NEbraska CERT Conference 2004

Computer Security and Information Assurance

BS7799: from initial review to certification

Ing. Leonardo García Rojas
CISSP, CISM

NEbraska CERT Conference 2004

Computer Security and Information Assurance

What is Data, 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.”

ISO/IEC 17799:2000

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

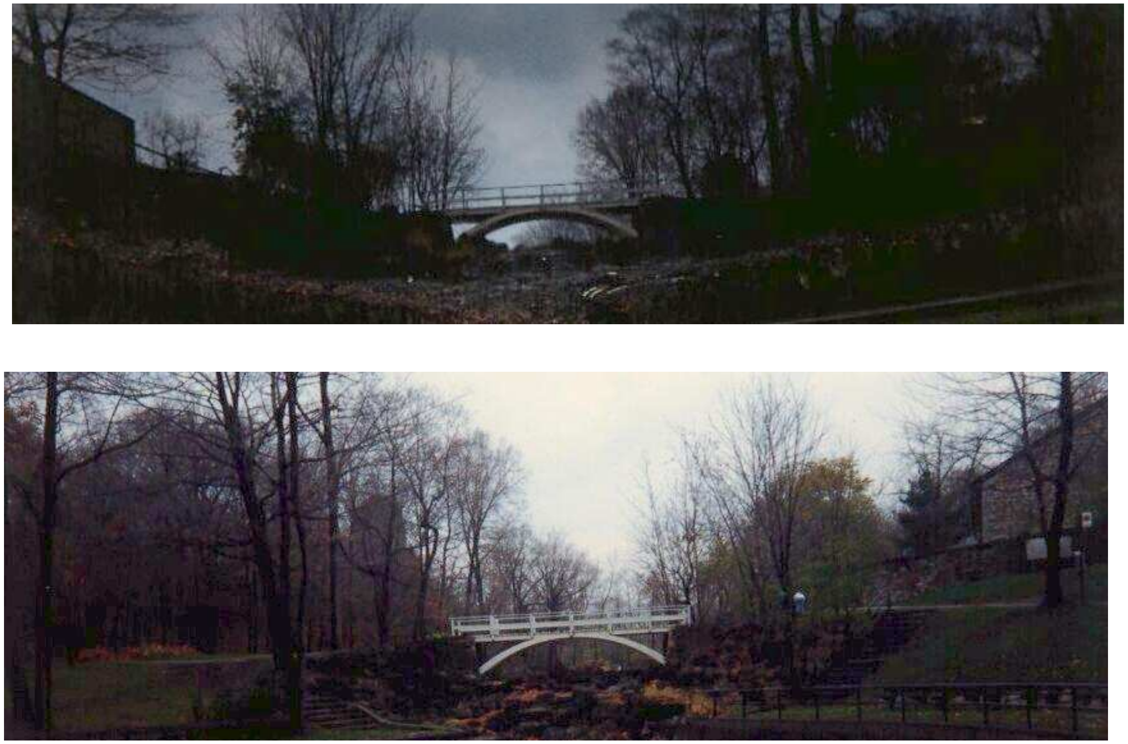
Types of information

- Data ready to guess decisions
  - Printed or written on paper
  - Stored electronically
  - Transmitted by regular mail or electronic mail
  - Corporate videos
  - Spoken in conversations

What is the diference between data and information?

MONTREAL, CANADA, NOV. 6, 1994

Data or Information ?



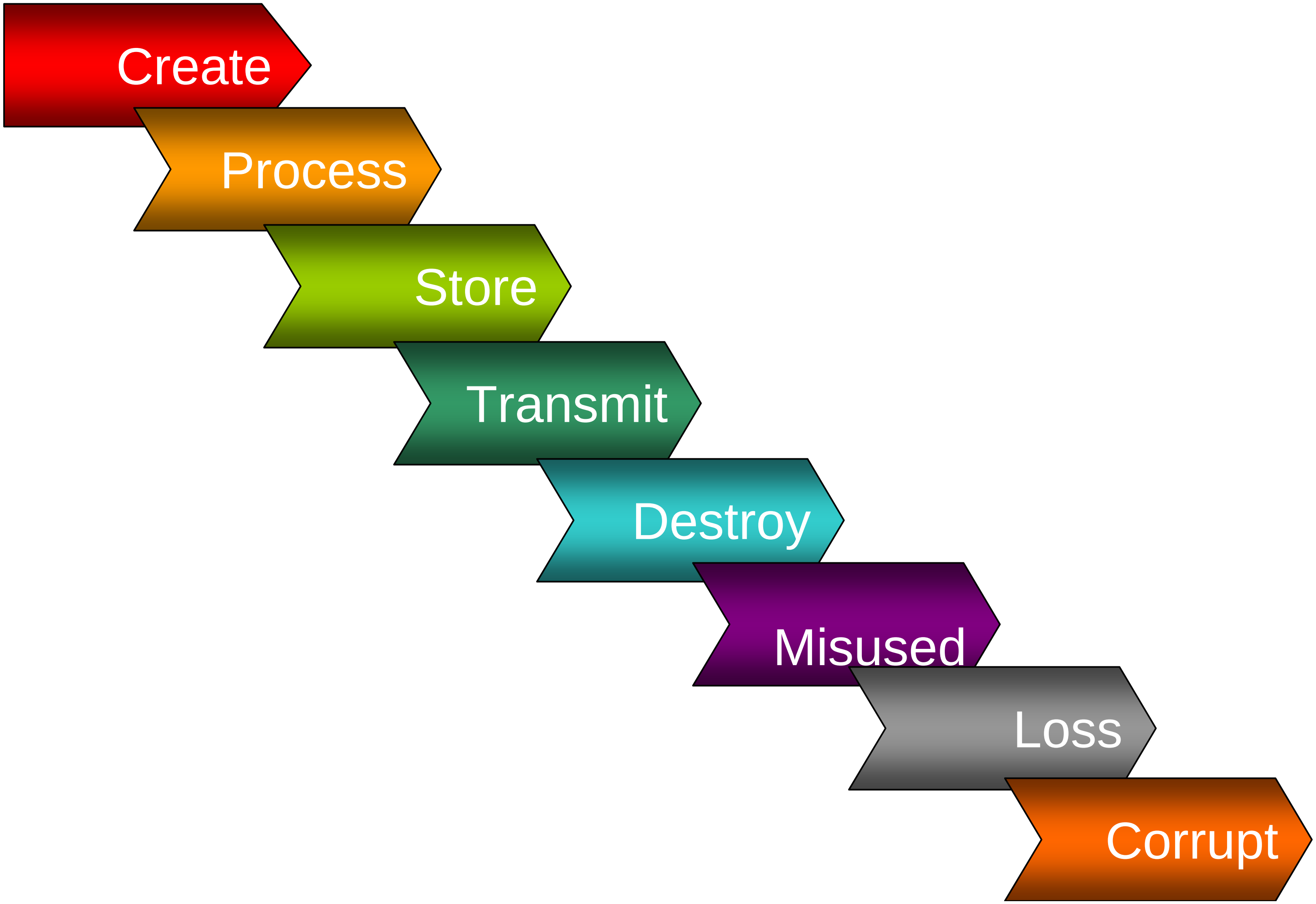
SAINT ELENE ISLAND, MONTREAL, CANADA, NOV. 6, 1994

Data or Information ?

NEbraska CERT Conference 2004
Computer Security and Information Assurance

Data or Information ?

Information life cycle



Create

Process

Store

Transmit

Destroy

Misused

Loss

Corrupt

Threats to Information

- **Examples**
  - **Employees**
  - **Low awareness of security issues**
  - **Growth in networking and distributed computing**
  - **Growth in complexity and effectiveness of hacking tools and viruses**
  - **E-Mail**
  - **Fire, flood, earthquake**

What is Information Security

- **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**

ISO/IEC 17799:2000

Achieving Information Security

- Implementing a set of controls
  - Policies
  - Practices
  - Procedures
  - Organizational structures
  - Software functions

- Controls are selected based on a Risk Assessment

NEbraska CERT Conference 2004

Computer Security and Information Assurance

What is an Information Security Management System?

ISMS

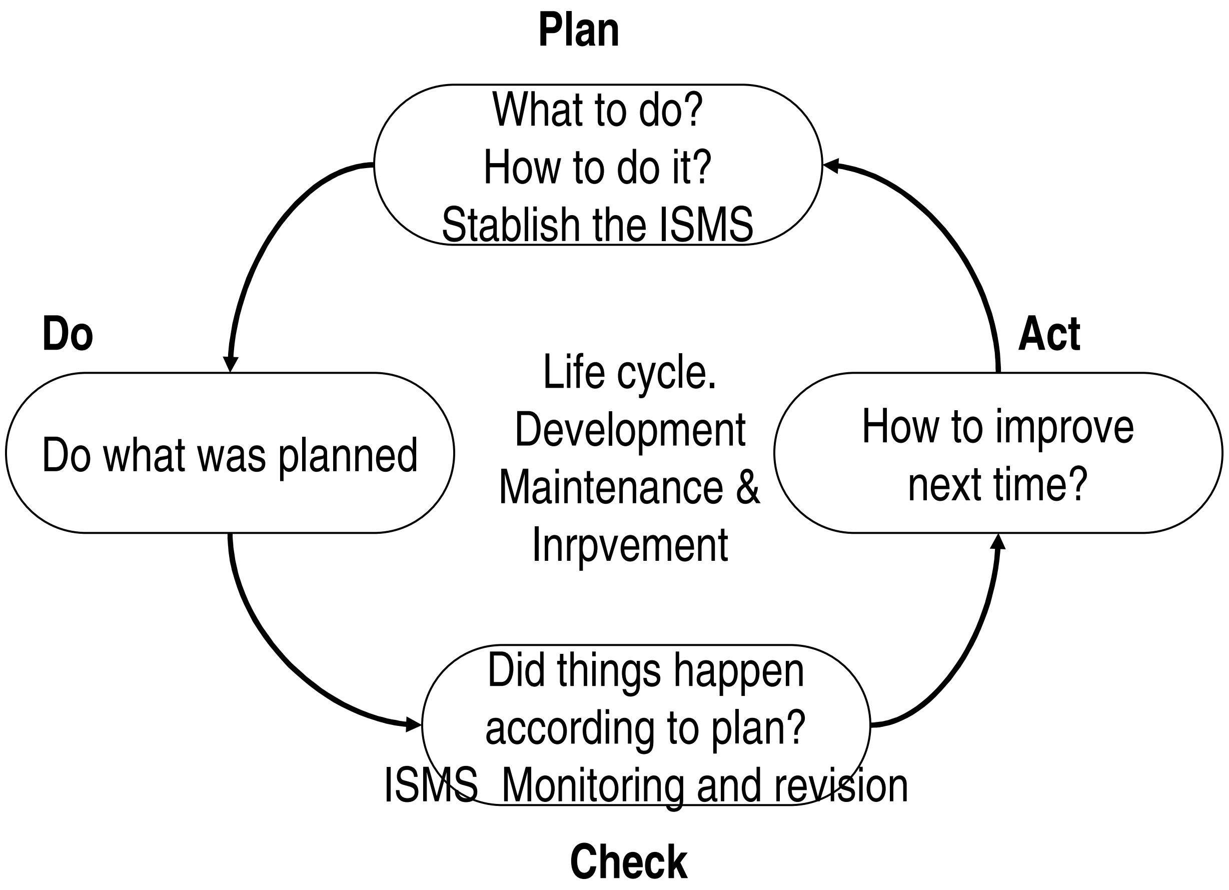
- A management system is a system to establish policy and objectives and to achieve those objectives.

- Management systems are used by organizations to develop their policies and to put these into effect via objectives and targets using:
  - Organizational structure
  - Systematic 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

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

PDCA applied to an ISMS process



Plan

What to do?
How to do it?
Stablish the ISMS

Do

Do what was planned

Life cycle.
Development
Maintenance &
Inrpvement

Act

How to improve
next time?

Did things happen
according to plan?
ISMS Monitoring and revision

Check

Information Security Management System

- ISMS
  - That part of the overall management system, based on a business risk assessment approach, to establish, implement, operate, monitor, review, maintain and improve information security

NEbraska CERT Conference 2004

Computer Security and Information Assurance

Information Security Management System

Information Security Management

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

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
- Related to the five-part "Guidelines for the Management of IT Security," or GMITS/ISO TR 13335

Integrated Approach

- **ISO 17799 defines best practices for information security management**

- **A management system should balance physical, technical, procedural, and personnel security**

- **Without a formal Information Security Management System, such as a BS 7799-2 based system, there is a greater risk to your security being breached**

- **Information security is a management process, not a technological process**

NEbraska CERT Conference 2004
Computer Security
and Information Assurance

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.”**

ISO/IEC 17799:2000

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

*** Ernst and Young "Information Security Survey 2002"**

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

*** Ernst and Young "Information Security Survey 2002"**

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

*** Ernst and Young "Information Security Survey 2002"**

Main Information Security Issues*

- *Business continuity plans exist at 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

*** Ernst and Young "Information Security Survey 2002"**

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

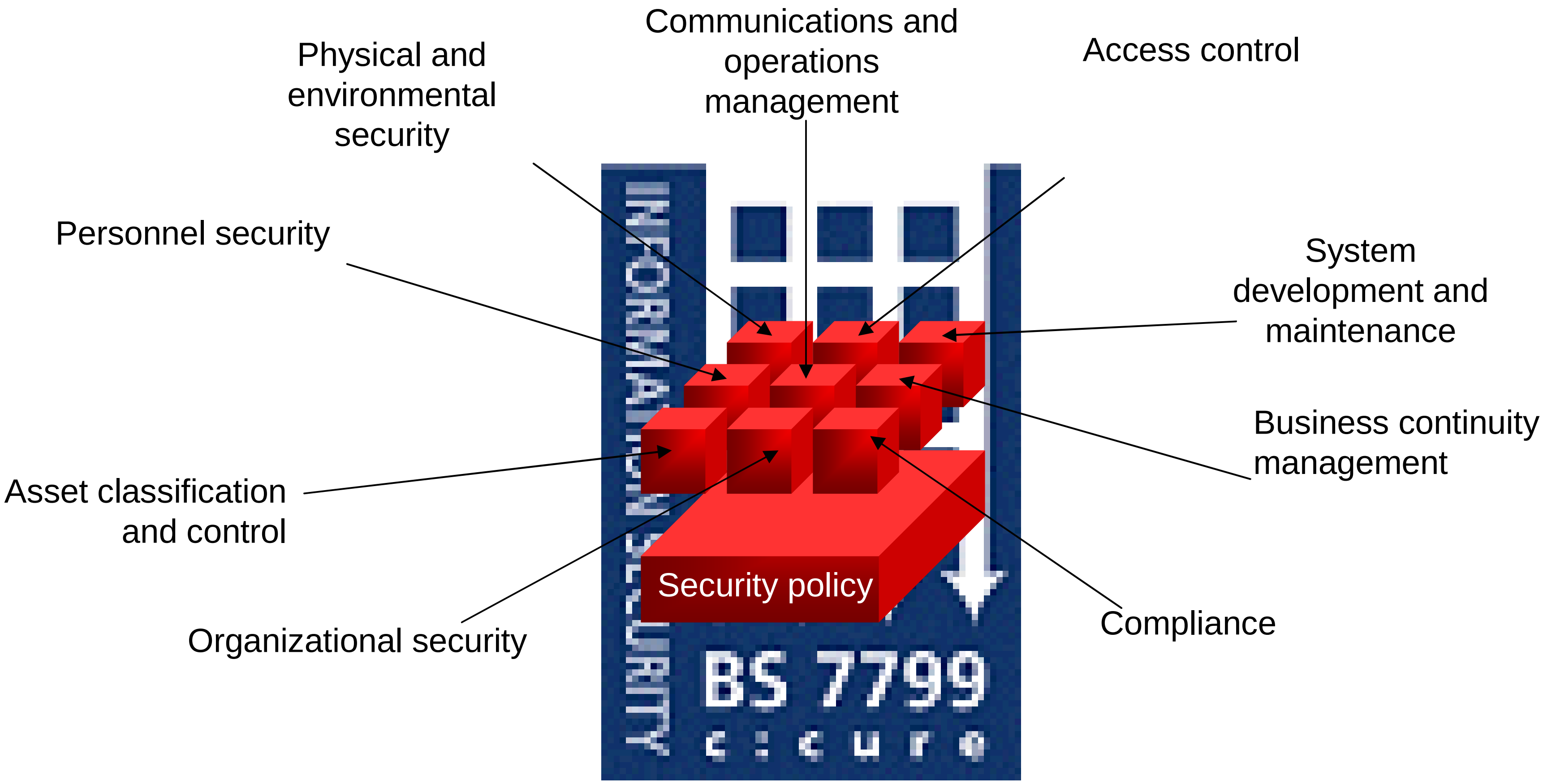
*** Ernst and Young "Information Security Survey 2002"**

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

*** Ernst and Young "Information Security Survey 2002"**

BS7799 & ISO 17799



Physical and environmental security

Communications and operations management

Access control

Personnel security

System development and maintenance

Business continuity management

Asset classification and control

Security policy

Organizational security

Compliance

A.3 Security policy

- A.3.1 Information security policy
  - A.3.1.1 Information security policy document
  - A.3.1.2 Review and evaluation

A.4 Organizational security

- A.4.1 Information security infrastructure
  - A.4.1.1 Management information security forum
  - A.4.1.2 Information security coordination
  - A.4.1.3 Allocation of information security responsibilities
  - A.4.1.4 Authorization process for information processing facilities
  - A.4.1.5 Specialist information security advice
  - A.4.1.6 Cooperation between organizations
  - A.4.1.7 Independent review of information security

A.4 Organizational security

- A.4.2 Security of third-party access
  - A.4.2.1 Identification of risks from third-party access
  - A.4.2.2 Security requirements in third-party contracts

- A.4.3 Outsourcing
  - A.4.3.1 Security requirements in outsourcing contracts

A.5 Asset classification and control

- A.5.1 Accountability for assets
  - A.5.1.1 Inventory of assets

- A.5.2 Information classification
  - A.5.2.1 Classification guidelines
  - A.5.2.2 Information labelling and handling

A.6 Personnel security

- A.6.1 Security in job definition and resourcing
  - A.6.1.1 Including security in job responsibilities
  - A.6.1.2 Personnel screening and policy
  - A.6.1.3 Confidentiality agreements
  - A.6.1.4 Terms and conditions of employmen
- A.6.2 User training
  - A.6.2.1 Information security education and training

A.6 Personnel security

- A.6.3 Responding to security incidents and malfunctions
  - A.6.3.1 Reporting security incidents
  - A.6.3.2 Reporting security weaknesses
  - A.6.3.3 Reporting software malfunctions
  - A.6.3.4 Learning from incidents
  - A.6.3.5 Disciplinary process

A.7 Physical and environmental security

- A.7.1 Secure areas
  - A.7.1.1 Physical security perimeter
  - A.7.1.2 Physical entry controls
  - A.7.1.3 Securing offices, rooms and facilities
  - A.7.1.4 Working in secure areas
  - A.7.1.5 Isolated delivery and loading areas

A.7 Physical and environmental security

- A.7.2 Equipment security
  - A.7.2.1 Equipment siting and protection
  - A.7.2.2 Power supplies
  - A.7.2.3 Cabling security
  - A.7.2.4 Equipment maintenance
  - A.7.2.5 Security of equipment off-premises
  - A.7.2.6 Secure disposal or re-use of equipment

- A.7.3 General controls
  - A.7.3.1 Clear desk and clear screen policy
  - A.7.3.2 Removal of property

A.8 Communications and operations management

- A.8.1 Operational procedures and responsibilities
  - A.8.1.1 Documented operating procedures
  - A.8.1.2 Operational change controls
  - A.8.1.3 Incident management procedures
  - A.8.1.4 Segregation of duties
  - A.8.1.5 Separation of development and operational facilities
  - A.8.1.6 External facilities management

NEbraska CERT Conference 2004
Computer Security and Information Assurance

A.8 Communications and operations management

- A.8.2 System planning and acceptance
  - A.8.2.1 Capacity planning
  - A.8.2.2 System acceptance
- A.8.3 Protection against malicious software
  - A.8.3.1 Controls against malicious software
- A.8.4 Housekeeping
  - A.8.4.1 Information back-up
  - A.8.4.2 Operator logs
  - A.8.4.3 Fault logging
- A.8.5 Network management
  - A.8.5.1 Network controls

A.8 Communications and operations management

- A.8.6 Media handling and security
  - A.8.6.1 Management of removable computer media
  - A.8.6.2 Disposal of media
  - A.8.6.3 Information handling procedures
  - A.8.6.4 Security of system documentation
- A.8.7 Exchanges of information and software
  - A.8.7.1 Information and software exchange agreements
  - A.8.7.2 Security of media in transit
  - A.8.7.3 Electronic commerce security
  - A.8.7.4 Security of electronic mail
  - A.8.7.5 Security of electronic office systems
  - A.8.7.6 Publicly available systems
  - A.8.7.7 Other forms of information exchange

A.9 Access control

- A.9.1 Business requirement for access control
  - A.9.1.1 Access control policy
- A.9.2 User access management
  - A.9.2.1 User registration
  - A.9.2.2 Privilege management
  - A.9.2.3 User password management
  - A.9.2.4 Review of user access rights
- A.9.3 User responsibilities
  - A.9.3.1 Password use
  - A.9.3.2 Unattended user equipment

A.9 Access control

- A.9.4 Network access control
  - A.9.4.1 Policy on use of network services
  - A.9.4.2 Enforced path
  - A.9.4.3 User authentication for external connections
  - A.9.4.4 Node authentication
  - A.9.4.5 Remote diagnostic port protection
  - A.9.4.6 Segregation in networks
  - A.9.4.7 Network connection control
  - A.9.4.8 Network routeing control
  - A.9.4.9 Security of network services

A.9 Access control

- A.9.5 Operating system access control
  - A.9.5.1 Automatic terminal identification
  - A.9.5.2 Terminal log-on procedures
  - A.9.5.3 User identification and authentication
  - A.9.5.4 Password management system
  - A.9.5.5 Use of system utilities
  - A.9.5.6 Duress alarm to safeguard users
  - A.9.5.7 Terminal time-out
  - A.9.5.8 Limitation of connection time

A.9 Access control

- A.9.6 Application access control
  - A.9.6.1 Information access restriction
  - A.9.6.2 Sensitive system isolation
- A.9.7 Monitoring system access and use
  - A.9.7.1 Event logging
  - A.9.7.2 Monitoring system use
  - A.9.7.3 Clock synchronization
- A.9.8 Mobile computing and teleworking
  - A.9.8.1 Mobile computing
  - A.9.8.2 Teleworking

A.10 System development and maintenance

- A.10.1 Security requirements of systems
  - A.10.1.1 Security requirements
- A.10.2 Security in application systems
  - A.10.2.1 Input data validation
  - A.10.2.2 Control of internal processing
  - A.10.2.3 Message authentication
  - A.10.2.4 Output data validation

NEbraska CERT Conference 2004
Computer Security and Information Assurance

A.10 System development and maintenance

- A.10.3 Cryptographic controls
  - A.10.3.1 Policy on the use of cryptographic controls
  - A.10.3.2 Encryption
  - A.10.3.3 Digital signatures
  - A.10.3.4 Non-repudiation services
  - A.10.3.5 Key management
- A.10.4 Security of system files
  - A.10.4.1 Control of operational software
  - A.10.4.2 Protection of system test data
  - A.10.4.3 Access control to program source library

A.10 System development and maintenance

- A.10.5 Security in development and support processes
  - A.10.5.1 Change control procedures
  - A.10.5.2 Technical review of operating system changes
  - A.10.5.3 Restrictions on changes to software packages
  - A.10.5.4 Covert channels and Trojan code
  - A.10.5.5 Outsourced software development

A.11 Business continuity management

- A.11.1 Aspects of business continuity management
  - A.11.1.1 Business continuity management process
  - A.11.1.2 Business continuity and impact analysis
  - A.11.1.3 Writing and implementing continuity plans
  - A.11.1.4 Business continuity planning framework
  - A.11.1.5 Testing, maintaining and re-assessing business continuity plans

A.12 Compliance

- A.12.1 Compliance with legal requirements
  - A.12.1.1 Identification of applicable legislation
  - A.12.1.2 Intellectual property rights (IPR)
  - A.12.1.3 Safeguarding of organizational records
  - A.12.1.4 Data protection and privacy of personal information
  - A.12.1.5 Prevention of misuse of information processing facilities
  - A.12.1.6 Regulation of cryptographic controls
  - A.12.1.7 Collection of evidence

A.12 Compliance

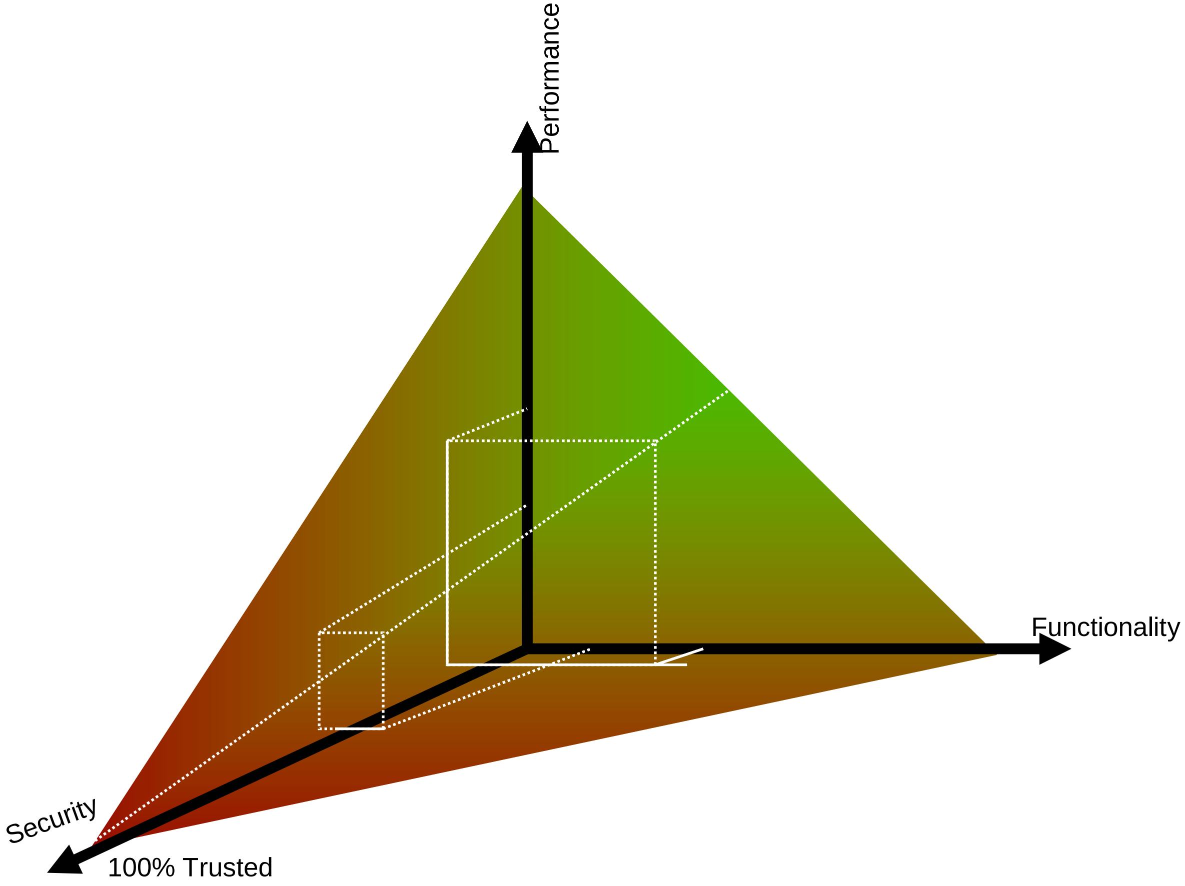
- A.12.2 Reviews of security policy and technical compliance
  - A.12.2.1 Compliance with security policy
  - A.12.2.2 Technical compliance checking
- A.12.3 System audit considerations
  - A.12.3.1 System audit controls
  - A.12.3.2 Protection of system audit tools

NEbraska CERT Conference 2004

Computer Security
and Information Assurance

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

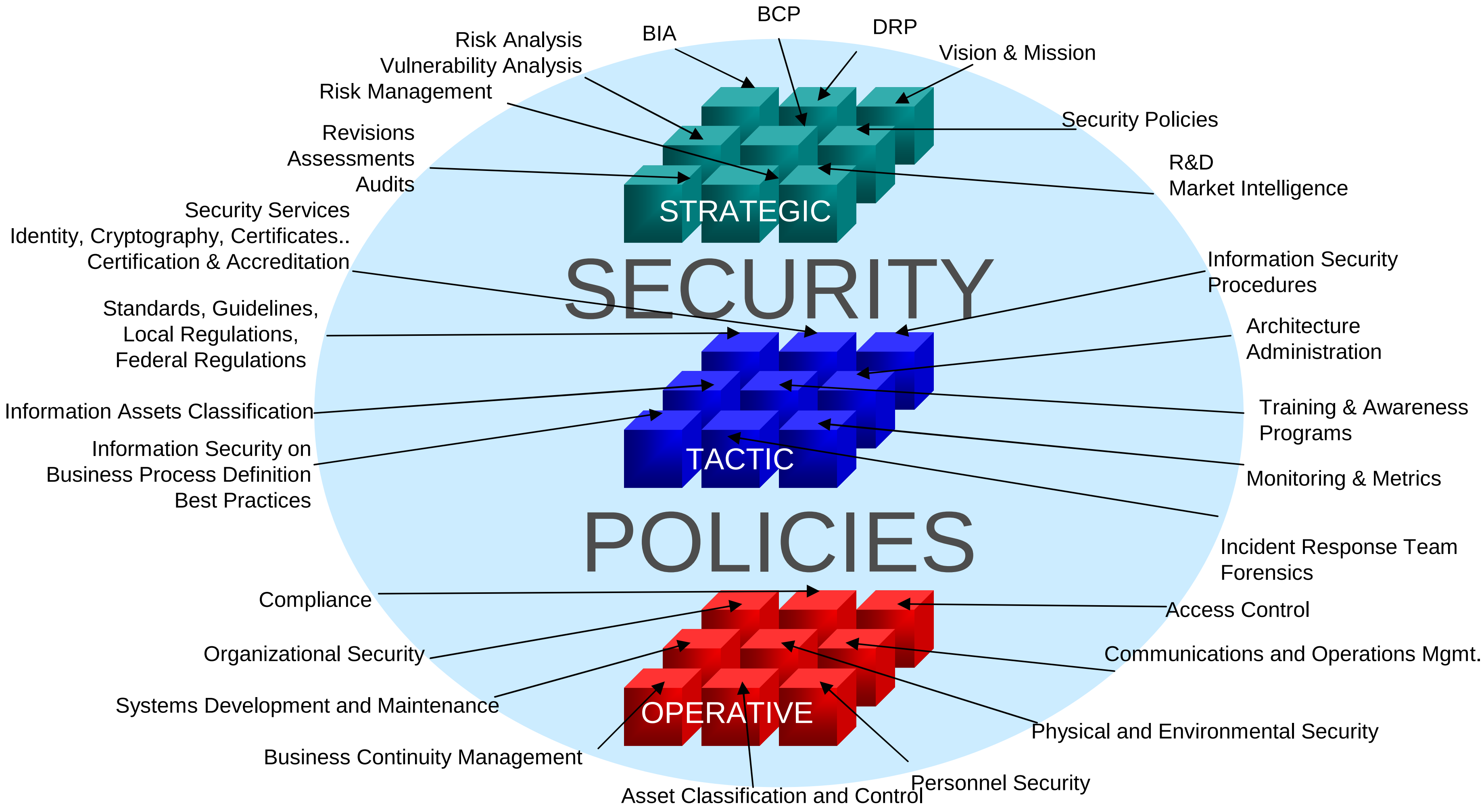
Tactic responsibilities

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

Operative responsibilities

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

Roles & responsibilities



SECURITY

POLICIES

STRATEGIC

BIA

BCP

DRP

Vision & Mission

Risk Analysis
Vulnerability Analysis
Risk Management

Revisions
Assessments
Audits

Security Policies

R&D
Market Intelligence

TACTIC

Security Services
Identity, Cryptography, Certificates..
Certification & Accreditation

Standards, Guidelines,
Local Regulations,
Federal Regulations

Information Assets Classification

Information Security on
Business Process Definition
Best Practices

Information Security
Procedures

Architecture
Administration

Training & Awareness
Programs

Monitoring & Metrics

Incident Response Team
Forensics

OPERATIVE

Compliance

Organizational Security

Systems Development and Maintenance

Business Continuity Management

Asset Classification and Control

Personnel Security

Physical and Environmental Security

Communications and Operations Mgmt.

Access Control

INFORMATION on the information assets

End Users
Vendors
Third Parties

Business Process on Regions or Third Parties

Public Networks

Business Process on the main facilities

Business Process TI support

Business Process Legal Framework

Business Process Personal (End Users, Partners, personal on regions, personnel on other offices)

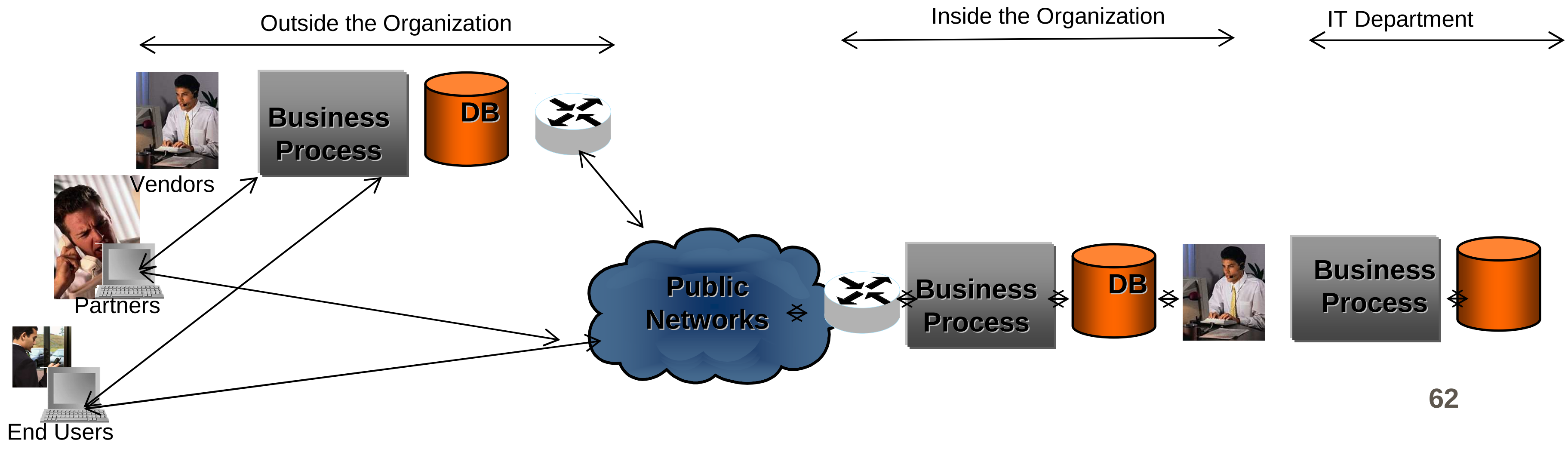
Business Process Data

Business Process Infrastructure Software (Programs, DB Schema)

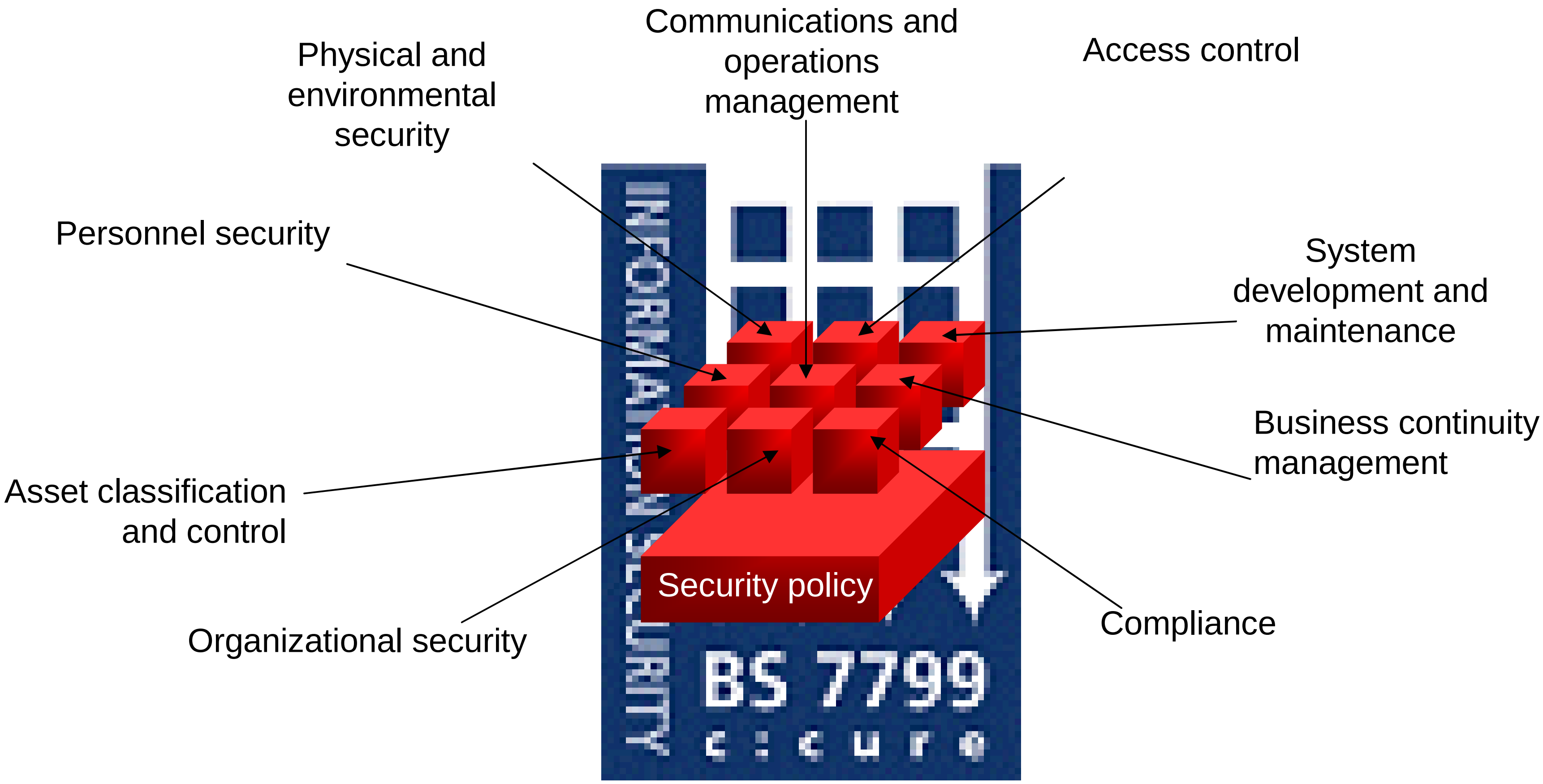
Software Infrastructure (RDBMS, Web Servers, Compilers, APIs, DNS, Mail)

Computing & Telecommunications Hardware

Support Infrastructure (UPSs, Facilities, Racks. HVAC,)



BS7799 & ISO 17799



Communications and operations management

Physical and environmental security

Access control

Personnel security

System development and maintenance

Business continuity management

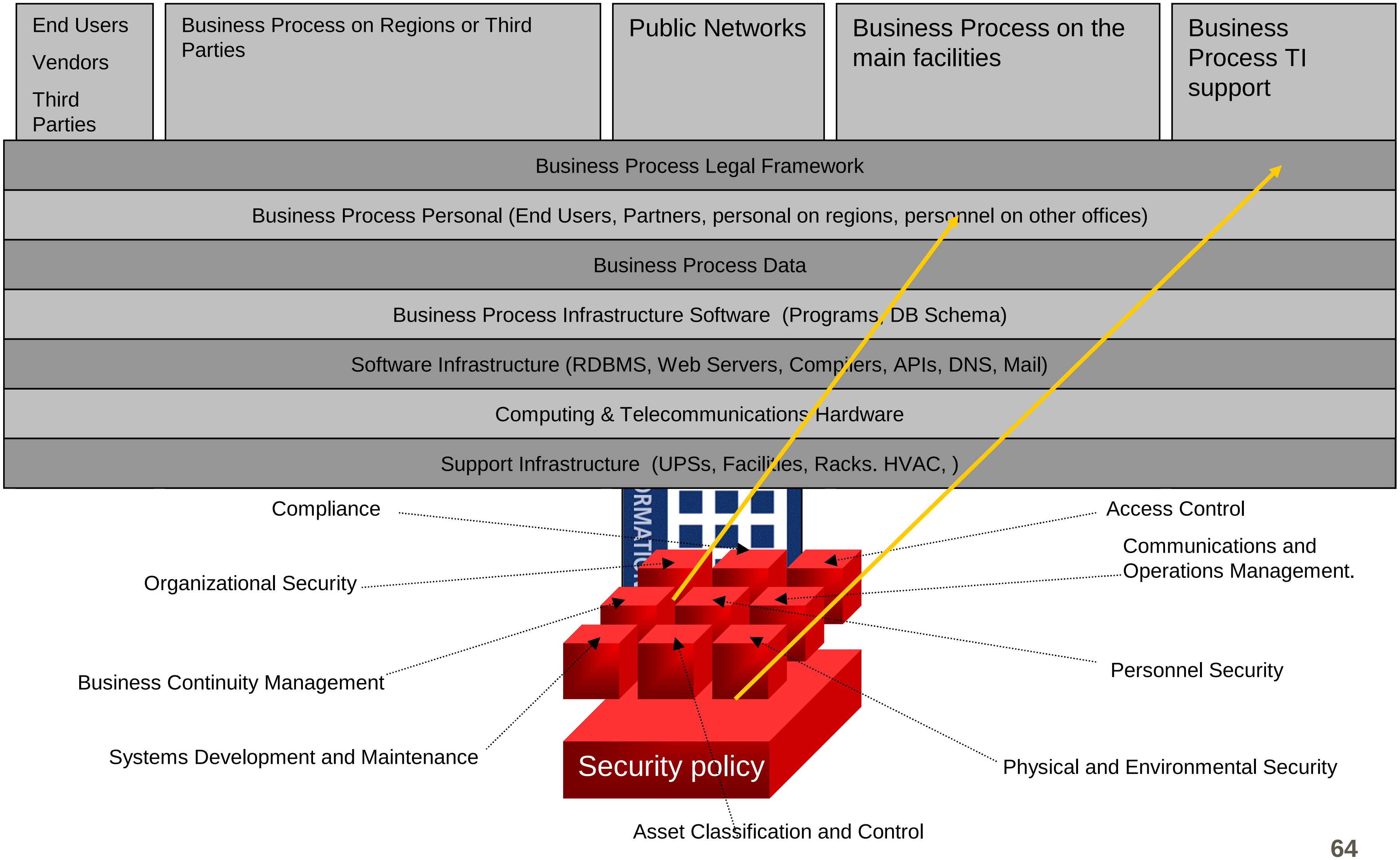
Asset classification and control

Security policy

Organizational security

Compliance

information security assets & Code of Practice



End Users

Vendors

Third Parties

Business Process on Regions or Third Parties

Public Networks

Business Process on the main facilities

Business Process TI support

Business Process Legal Framework

Business Process Personal (End Users, Partners, personal on regions, personnel on other offices)

Business Process Data

Business Process Infrastructure Software (Programs, DB Schema)

Software Infrastructure (RDBMS, Web Servers, Compilers, APIs, DNS, Mail)

Computing & Telecommunications Hardware

Support Infrastructure (UPSs, Facilities, Racks. HVAC,)

Compliance

Organizational Security

Business Continuity Management

Systems Development and Maintenance

Security policy

Asset Classification and Control

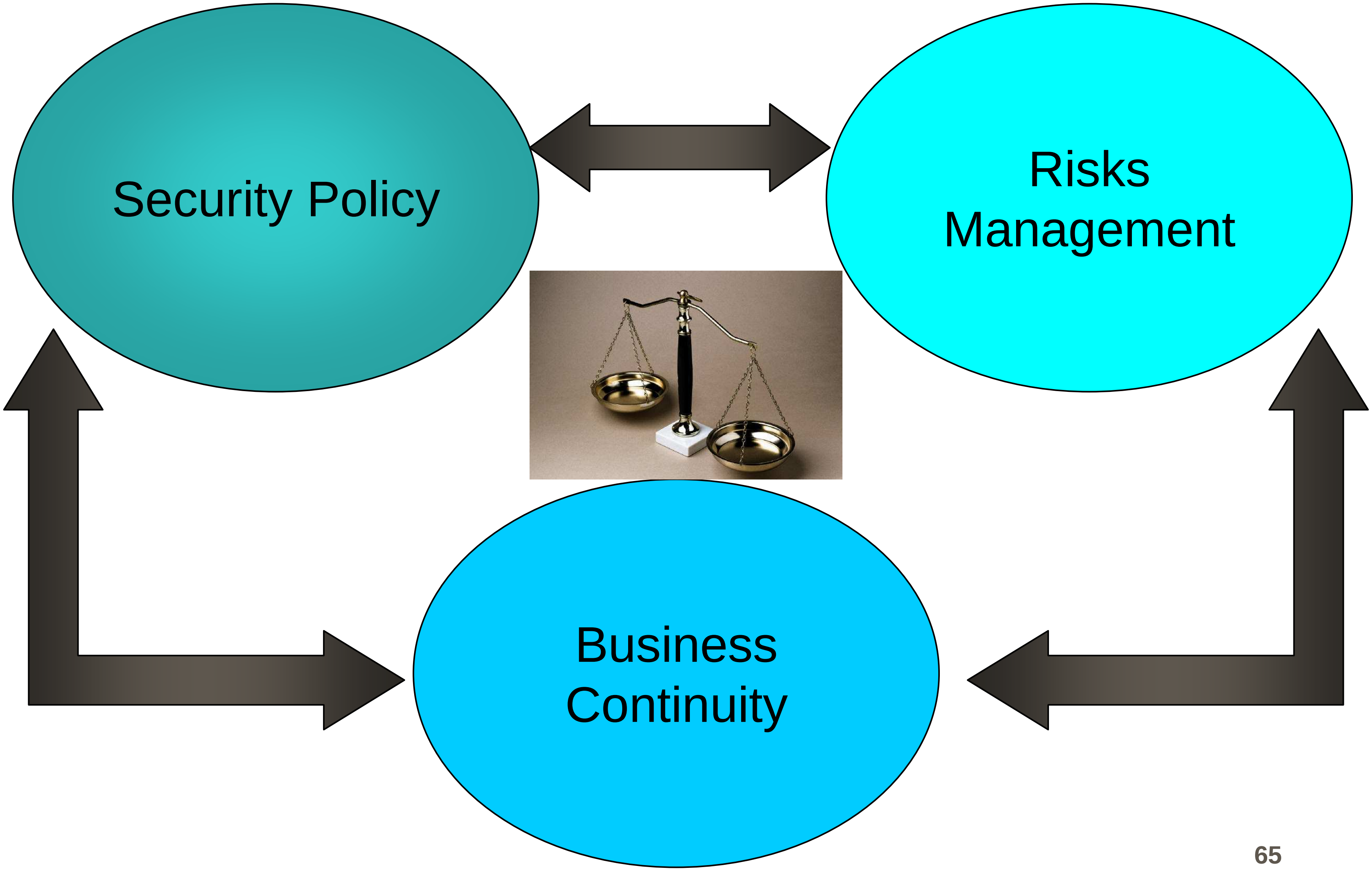
Access Control

Communications and Operations Management.

Personnel Security

Physical and Environmental Security

ISMS Main Processes



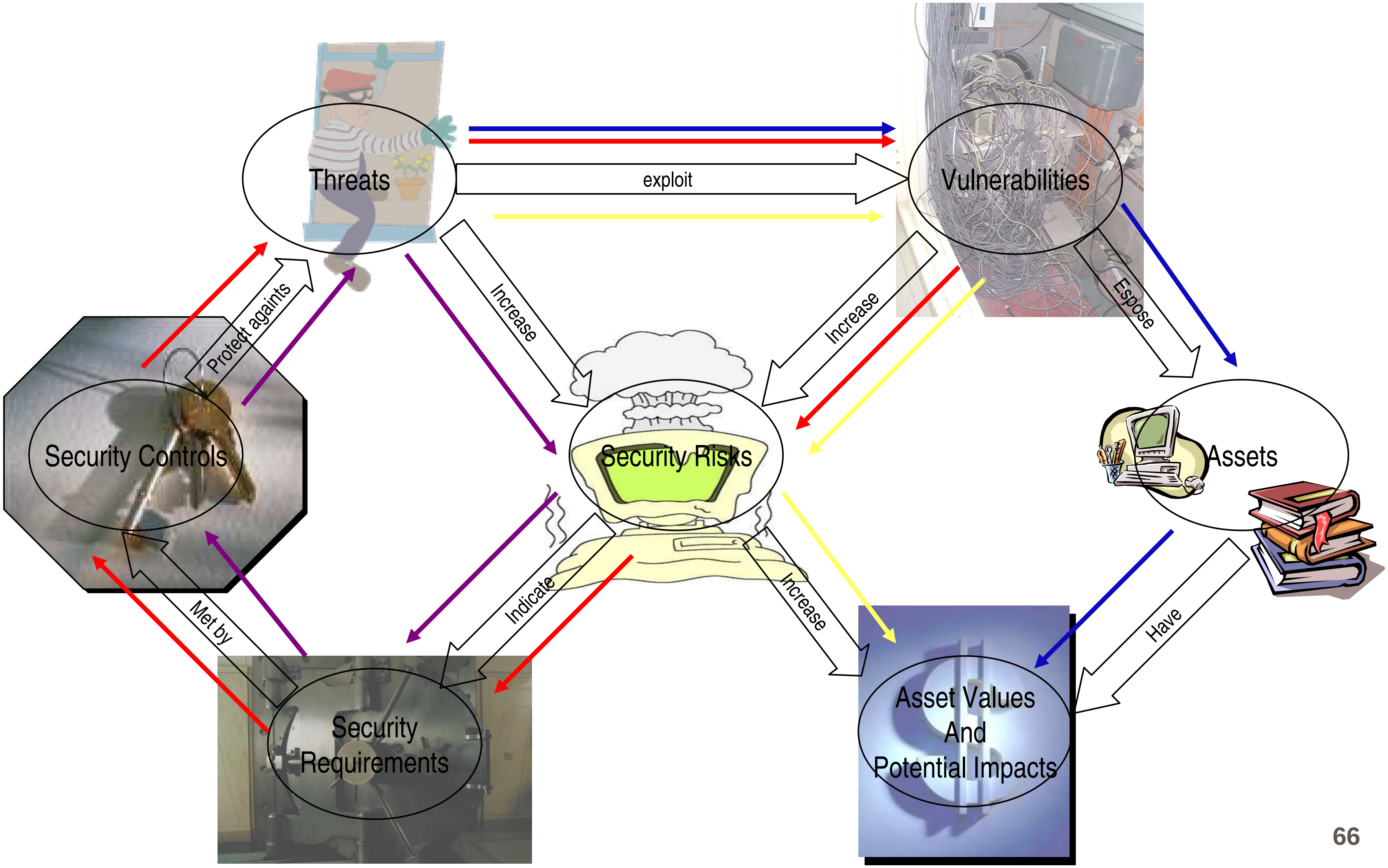
Security Policy

Risks Management

Business Continuity

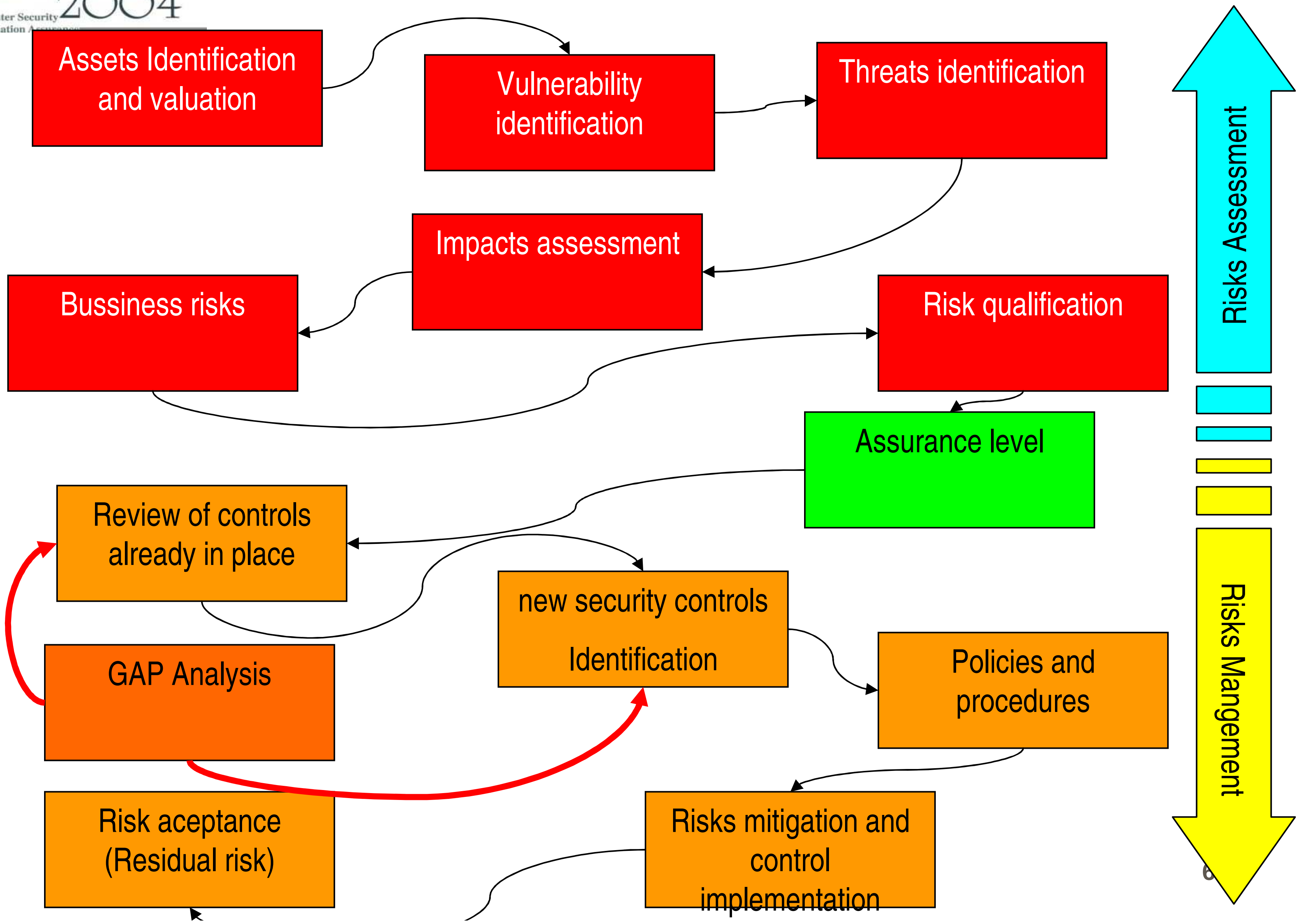
NEbraska CERT Conference 2004
Computer Security and Information Assurance

ISMS risks management



Nebraska CERT Conference 2004
Computer Security and Information Assurance

Risks Assessment and Management



Assets Identification and valuation

Vulnerability identification

Threats identification

Impacts assessment

Bussiness risks

Risk qualification

Assurance level

Review of controls already in place

new security controls Identification

Policies and procedures

GAP Analysis

Risk aceptance (Residual risk)

Risks mitigation and control implementation

Risks Assessment

Risks Mangement

Risk Analysis Tools and Methods

- @Risk
- Analyse des Risques Programmes
- AnalyZ
- AROME+
- BDS Risk Assesor
- BDSS (Bayesian Decision Support System)
- Buddy System
- COBRA (Consultative, Objetive and Bifunctional Risk Analysis)
- CONTROL-IT
- CRITI_CAL
- CRAMM (CCTA Risk Analysis and Management Method)
- DDIS (Datenschutz-und-datensicherheits Informations system)
- LAVA (Los Alamos Vulnerability Analysis)
- LRAM & ALRAM ([Automated]Livermore Risk Analysis Methodology)
- MELISA
- MINIRISK
- PREDICT
- PSICHE
- RANK-IT
- RISAN
- Risiko
- RiskCALC
- RiskPAC
- RiskWatch
- Security By Analysis (SBA)
- SISSI
- Triage Software
- Xacta
- XRM (eXpert Risk Management)

ISMS Bussiness continuity

- **Program Management**
  - **Program Administration**
  - **Program Coordinator**
  - **Advisory Committee**
  - **Program Evaluation**

ISMS Bussiness continuity

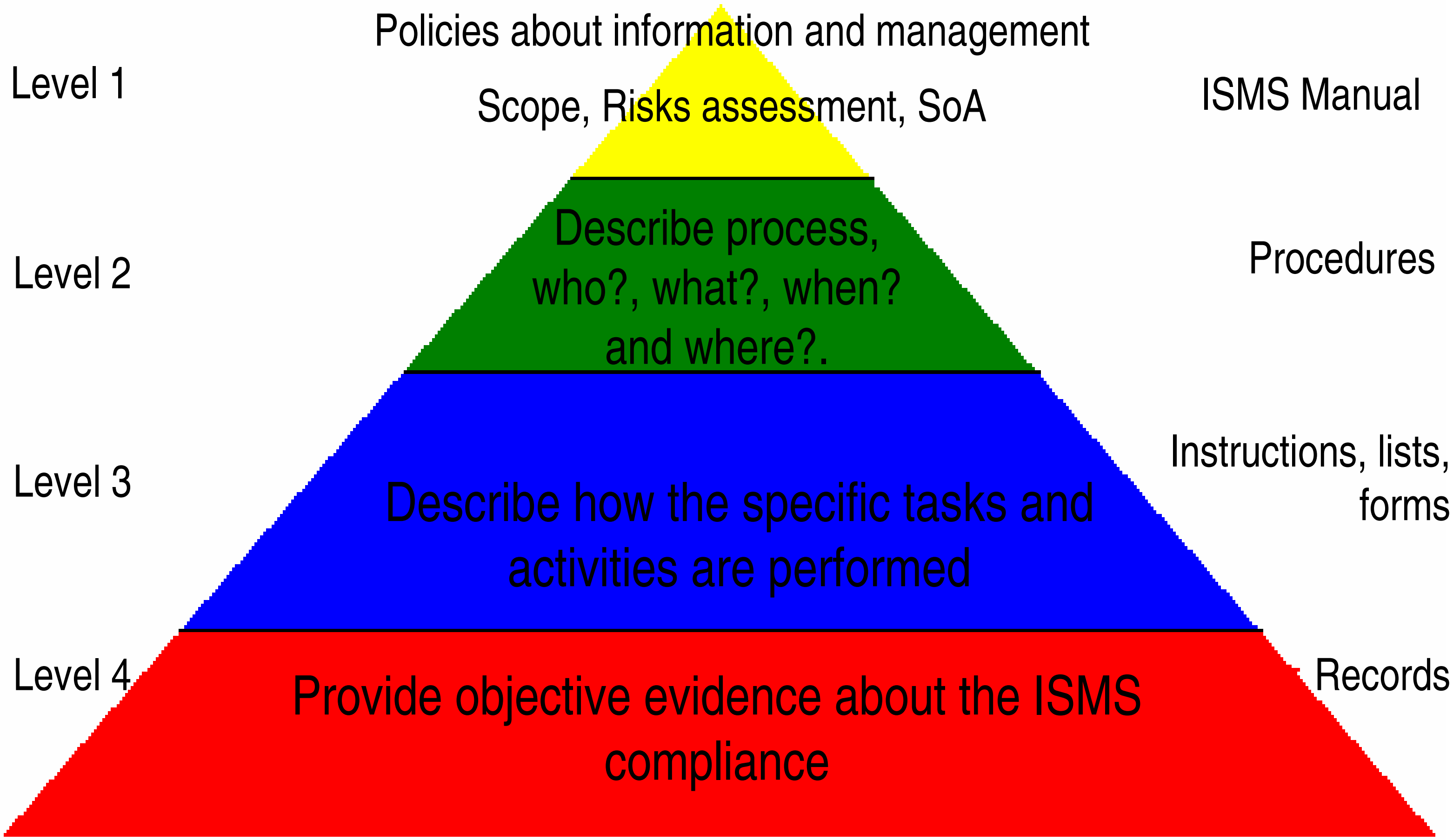
- **Program Elements**
  - Laws and Authorities
  - Hazard Identification, Risk Assessment,and Impact Analysis
  - Hazard Mitigation
  - Resource Management
  - Mutual Aid
  - Planning
  - Direction, Control, and Coordination
  - Communications and Warning
  - Operations and Procedures
  - Logistics and Facilities
  - Training
  - Exercises, Evaluations, and Corrective Actions
  - Crisis Communication and Public Information
  - Finance and Administration

ISMS Security Policy

- A written policy document shall be available to all employes responsible for information
  - Define the information security policy
  - Define the scope of the ISMS
  - Undertake risk assessment
  - Manage the risk
  - Select control objectives and controls to be implemented
- Prepare the SoA
- Comply with the documental requirements

NEbraska CERT Conference 2004
Computer Security and Information Assurance

Documental requirements


Level 1
Policies about information and management
Scope, Risks assessment, SoA
ISMS Manual
Level 2
Describe process, who?, what?, when? and where?.
Procedures
Level 3
Describe how the specific tasks and activities are performed
Instructions, lists, forms
Level 4
Provide objective evidence about the ISMS compliance
Records

Documental requirements

- Level 1 ISMS Manual
  - **Management structure, including the information security policy, objective controls, specific controls according the SoA**
  - **Should be linked with documents on the another levels**

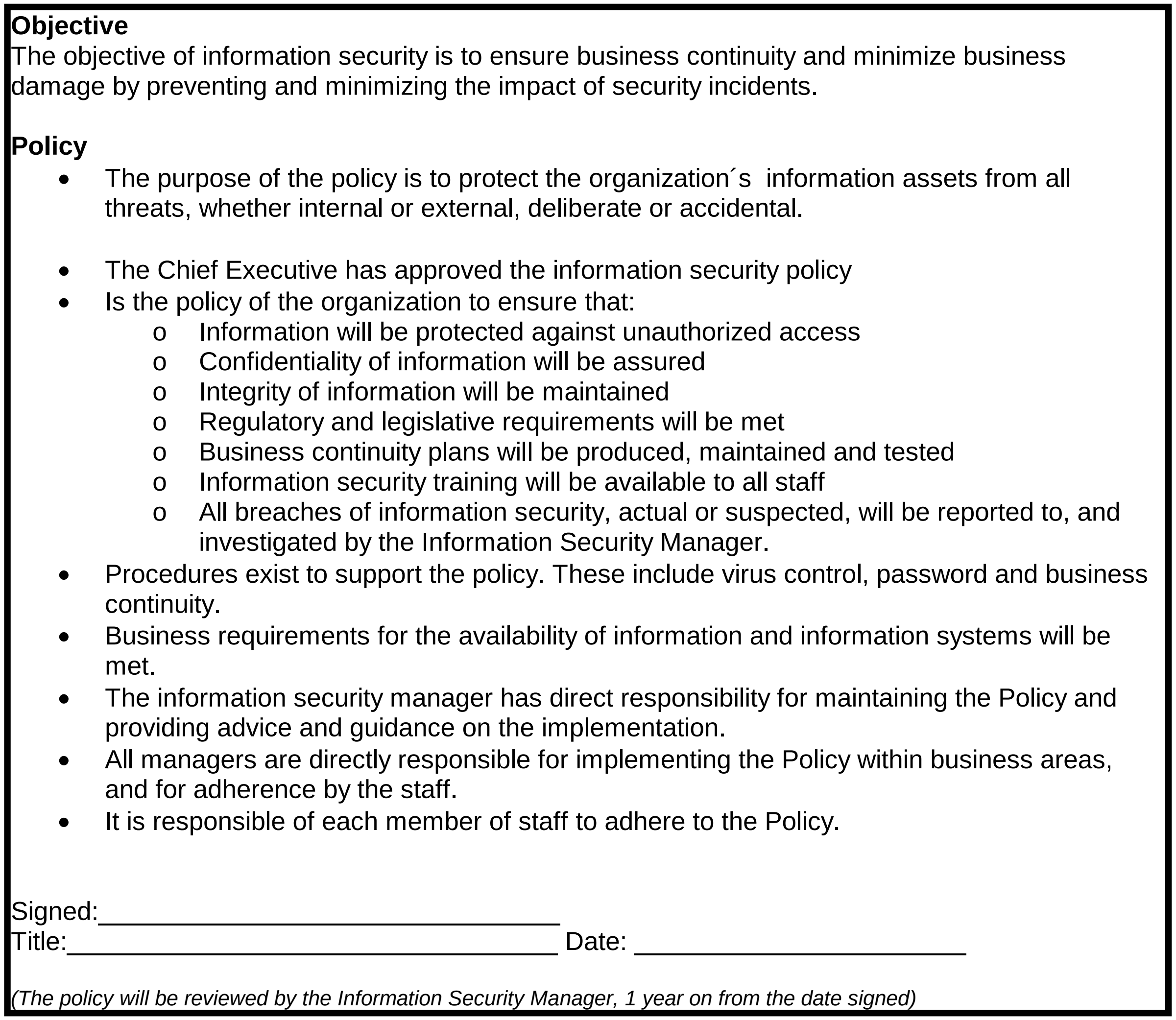
- Level 2 Procedures.
  - **Procedures adopted to implement the controls.**
  - **Describe process, who?, what?, when? and where?, between different roles and departments.**

Documental requirements

- Level 3. Instructions, lists, forms
  - **Describe how the specific tasks and activities are performed**
  - **Specific specific tasks, work detail instructions, forms, flow diagrams, standards, and systems manuals.**

- Level 4. Records
  - **Record are objective activity evidences according the levels 1,2, 3.**
  - **Can be mandatory or discretional.**
  - **Visitors books, audit records, review records, authorization forms, access control logs on computers**

Example policy statement



Objective
The objective of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents.

Policy

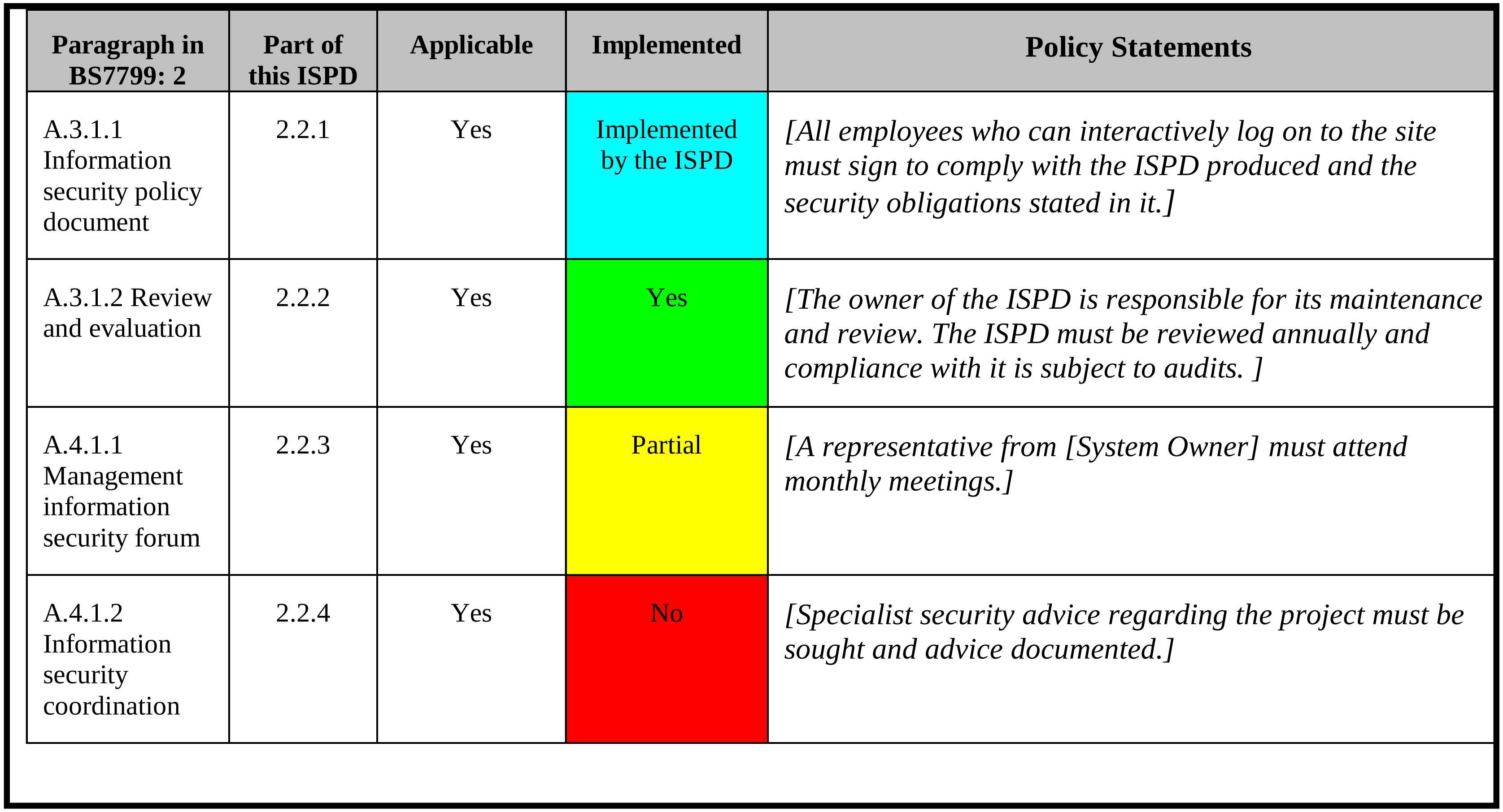
- The purpose of the policy is to protect the organization´s information assets from all threats, whether internal or external, deliberate or accidental.

- The Chief Executive has approved the information security policy
- Is the policy of the organization to ensure that:
  - o Information will be protected against unauthorized access
  - o Confidentiality of information will be assured
  - o Integrity of information will be maintained
  - o Regulatory and legislative requirements will be met
  - o Business continuity plans will be produced, maintained and tested
  - o Information security training will be available to all staff
  - o All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Manager.
- Procedures exist to support the policy. These include virus control, password and business continuity.
- Business requirements for the availability of information and information systems will be met.
- The information security manager has direct responsibility for maintaining the Policy and providing advice and guidance on the implementation.
- All managers are directly responsible for implementing the Policy within business areas, and for adherence by the staff.
- It is responsible of each member of staff to adhere to the Policy.

Signed:________________________________
Title:__________________________________ Date: _______________________

(The policy will be reviewed by the Information Security Manager, 1 year on from the date signed)

SoA



Paragraph in BS7799: 2	Part of this ISPD	Applicable	Implemented	Policy Statements
A.3.1.1 Information security policy document	2.2.1	Yes	Implemented by the ISPD	*[All employees who can interactively log on to the site must sign to comply with the ISPD produced and the security obligations stated in it.]*
A.3.1.2 Review and evaluation	2.2.2	Yes	Yes	*[The owner of the ISPD is responsible for its maintenance and review. The ISPD must be reviewed annually and compliance with it is subject to audits.]*
A.4.1.1 Management information security forum	2.2.3	Yes	Partial	*[A representative from [System Owner] must attend monthly meetings.]*
A.4.1.2 Information security coordination	2.2.4	Yes	No	*[Specialist security advice regarding the project must be sought and advice documented.]*

SoA

#Dom	Domain	# Obj	Objective	#Control	ect	Document
3	A.3 Security policy	3.1	A.3.1 Information security policy	3.1.1	A.3.1.1 Information security policy document	Y	00102 – Policy
				3.1.2	A.3.1.2 Review and evaluation	Y	00102 – Policy
4	A.4 Organizational security	4.1	A.4.1 Information security infrastructure	4.1.1	A.4.1.1 Management information security forum	Y	00108 – Risks management
				4.1.2	A.4.1.2 Information security coordination	Y	00108 – Risks management
				4.1.3	A.4.1.3 Allocation of information security responsibilities	Y	00108 – Risks management
				4.1.4	A.4.1.4 Authorization process for information processing facilities	Y	00304 – Equipment manual
				4.1.5	A.4.1.5 Specialist information security advice	Y	00108 – Risks management
				4.1.6	A.4.1.6 Cooperation between organizations	Y	00120 - Individual contracts
				4.1.7	A.4.1.7 Independent review of information security	Y	00108 – Risks management
		4.2	A.4.2 Security of third-party access	4.2.1	A.4.2.1 Identification of risks from third-party access	Y	00107 – Risk Audit

SoA

Control	Selected (yes/no)	Justification
A.8.3.1 Controls against malicious software	Yes	Highlighted by risk assessment. High risk of damage to PC systems and network servers. Baseline control for organization wide implementation
A.9.4.3 User authentication for external connections	Yes	High risk of unauthorized access through dial up lines. Security policy specifies authentication to be mandatory. Baseline control for organization wide implementation
A.9.5.6 Duress alarm to safeguard users	No	Not relevant in this organization. Not identifiable threat. Specifically excluded from baseline.
A.10.1.1 Security requirements	Yes	Refer to Functional Specification, document number 100.190.010
A.12.3.2 Protection of system audit tools	no	Not relevant to this domain (application system)

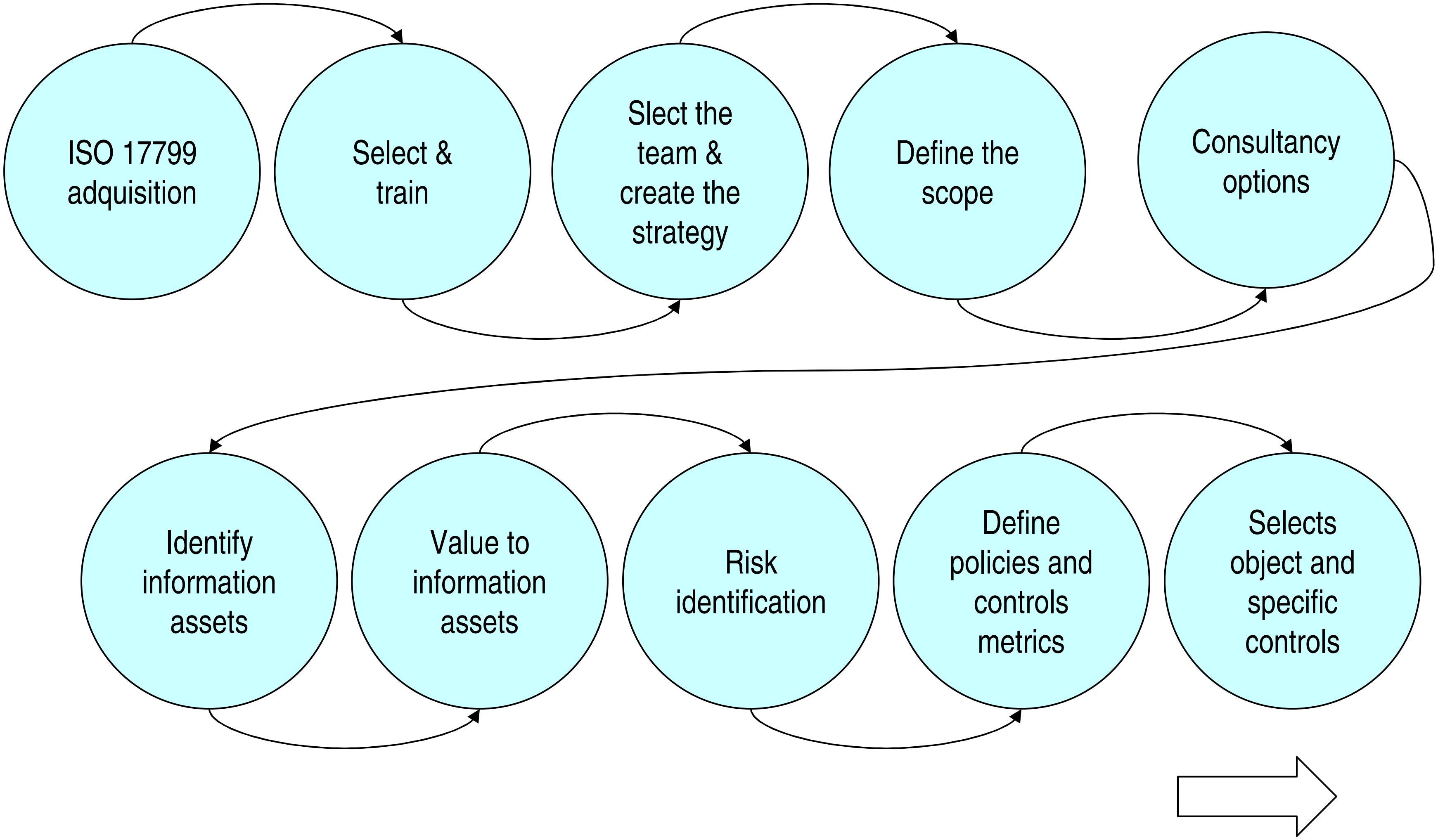
NEbraska CERT Conference 2004

Computer Security and Information Assurance

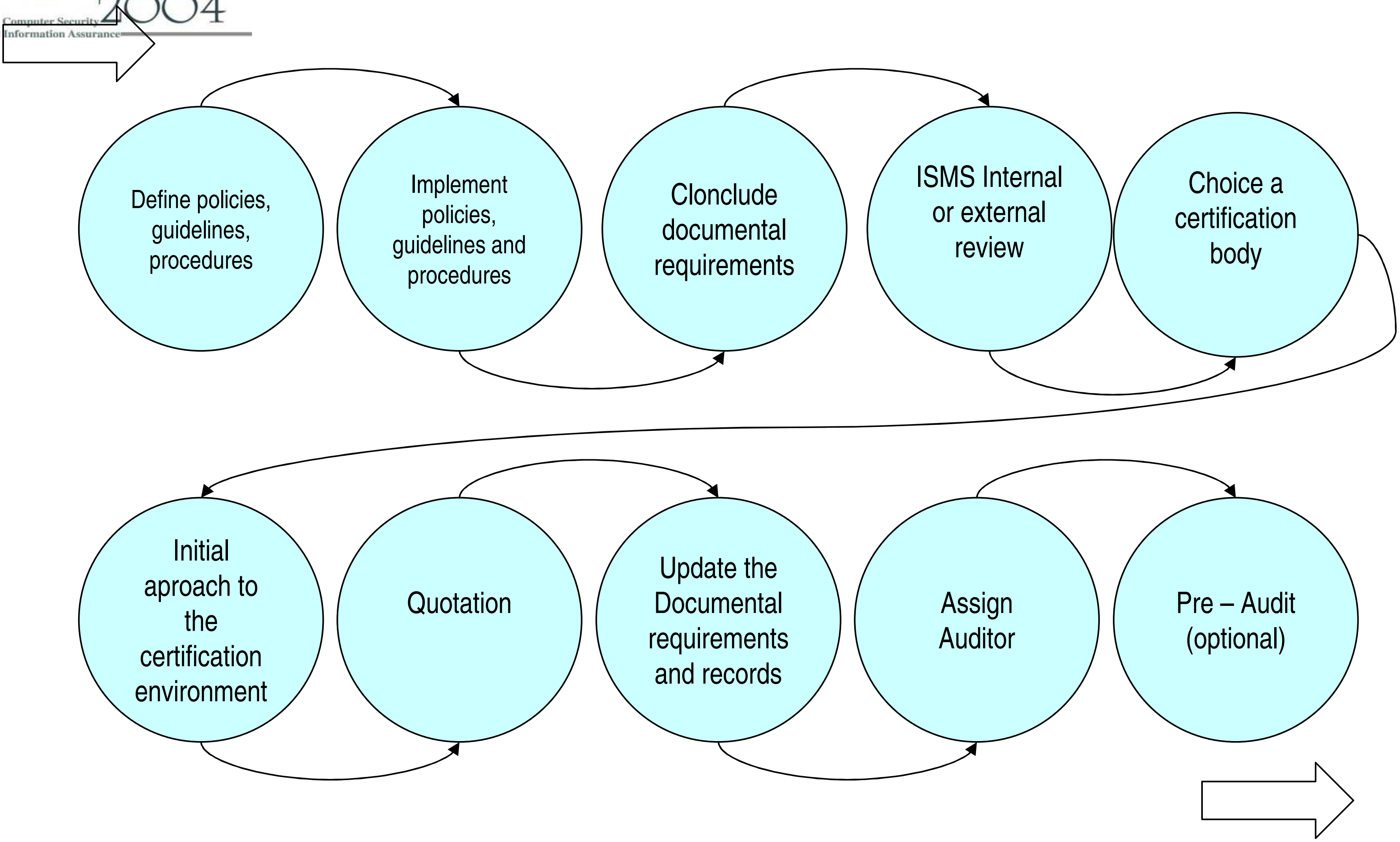
The path to certification

NEbraska CERT Conference 2004
Computer Security and Information Assurance

The path to certification


ISO 17799 adquisition
Select & train
Slect the team & create the strategy
Define the scope
Consultancy options
Identify information assets
Value to information assets
Risk identification
Define policies and controls metrics
Selects object and specific controls

The path to certification



Define policies, guidelines, procedures

Implement policies, guidelines and procedures

Clonclude documental requirements

ISMS Internal or external review

Choice a certification body

Initial aproach to the certification environment

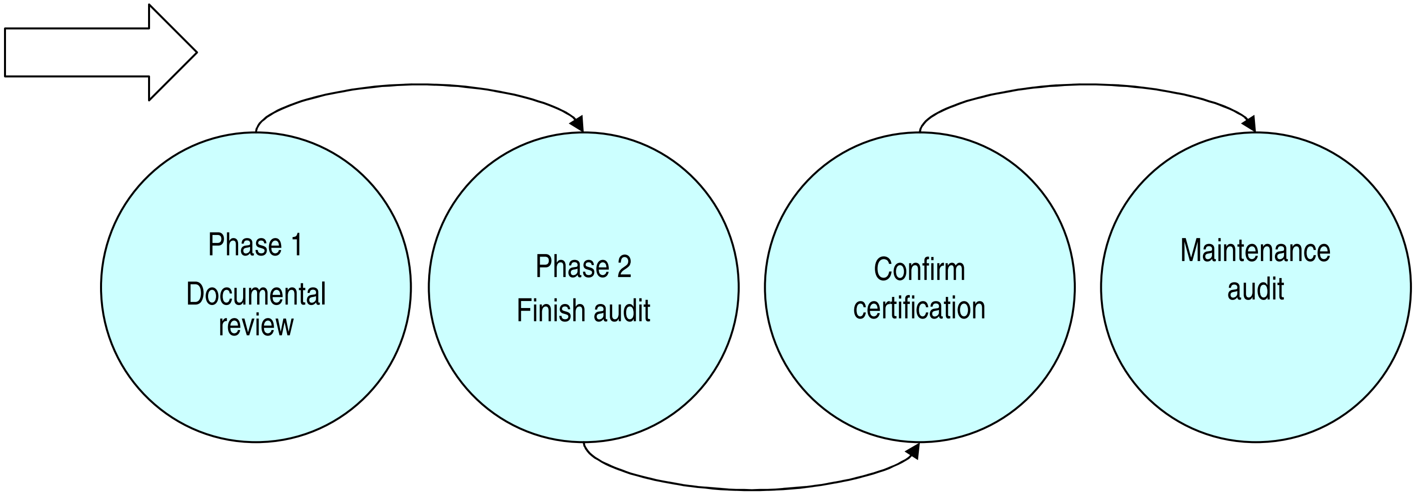
Quotation

Update the Documental requirements and records

Assign Auditor

Pre – Audit (optional)

The path to certification



Phase 1

Documental review

Phase 2

Finish audit

Confirm certification

Maintenance audit

If the audit is sucessful

Every 6 months internal

(Recertification every 3 years)

Questions

Ing. Leonardo García Rojas

CISSP, CISM

+52 55 5342-3575

Innovaciones Telemáticas

lgarcia@intelematica.com.mx

leonardo_garciar@yahoo.com