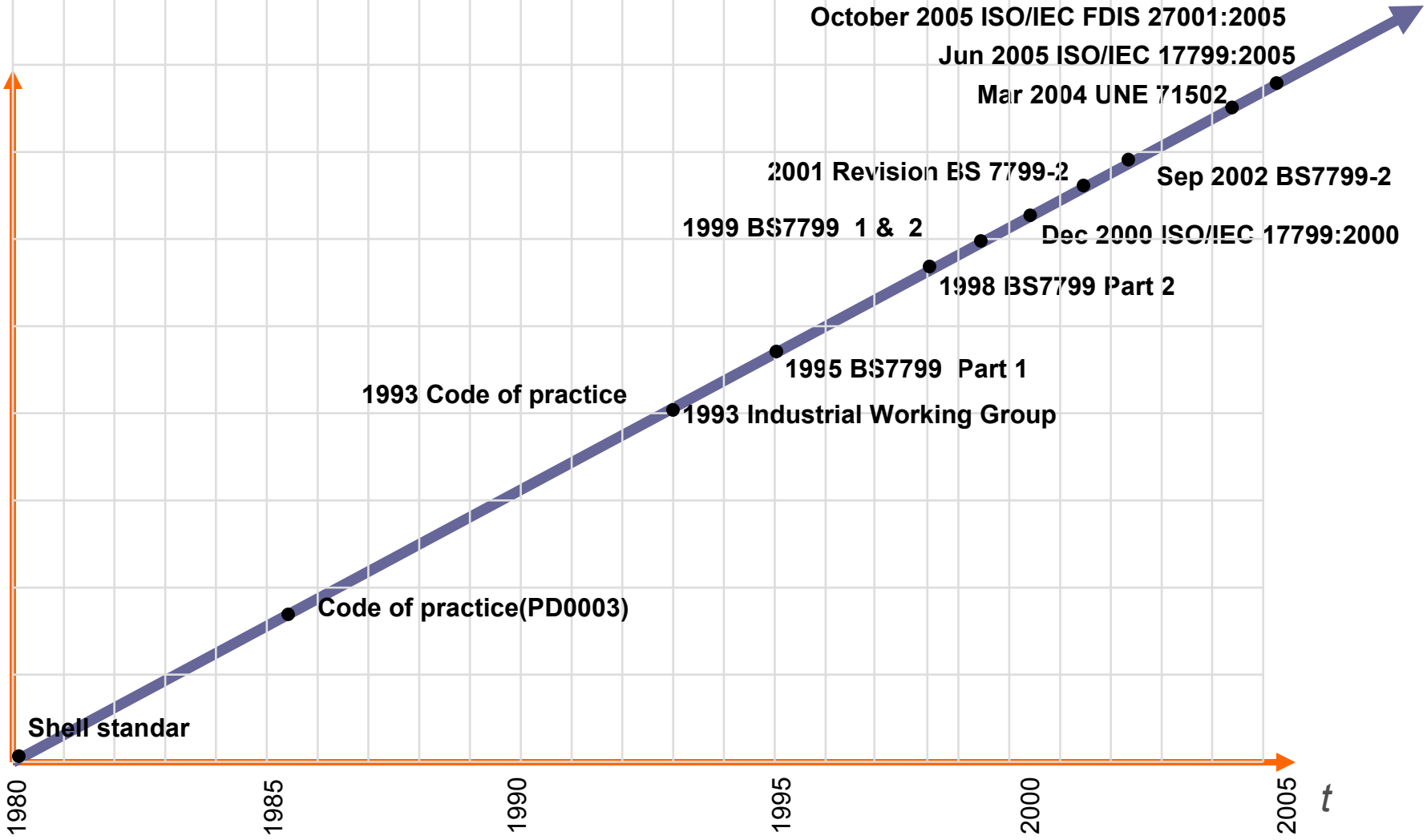
PDCA Model


Plan
Establish the ISMS
Do
Implement and operate the ISMS
ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check

ISMS

- A management system is a system to establish policy and objectives and to achieve those objectives.
- Management systems are used by organizations to develop their policies and to put these into effect via objectives and targets using:
  - Organizational structure
  - Processes and associated resources
  - Measurement and evaluation methodology
  - Review process to ensure problems are corrected and opportunities for improvement are recognized and implemented when justified

History

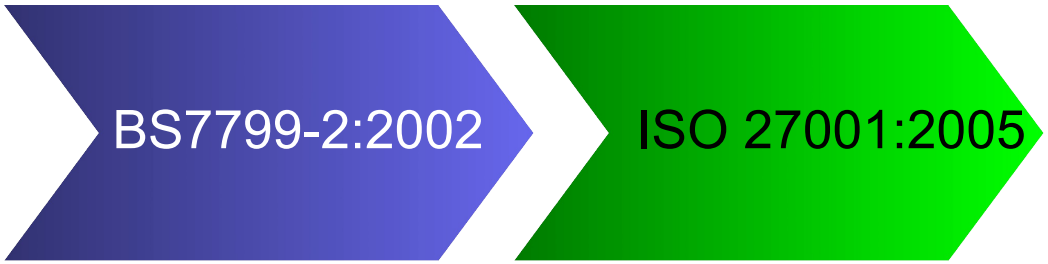

October 2005 ISO/IEC FDIS 27001:2005
Jun 2005 ISO/IEC 17799:2005
Mar 2004 UNE 71502
2001 Revision BS 7799-2
Sep 2002 BS7799-2
1999 BS7799 1 & 2
Dec 2000 ISO/IEC 17799:2000
1998 BS7799 Part 2
1995 BS7799 Part 1
1993 Code of practice
1993 Industrial Working Group
Code of practice(PD0003)
Shell standar
1980
1985
1990
1995
2000
2005
t

International Transition

10 Domains
36 Objetive controls
127 Controls

10 Domains
36 Objetive controls
127 Controls

11 Domains
39 Objetive controls
133 Controls



10 Domains
36 Objetive controls
127 Controls

10 Domains
36 Objetive controls
127 Controls

ISMS Implementation

The scope and boundaries of the ISMS are defined including details of and justification for any exclusion from the scope

ISMS Policy

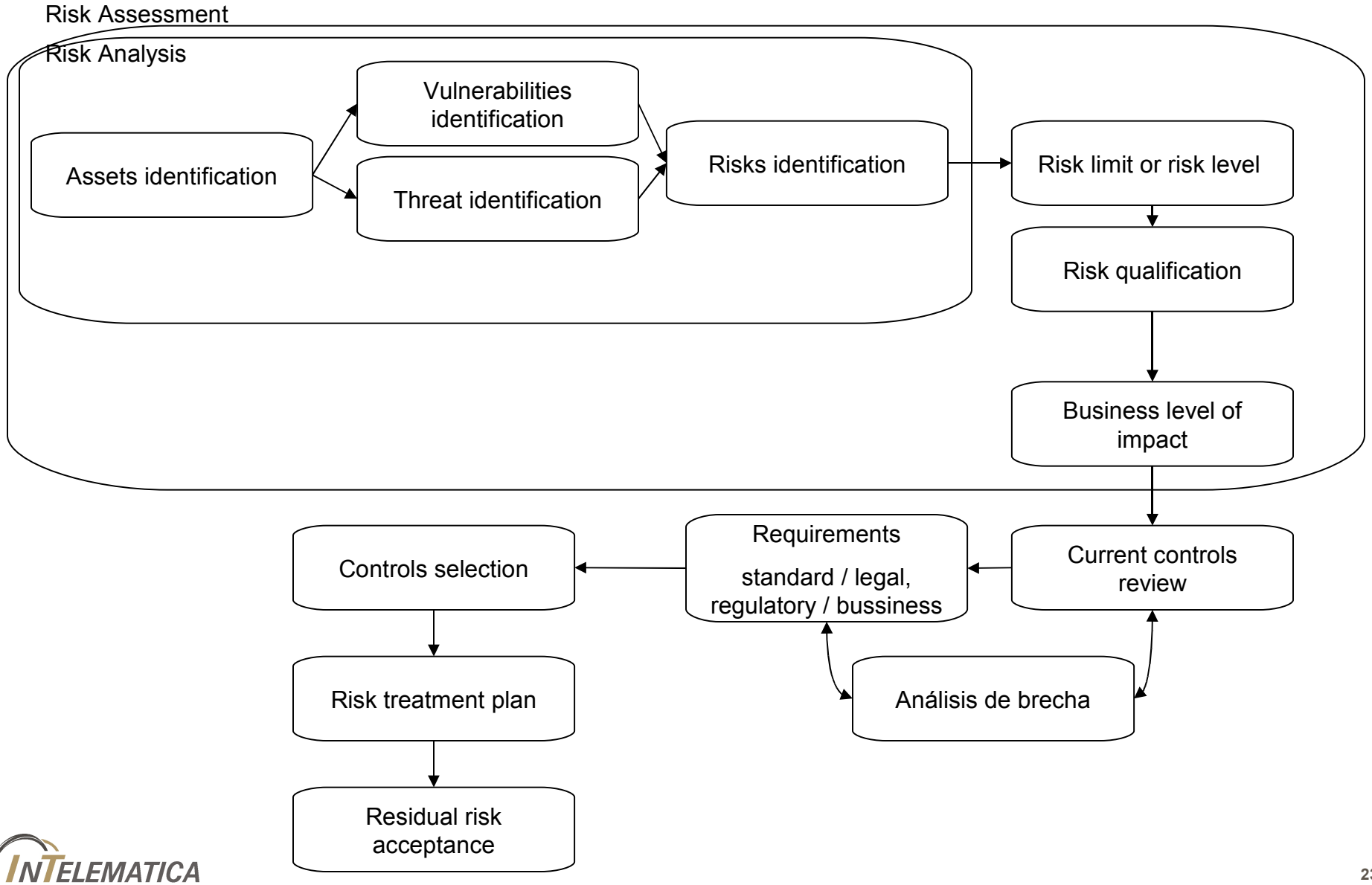
- The ISMS policy aligns with the organisation's strategic risk management context.
- The ISMS policy is regarded as a superset of the information security policy.

Risk Assessment

- The selected risk assessment methodology ensures that risk assessments produce comparable and reproducible results.

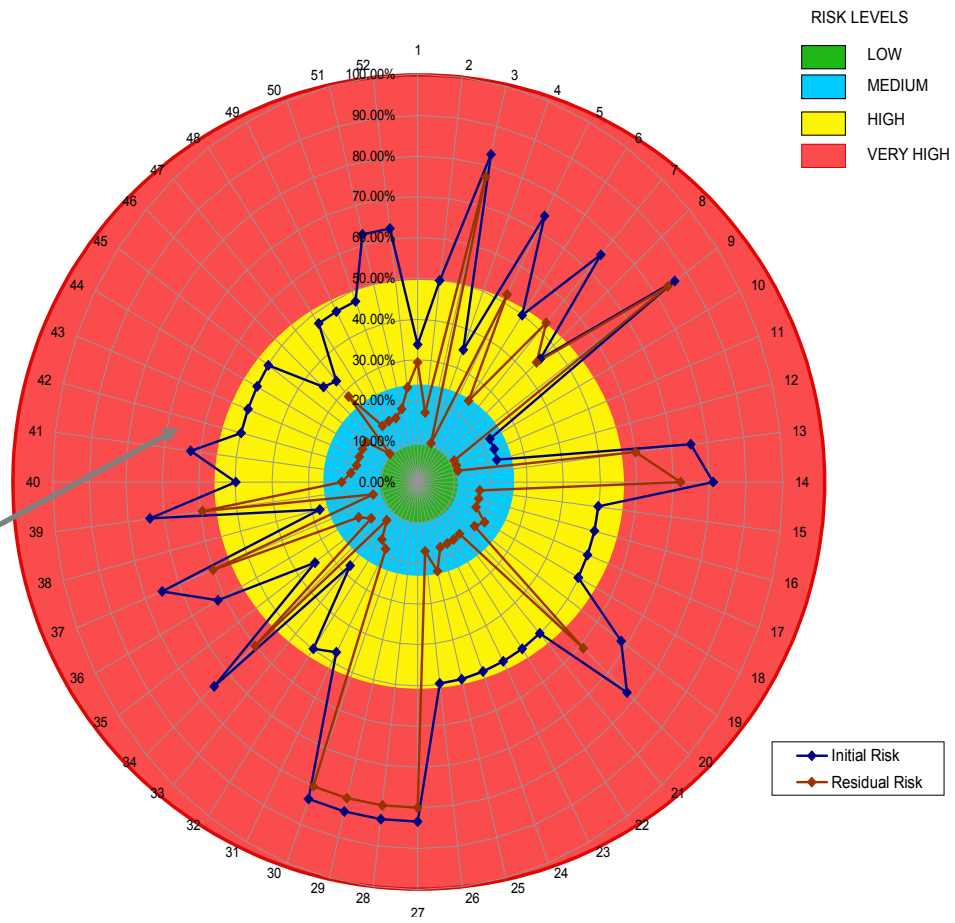
- The organisation needs to perform and analysis and evaluation of the risks and assess the business impact resulting from a security failure, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

Risk management

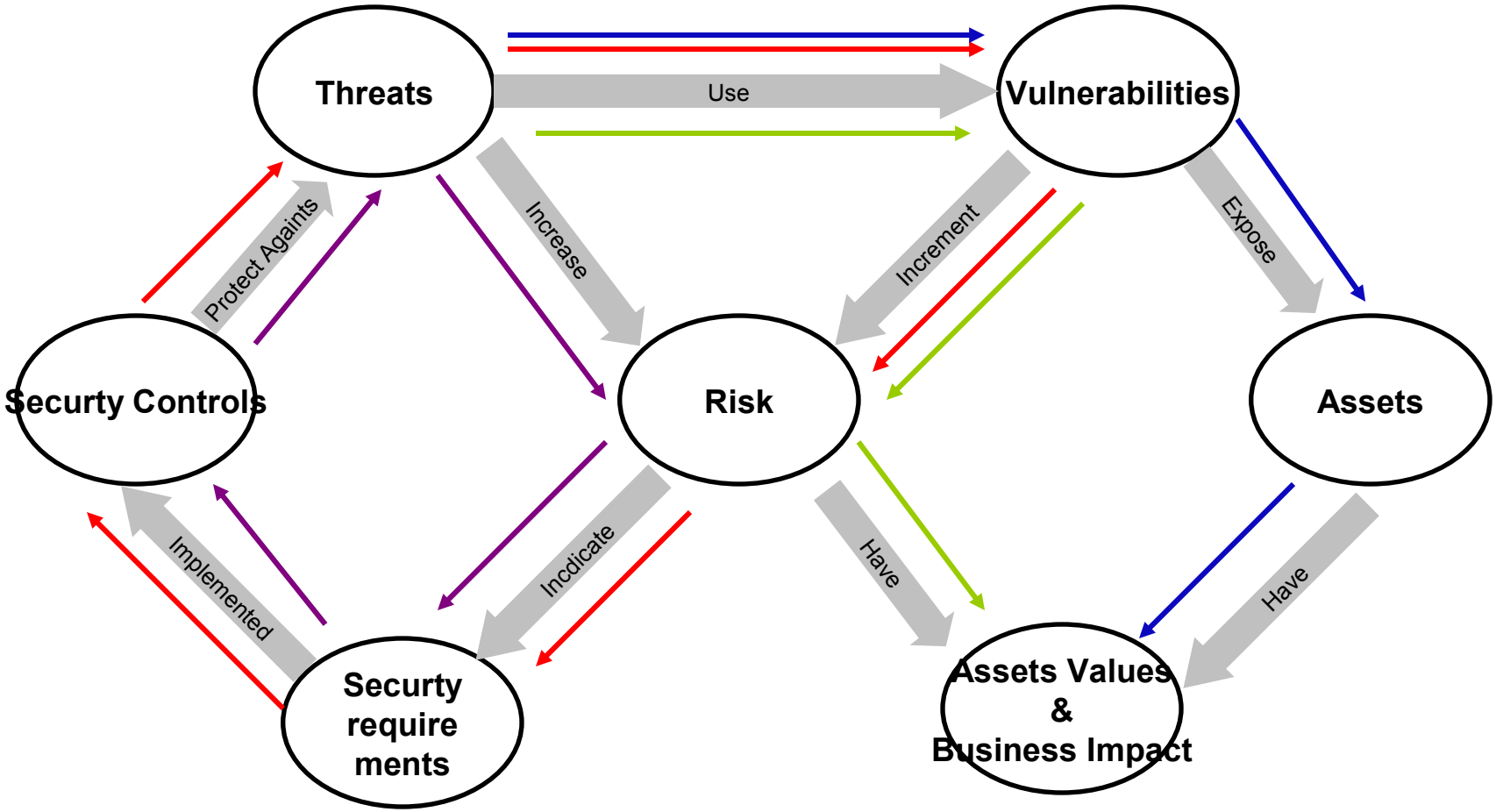


Risk assessment

Impact \ Likelihood	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
VERY LOW	LOW	LOW	LOW	LOW	MEDIUM
LOW	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
MEDIUM	LOW	MEDIUM	HIGH	HIGH	HIGH
HIGH	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
VERY HIGH	MEDIUM	HIGH	HIGH	VERY HIGH	VERY HIGH



Risk life cycle



Select controls

- Select and implement control objectives and controls to meet the requirements identified by the risk assessment and risk treatment process.

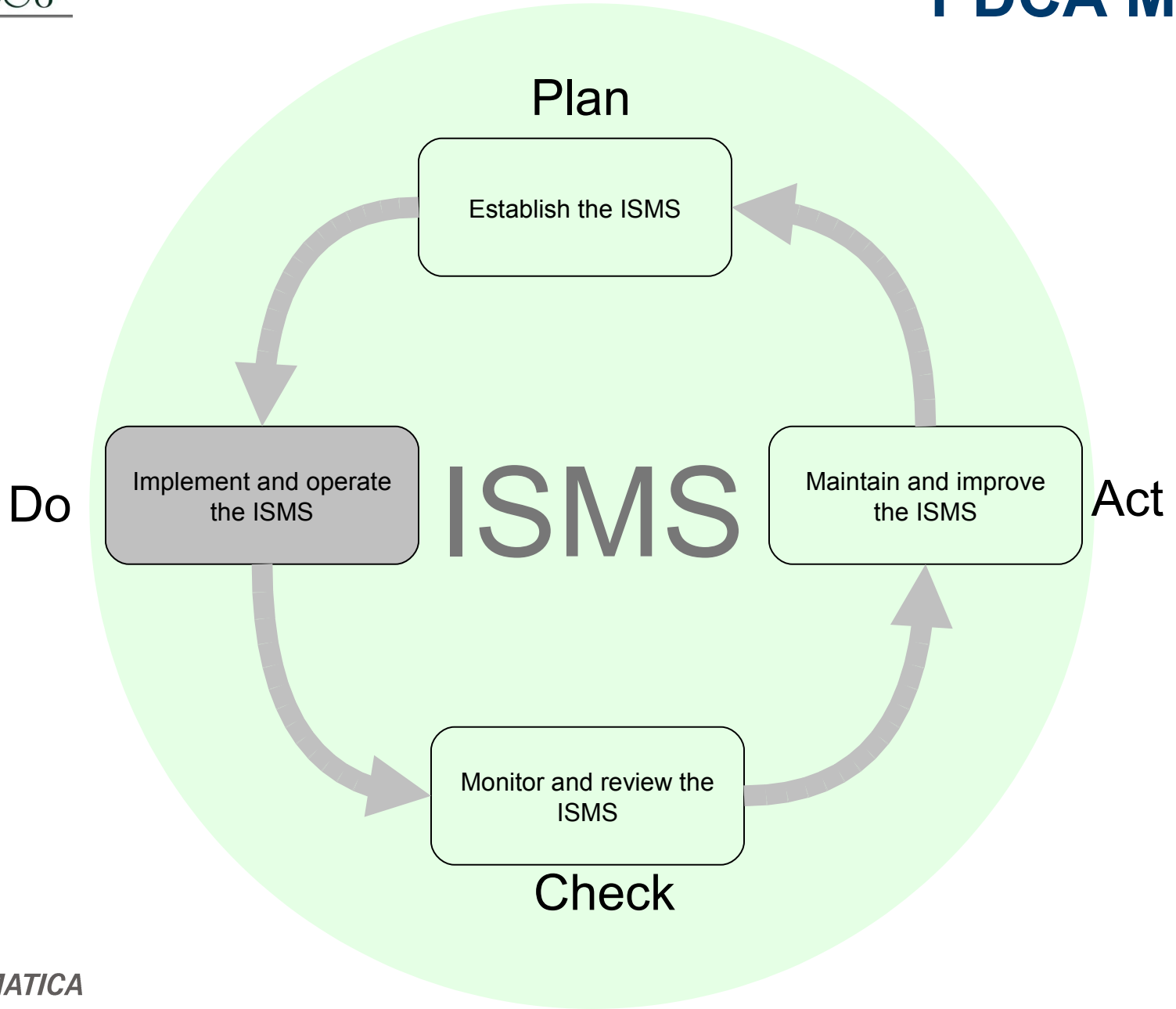
- The selection takes into account the criteria for accepting risks as well as legal, regulatory and contractual requirements.

Statement of applicability

- The statement of applicability includes currently implemented control objectives and controls, and justification for the exclusion of any controls from Annex A.

- Where controls are excluded, their exclusion does not affect the organisation's ability and/or responsibility to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements.

PDCA Model


Plan
Establish the ISMS
Do
Implement and operate the ISMS
ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check

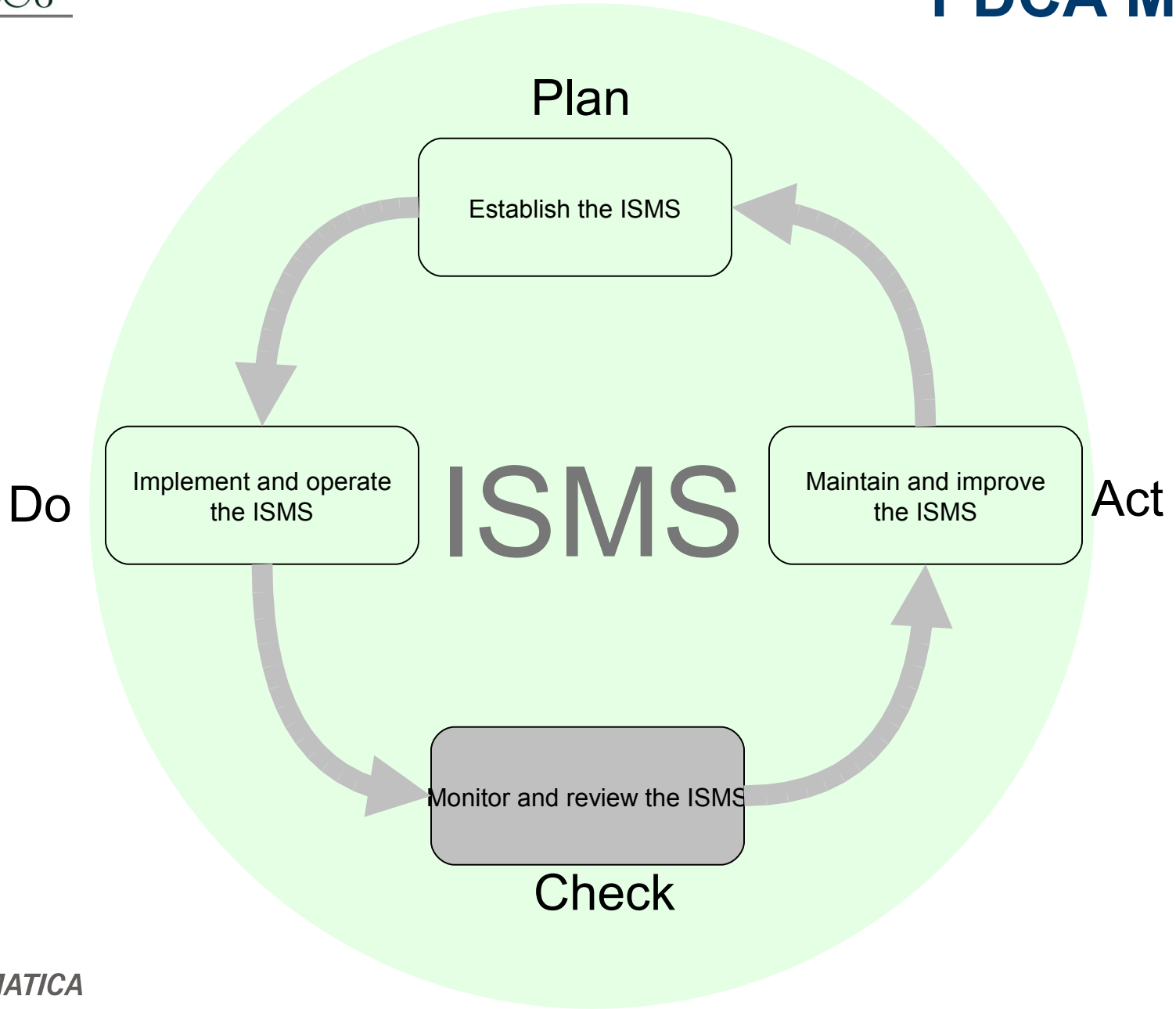
Metrics

- The organization shall have a method of measuring the effectiveness of the selected controls or groups of controls.
- Metrics should be used to assess the effectiveness of the controls to produce comparable and reproducible results.

Implementation

- **The organization shall do the following.**
  - **Implement the risk treatment plan**
  - **Implement controls**
  - **Implement training and awareness programmes**
  - **Manage operation of the ISMS.**
  - **Manage resources for the ISMS**
  - **Implement detection of security events**
  - **Response to security incidents**

PDCA Model


Plan
Establish the ISMS
Do
Implement and operate the ISMS
ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check

Check

- **Monitoring and review procedures and other controls are executed to:**
  - **promptly detect errors in the results processing**
  - **promptly identify attempted and successful security breaches and incidents**
  - **help detect security events and thereby prevent security incidents by the use of indicators**
  - **determine whether the actions taken to resolve a breach of security were effective.**

Check

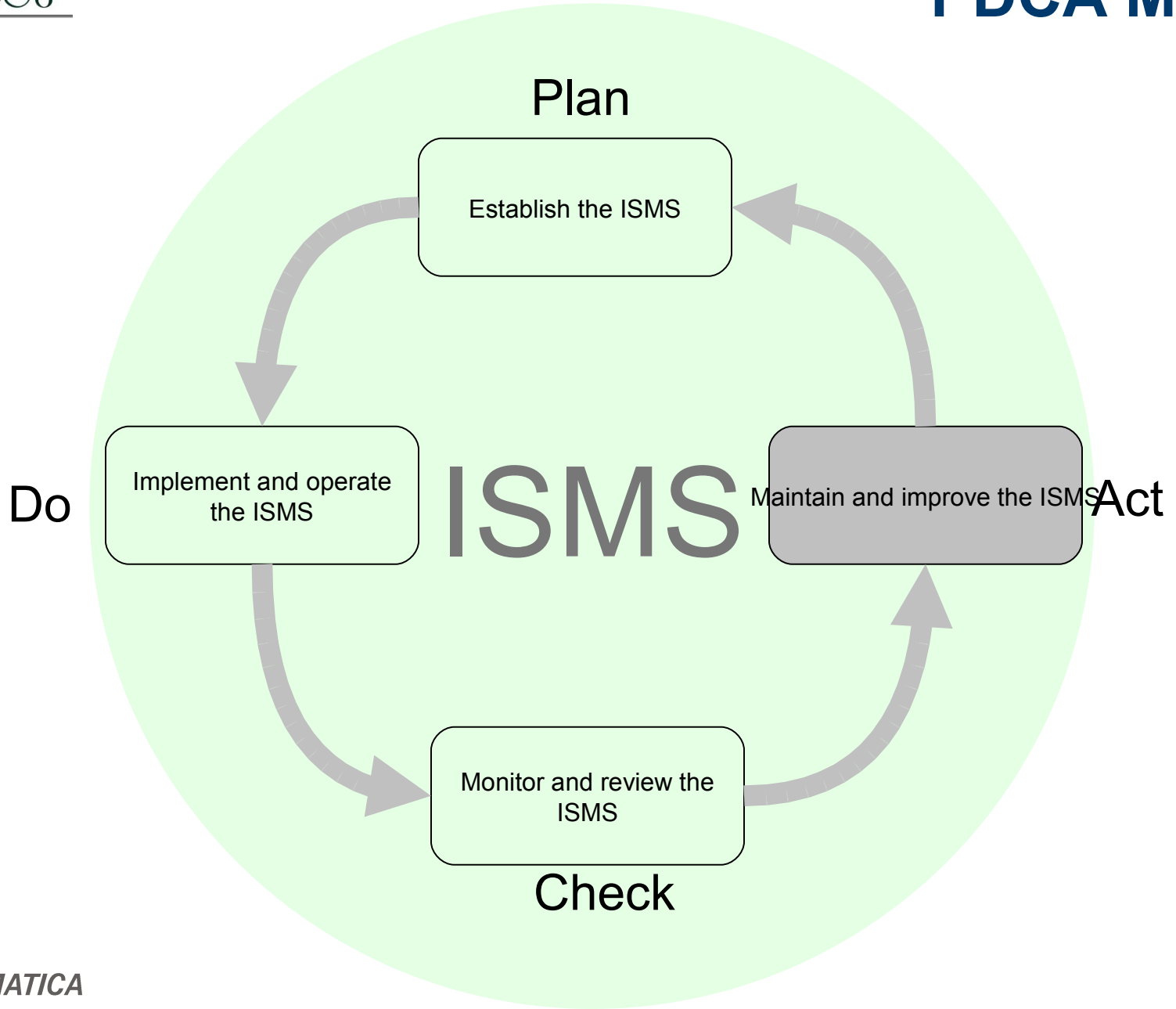
- Regular reviews of the effectiveness of the ISMS are undertaken; including meeting ISMS policy.
- The effectiveness of controls is measured to verify that security requirements have been met.

Check

- **Risk assessments are reviewed at planned intervals and the level of residual risk and identified acceptable risk is reviewed.Reviews take into account the effectiveness of the implemented controls.**

- **Security plans are updated to take into account the findings of monitoring and review activities.**

PDCA Model


Plan
Establish the ISMS
Do
Implement and operate the ISMS
ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check

Act

- Implement the identified improvements in the ISMS.
- Take appropriate corrective and preventive actions
- Actions and improvements are communicated to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed

ISMS Documentation

- Documented statements of the ISMS policy and objectives
- Scope of the ISMS
- Procedures and controls in support of the ISMS
- Description of the risk assessment methodology
- Risk assessment report
- Risk treatment plan
- Procedures needed by the organization to ensure the effective planning, operation and control and describe how to measure the effectiveness of controls
- Records required by ISO 27001
- Statement of Applicability.

Management responsibilities

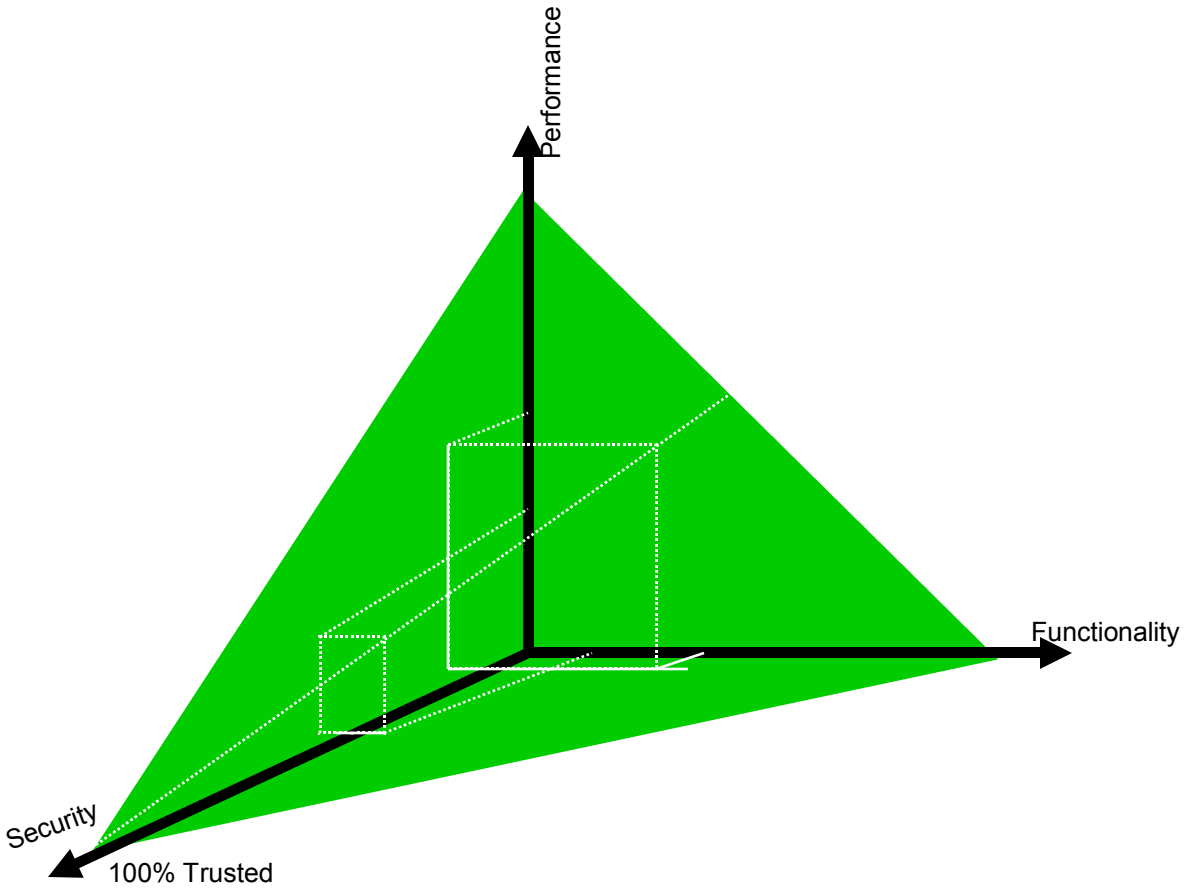
- Establishing an ISMS policy
- Ensuring that ISMS objectives and plans are established
- Establishing roles and responsibilities
- Communicating to the organization the importance of meeting ISMS
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS
- Deciding the criteria for accepting risks and the acceptable levels of risk
- Ensuring that internal ISMS audits are conducted
- Conducting management reviews of the ISMS
- Training, awareness and competence

Internal ISMS audits

- **The organization shall conduct internal ISMS audits at planned intervals (at least once a uear) to determine whether the control objectives, controls, processes and procedures of its ISMS:**
  - **Conform to the requirements of ISO 27001, and relevant legislation or regulations;**
  - **Conform to the identified information security requirements;**
  - **Are effectively implemented and maintained; and**
  - **Perform as expected.**

Implementing the Information Security Management System

Information security views



Strategic responsibilities

- Vision & Mision
- Miantenence to Security Policies
- Revisions, Assessments, Audits
- Risk Analysis
- Vulnerability Analysis
- Risk Management
- BIA
- BCP DRP
- Research and Development
- Market Intelligence

Tactic responsibilities

- Security Services
- Identity, Cryptography, Certificates..
- Certification & Accreditation
- Standards, Guidelines,
- Local Regulations,
- Federal Regulations

Tactic responsibilities

- Information Security on Business Process Definition
- Best Practices
- Information Security Procedures
- Architecture Administration
- Training & Awareness Programs

Tactic responsibilities

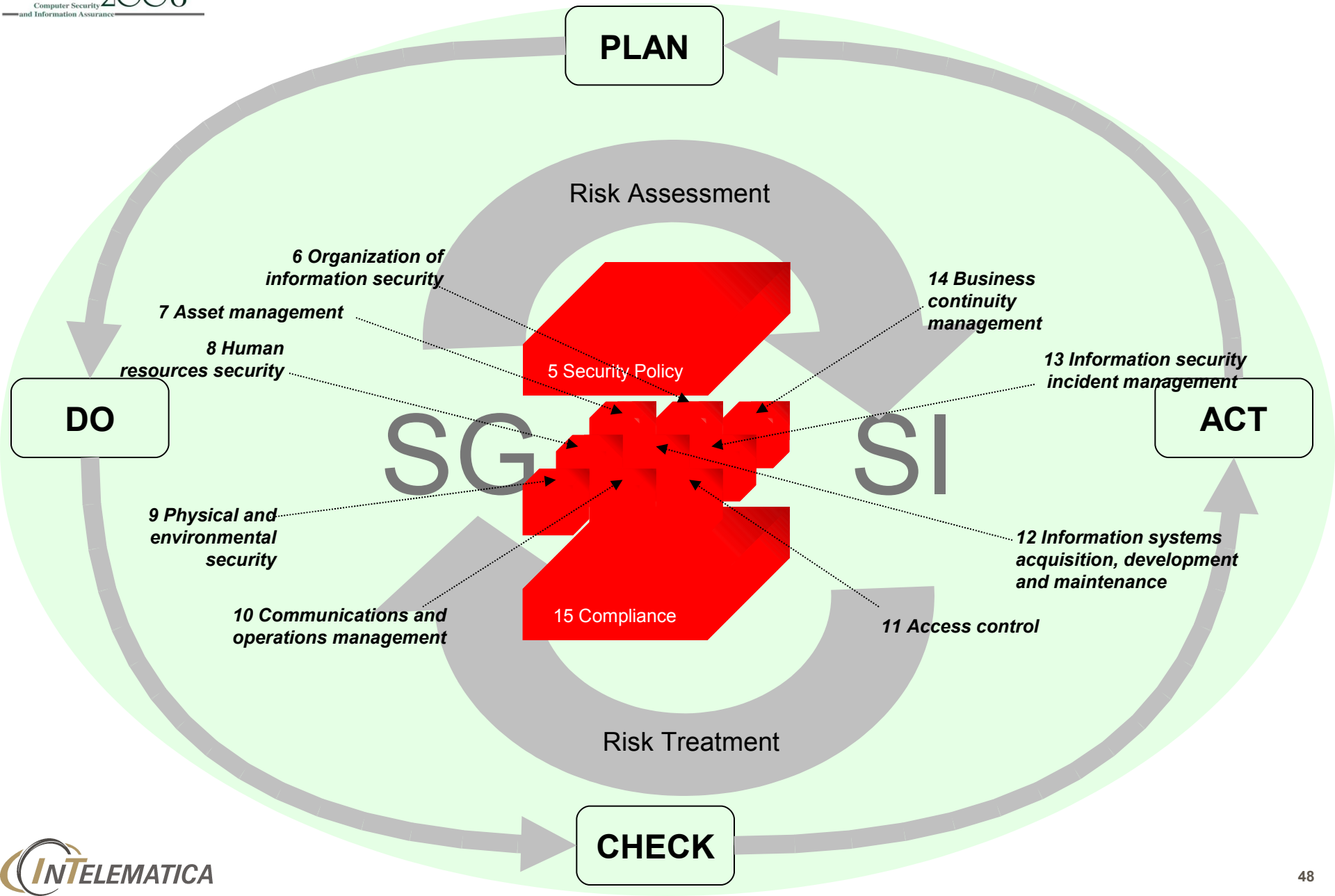
- Monitoring & Metrics
- Incident Response Team
- Forensics
- Information Assets Classification

Operative responsibilities

- 5 Security policy
- 6 Organization of information security
- 7 Asset management
- 8 Human resources security
- 9 Physical and environmental security
- 10 Communications and operations management
- 11 Access control
- 12 Information systems acquisition, development and maintenance
- 13 Information security incident management
- 14 Business continuity management
- 15 Compliance

ISO 27001:2005 controls

ISMS based on ISO 27001.2005



5 Security policy

- 5.1 information security policy
  - 5.1.1 information security policy document
  - 5.1.2 review of the information security policy

6 Organization of information security

- 6.1 internal organization
  - 6.1.1 management commitment to information security
  - 6.1.2 information security co-ordination
  - 6.1.3 allocation of information security responsibilities
  - 6.1.4 authorization process for information processing facilities
  - 6.1.5 confidentiality agreements
  - 6.1.6 contact with authorities
  - 6.1.7 contact with special interest groups
  - 6.1.8 independent review of information security
- 6.2 external parties
  - 6.2.1 identification of risks related to external parties
  - 6.2.2 addressing security when dealing with customers
  - 6.2.3 addressing security in third party agreements

7 Asset manageme

- 7.1 responsibility for assets
  - 7.1.1 inventory of assets
  - 7.1.2 ownership of assets
  - 7.1.3 acceptable use of assets
- 7.2 information classification
  - 7.2.1 classification guidelines
  - 7.2.2 information labeling and handling

8 Human resources security

- 8.1 prior to employment
  - 8.1.1 roles and responsibilities
  - 8.1.2 screening
  - 8.1.3 terms and conditions of employment
- 8.2 during employment
  - 8.2.1 management responsibilities
  - 8.2.2 information security awareness, education, and training
  - 8.2.3 disciplinary process
- 8.3 termination or change of employment
  - 8.3.1 termination responsibilities
  - 8.3.2 return of assets
  - 8.3.3 removal of access rights

9 Physical and environmental security

- 9.1 secure areas
  - 9.1.1 physical security perimeter
  - 9.1.2 physical entry controls
  - 9.1.3 securing offices, rooms, and facilities
  - 9.1.4 protecting against external and environmental threats
  - 9.1.5 working in secure areas
  - 9.1.6 public access, delivery, and loading areas
- 9.2 equipment security
  - 9.2.1 equipment siting and protection
  - 9.2.2 supporting utilities
  - 9.2.3 cabling security
  - 9.2.4 equipment maintenance
  - 9.2.5 security of equipment off-premises
  - 9.2.6 secure disposal or re-use of equipment
  - 9.2.7 removal of property

10 Communications and operations management

- 10.1 operational procedures and responsibilities
  - 10.1.1 documented operating procedures
  - 10.1.2 change management
  - 10.1.3 segregation of duties
  - 10.1.4 separation of development, test, and operational facilities
- 10.2 third party service delivery management
  - 10.2.1 service delivery
  - 10.2.2 monitoring and review of third party services
  - 10.2.3 managing changes to third party services
- 10.3 system planning and acceptance
  - 10.3.1 capacity management
  - 10.3.2 system acceptance
- 10.4 protection against malicious and mobile code
  - 10.4.1 controls against malicious code
  - 10.4.2 controls against mobile code

10 Communications and operations management

- 10.5 back-up
  - 10.5.1 information back-up
- 10.6 network security management
  - 10.6.1 network con 45
  - 10.6.2 security of network services
- 10.7 media handling
  - 10.7.1 management of removable media
  - 10.7.2 disposal of media
  - 10.7.3 information handling procedures
  - 10.7.4 security of system documentation
- 10.8 exchange of information
  - 10.8.1 information exchange policies and procedures
  - 10.8.2 exchange agreements
  - 10.8.3 physical media in transit
  - 10.8.4 electronic messaging
  - 10.8.5 business information systems

10 Communications and operations management

- 10.9 electronic commerce services
  - 10.9.1 electronic commerce
  - 10.9.2 on-line transactions
  - 10.9.3 publicly available information
- 10.10 monitoring
  - 10.10.1 audit logging
  - 10.10.2 monitoring system use
  - 10.10.3 protection of log information
  - 10.10.4 administrator and operator logs
  - 10.10.5 fault logging
  - 10.10.6 clock synchronization

11 Access control

- 11.1 business requirement for access control
  - 11.1.1 access control policy
- 11.2 user access management
  - 11.2.1 user registration
  - 11.2.2 privilege management
  - 11.2.3 user password management
  - 11.2.4 review of user access rights
- 11.3 user responsibilities
  - 11.3.1 password use
    - 11.3.2 unattended user equipment
  - 11.3.3 clear desk and clear screen policy
- 11.4 network access control
  - 11.4.1 policy on use of network services
  - 11.4.2 user authentication for external connections
  - 11.4.3 equipment identification in networks
  - 11.4.4 remote diagnostic and configuration port protection
  - 11.4.5 segregation in networks
  - 11.4.6 network connection control
  - 11.4.7 network routing control

11 Access control

- 11.5 operating system access control
  - 11.5.1 secure log-on procedures
  - 11.5.2 user identification and authentication
  - 11.5.3 password management system
  - 11.5.4 use of system utilities
  - 11.5.5 session time-out
  - 11.5.6 limitation of connection time
- 11.6 application and information access control
  - 11.6.1 information access restriction
  - 11.6.2 sensitive system isolation
- 11.7 mobile computing and teleworking
  - 11.7.1 mobile computing and communications
  - 11.7.2 teleworking

12 Information systems acquisition, development and maintenance

- 12.1 security requirements of information systems
  - 12.1.1 security requirements analysis and specification
- 12.2 correct processing in applications
  - 12.2.1 input data validation
  - 12.2.2 control of internal processing
  - 12.2.3 message integrity
  - 12.2.4 output data validation
- 12.3 cryptographic controls
  - 12.3.1 policy on the use of cryptographic controls
  - 12.3.2 key management
- 12.4 security of system files
  - 12.4.1 control of operational software
  - 12.4.2 protection of system test data
  - 12.4.3 access control to program source code
- 12.5 security in development and support processes
  - 12.5.1 change control procedures
  - 12.5.2 technical review of applications after operating system changes
  - 12.5.3 restrictions on changes to software packages
  - 12.5.4 information leakage
  - 12.5.5 outsourced software development
- 12.6 technical vulnerability management
  - 12.6.1 control of technical vulnerabilities

13 Information security incident management

- 13.1 reporting information security events and weaknesses
  - 13.1.1 reporting information security events
  - 13.1.2 reporting security weaknesses
- 13.2 management of information security incidents and improvements
  - 13.2.1 responsibilities and procedures
  - 13.2.2 learning from information security incidents
  - 13.2.3 collection of evidence

14 Business continuity management

- 14.1 information security aspects of business continuity management
  - 14.1.1 including information security in the business continuity management process
  - 14.1.2 business continuity and risk assessment
  - 14.1.3 developing and implementing continuity plans including information security
  - 14.1.4 business continuity planning framework
  - 14.1.5 testing, maintaining and re-assessing business continuity plans

15 Compliance

- 15.1 compliance with legal requirements
  - 15.1.1 identification of applicable legislation
  - 15.1.2 intellectual property rights (ipr)
  - 15.1.3 protection of organizational records
  - 15.1.4 data protection and privacy of personal information
  - 15.1.5 prevention of misuse of information processing facilities
  - 15.1.6 regulation of cryptographic controls
- 15.2 compliance with security policies and standards, and technical compliance
  - 15.2.1 compliance with security policies and standards
  - 15.2.2 technical compliance checking
  - 15.3 information systems audit considerations
  - 15.3.1 information systems audit controls
  - 15.3.2 protection of information systems audit tools

NEbraska CERT Conference 2006
Computer Security and Information Assurance

The Information Security Management Process based on ISO 27001

Ing. Leonardo García Rojas

CISSP, CISM, CISA, ISO9000LA, ISMS IRCA LA, BS7799LA, PMP

leonardo_garciar@yahoo.com

lgarcia@intelematica.com.mx