Information Security Management System BS 7799-2: 2002

Bill Casti, CQA – Security & Privacy Professional Services

Configuration Management Working Group
Tysons Corner, VA
11 November 2003

What is Information?

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

BS ISO 17799:2000

Information Lifecycle

Information can be:

Created

Stored

Destroyed?

Processed

Transmitted

Used – for proper and improper purposes

Lost

Corrupted

Types of Information

Information can be:

- Printed or written on paper
- Stored electronically
- Transmitted by mail or using electronic means
- Shown on corporate videos
- Verbal – spoken in conversation

"Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected" (BS ISO 17799:2000)

Example 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

Information Security Management

The ISO 17799 Way

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

What is Information Security?

BS ISO 17799:2000 defines this as:

- **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

Let’s Eliminate Some Confusion

What’s the difference between BS ISO 17799:2000 and BS 7799-2:2002?

- ISO 17799 is the “shoulds”, the “best practices” for implementation; it is the same as BS 7799, Part 1.
- BS 7799-2:2002 is the “musts”, the requirements against which organizations are audited for registration; no audits are conducted against ISO 17799.
- There’s no such thing as an “ISO 17799 certification”. If you pass, you will be accredited to BS 7799-2:2002.
- BS 7799-2 is on an ISO “fast track” for approval as ISO 17799-2; release maybe in 2004.

CIA Balance

Confidentiality

Availability

Integrity

In some organizations, integrity and/or availability may be more important than confidentiality.

Critical Success Factors

- Security plan that reflects business objectives
- Implementation approach is consistent with company culture
- Visible support and commitment from all management
- Good understanding of security requirements, risk assessment and risk management
- Effective marketing of security to all managers and staff

Critical Success Factors (concl.)

- Distribution of guidance on information security policy and standards to all employees and contractors
- Providing appropriate training and education
- A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement

A.3 Security Policy
A.3.1 Information Security Management Plan

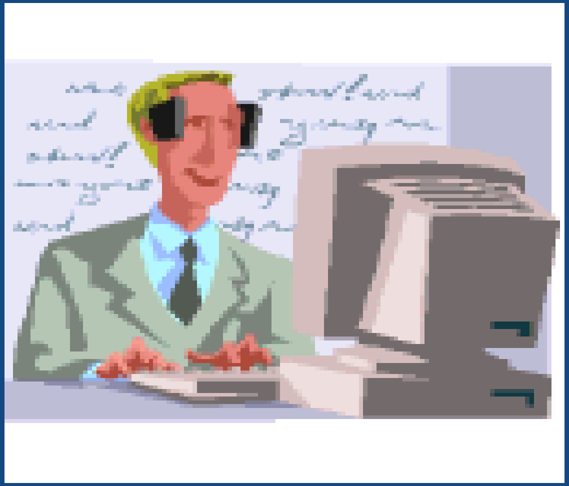
- Information security policy document.
- Review and evaluation.
- All information protection procedures apply to all personnel within the registration scope area.

A.4 Organizational Security
A.4.1 Information Security Infrastructure

- Management Information Security Forum
  - Information security co-ordination
  - Allocation of information security responsibilities
  - Authorization process for information processing facilities
  - SME information security advice
  - Manages cooperation between interfacing groups and teams
  - Independent review of information security (peer review)

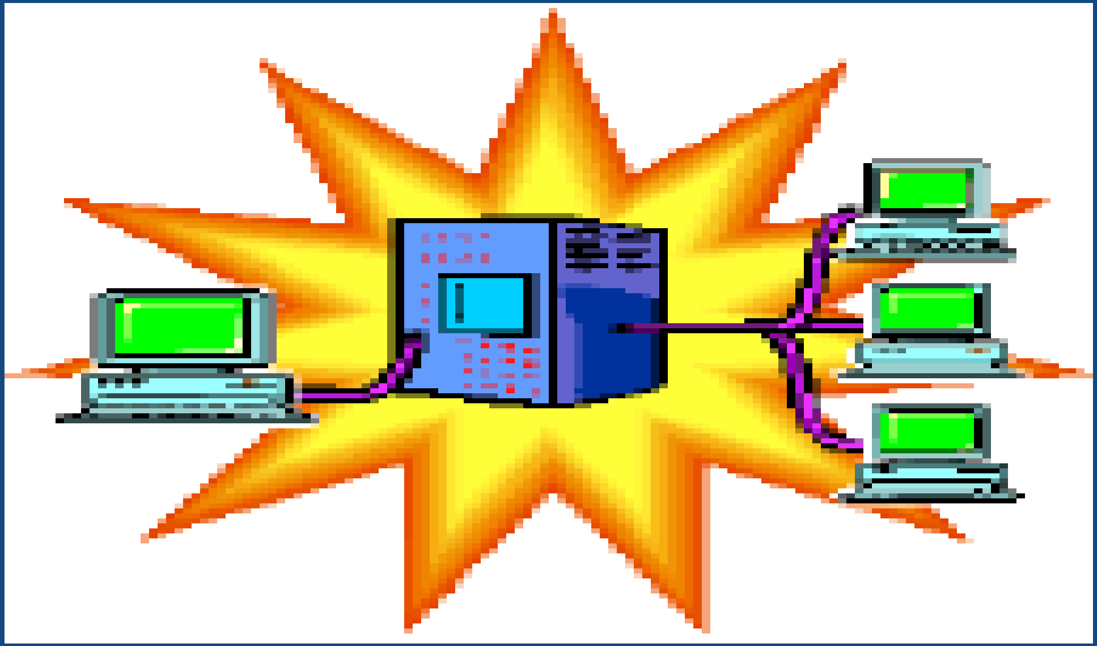
A.4 Organizational Security
A.4.2 Security of Third Part Access

- Identification of risks from third party access
- Security requirements in third party contracts



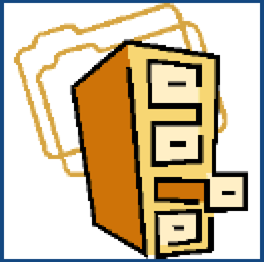
A.4 Organizational Security
A.4.3 Outsourcing

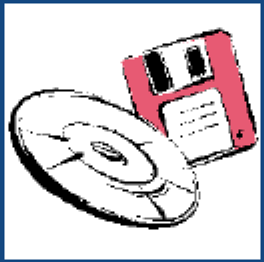
- Security requirements in teaming and outsourcing agreements



A.5 Asset Classification and Control
A.5.1 Accountability for Assets

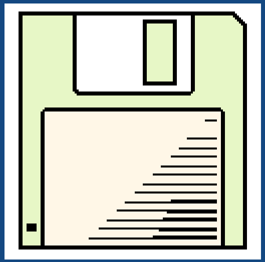
- Inventory of assets





A.5 Asset Classification and Control
A.5.2 Information Classification

- Classification guidelines
- Information labeling and handling



Protectively Marked

Top Secret

Secret

Confidential

Restricted

A.6 Personnel Security
A.6.1 Security in Job Definition and Resourcing

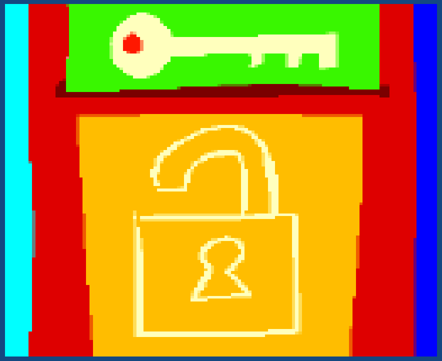
- Include security in job responsibilities
- Personnel screening and policy
- Confidentiality agreements
- Terms and conditions of employment

A.6 Personnel Security
A.6.2 User Training

- Information security education and training

A.6 Personnel Security
A.6.3 Responding to Security Incidents and Malfunctions

- Reporting security incidents
- Reporting security weaknesses
- Reporting software malfunctions
- Learning from incidents
- Disciplinary process



A.7 Physical Security
A.7.1 Secure Areas

- Physical security perimeter
- Physical entry controls
- Securing offices, rooms and facilities
- Working in secure areas
- Isolated delivery and loading areas

A.7 Physical Security
A.7.2 Equipment Security

- Equipment siting and protection
- Power supplies
- Cabling security
- Equipment maintenance
- Security of equipment off-premises
- Secure disposal or re-use of equipment

A.7 Physical Security
A.7.3 General Controls

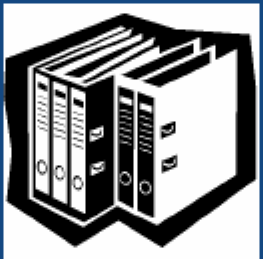
- Clear desk and clear screen policy:

When you leave your office workstation, your monitor screensaver should be engaged and locked.

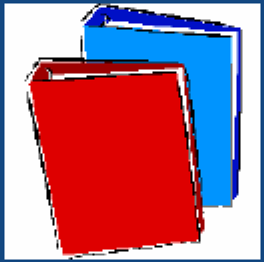
- Removal of property:

All company property leaving the site must be accompanied by a properly assigned and approved Corporate Property Pass

A.8 Communication and Operations Management
A.8.1 Operational Procedures and Responsibilities



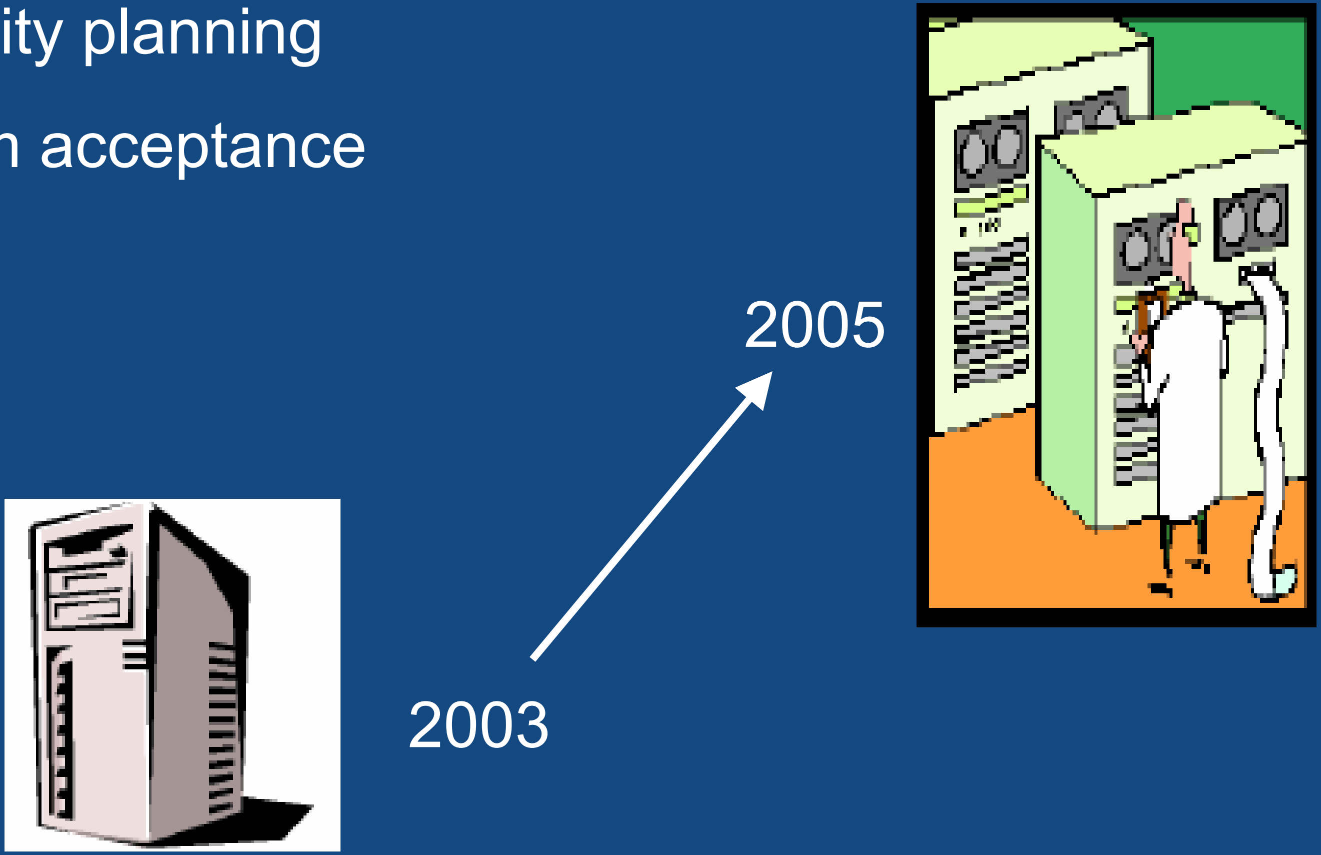
- Documented operating procedures
- Operational change controls
- Incident management procedures
- Segregation of duties



- Separation of development and operational facilities
- External facilities management (lab coordinator)

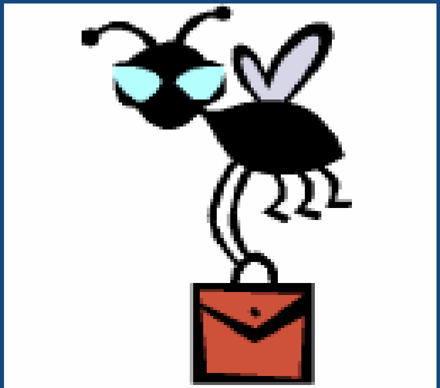
A.8 Communications and Operations Management
A.8.2 System Planning and Acceptance

- Capacity planning
- System acceptance



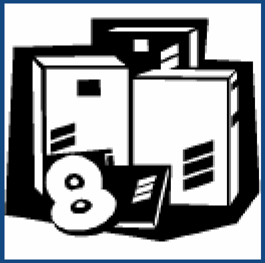
A.8 Communication and Operations Management
A.8.3 Protection Against Malicious Software

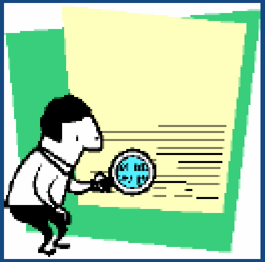
- Controls against malicious software

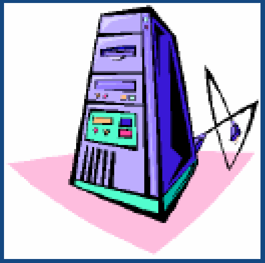


A.8 Communications and Operations Management
A.8.4 Housekeeping

- Information backup
- Operator logs
- Fault logging

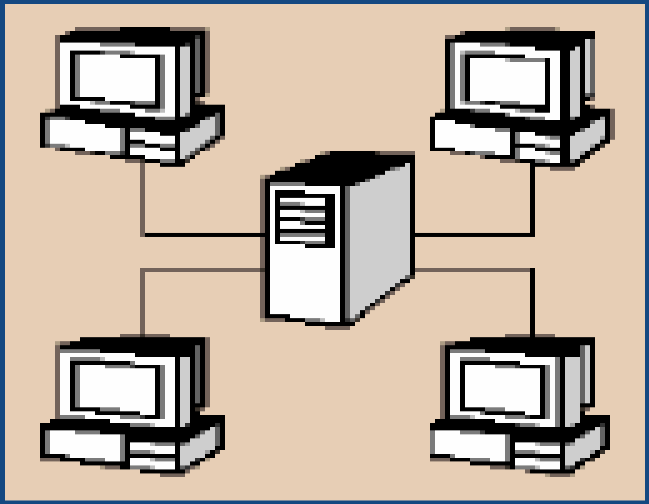






A.8 Communication and Operations Management
A.8.5 Network Management

- Network controls



A.8 Communication and Operations Management
A.8.7 Exchanges of Information and Software

- Information and software exchange
- Security of media in transit
- Security of customer-bound email
- Security of electronic office systems
- Publicly-available systems
- Other forms of information exchange

A.9 Access Control
A.9.1 Business Requirements for Access Control

- Access control policy

You are not authorized to access this system

A.9 Access Control
A.9.2 User Access Management

- User registration
- Privilege management
- User password management
- Review of user access rights

A.9 Access Control
A.9.3 User Responsibilities

- Password use
- Unattended user equipment

A.9 Access Control
A.9.4 Network Access Control

- Policy on use of network services
- Enforced path
- User authentication for external connections
- Node authentication
- Remote diagnostic port protection
- Segregation in networks
- Network connection control
- Network routing control
- Security of network services

A.9 Access Control
A.9.5 Operating System Access Control

- Automatic terminal identification
- Terminal log-in procedures
- User identification and authentication
- Password management system
- Use of system facilities
- Duress alarm to safeguard users
- Terminal timeout
- Limitation of connection time

A.9 Access Control
A.9.6 Application Access Control

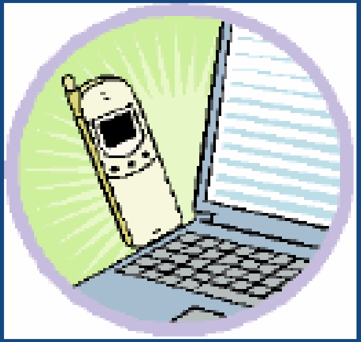
- Information access restriction
- Sensitive system isolation

A.9 Access Control
A.9.7 Monitoring System Access and Use

- Event logging
- Monitoring system use
- Clock synchronization

A.9 Access Control
A.9.8 Mobile Computing and Teleworking

- Mobile computing
- Teleworking



A.10 Security Development and Maintenance
A.10.1 Security Requirements of Systems

- Security requirements analysis and specification

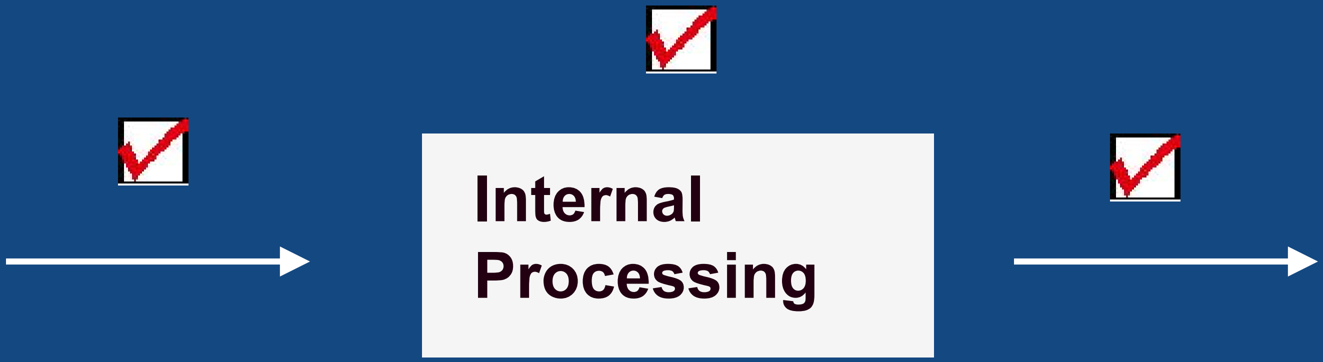
Specifications

Business Case

Security Requirements

A.10 Security Development and Maintenance
A.10.2 Security in Application Systems

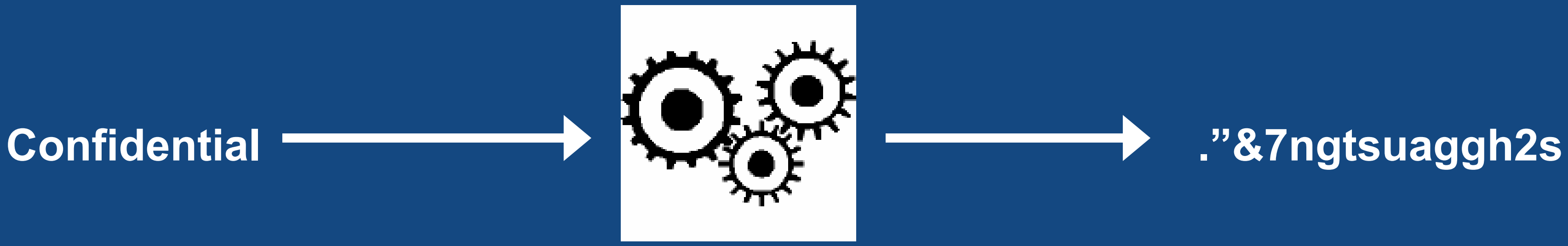
- Input data validation
- Control of internal processing
- Message authentication
- Output data validation



Internal Processing

A.10 Security Development and Maintenance
A.10.3 Cryptographic Controls

- Policy on use of cryptographic controls
- Encryption
- Digital signatures
- Non-repudiation services
- Key management

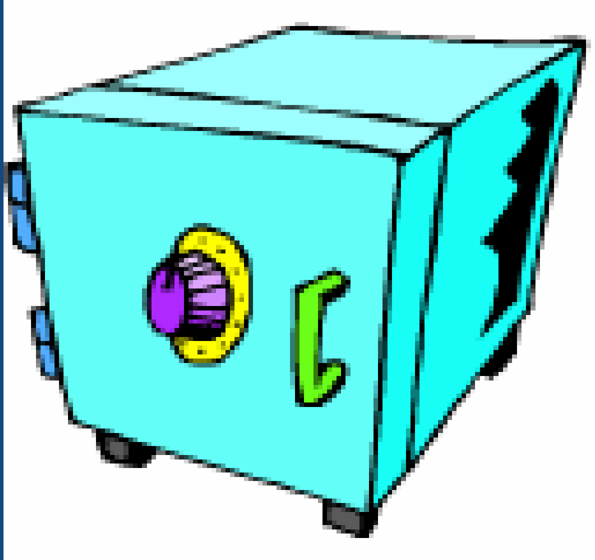


Confidential

.”&7ngtsuaggh2s

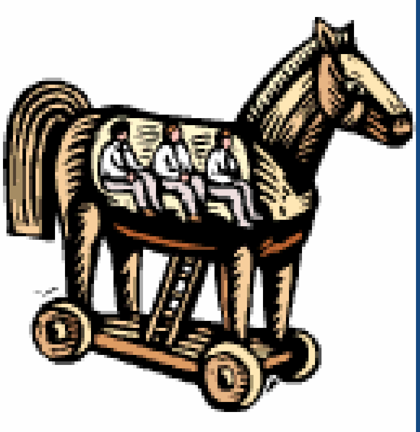
A.10 Security Development and Maintenance
A.10.4 Security of System Files

- Control of operational software
- Protection of system test data
- Access control to program source library



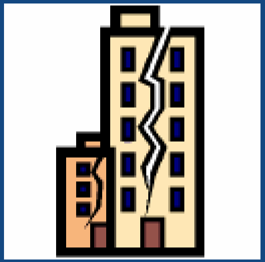
A.10 Security Development and Maintenance
A.10.4 Security in Development and Support Processes

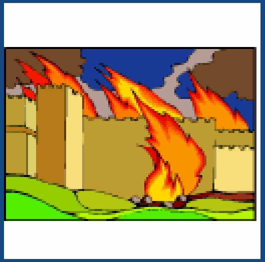
- Change control procedures
- Technical review of operating system changes
- Restrictions on changes to software packages
- Covert channels and Trojan code
- Control of outsourced software development



A.11 Business Continuity Management
A.11.1 Aspects of Business Continuity Management

- Business continuity management process
- Business continuity and impact analysis
- Writing and implementing continuity plans
- Business continuity planning framework
- Testing, maintaining and re-assessing business continuity plans





A.12 Compliance
A.12.1 Compliance with Legal Requirements

- Identification of applicable legislation
- Intellectual property rights (IPR)
- Safeguarding of organizational records
- Data protection and privacy of personal information
- Prevention of misuse of information processing facilities
- Regulation of cryptographic controls
- Collection of evidence

A.12 Compliance
A.12.2 Reviews of Security Policy and Technical Compliance

- Compliance with information security plan and policies
- Technical compliance checking

A.12 Compliance
A.12.3 System Audit Considerations

- System audit controls
- Protection of system audit tools

Note

“Not all of the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization.”

BS 7799-2:2002

BS 7799 Requirement

- Implementation and certification to BS 7799 is based on the results of a formal Risk Assessment
- Is the assessment appropriate?

Risk

- *Risk*: the possibility of incurring misfortune or loss; hazard
- *At risk*: Vulnerable; likely to be lost or damaged
- *Take or run a risk*: to proceed in an action without regard to the possibility of danger involved in it
- *Risk*: (verb) to expose to danger or loss

Security Risk

A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of information assets.

Risk Assessment Process

- Identifying assets and assigning values
- Identifying threats to these assets and assessing their likelihood
- Identifying vulnerabilities and assessing how easily they might be exploited
- Identifying the protection provided by the controls in place
- Assessing the overall risk resulting from the above

Risk Assessment and Treatment Process

Risk Assessment

Asset Identification and Valuation

Identification of Vulnerabilities

Identification of Threats

Evaluation of Impacts

Business Risks

Rating/Ranking of Risks

Risk Treatment

Review of existing security controls

Gap Analysis

Identification of new security controls

Policy and Procedures

Implementation and Risk Reduction

Risk Acceptance (residual risk)

Threat

- A declaration of the intent to inflict harm, pain or misery
- Potential to cause an unwanted incident, which may result in harm to a system or organization and its assets
- Intentional or accidental, man-made or an act of God
- Assets are subject to many kinds of threats which exploit vulnerabilities

Threats

- Natural disaster – flooding, hurricane, tornado, earthquake, lightning
- Human – staff shortage, maintenance error, user error
- Technological – failure of network, traffic overloading, hardware failure
- Deliberate threats
- Accidental threats
- Threat frequency

Vulnerability

- A vulnerability is a weakness/hole in an organization’s information security
- A vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset
- A vulnerability, if not managed, will allow a threat to materialize

Vulnerabilities

- Absence of key personnel
- Unstable power grid
- Unprotected cabling lines
- Lack of security awareness
- Wrong allocation of password rights
- Insufficient security training
- No firewall installed
- Unlocked door

Risk

Risk

=

Value x Threat x Vulnerability (Impact)

x Likelihood of Occurrence

Ranking of Threats by Measures of Risk

Threat Descriptor A	Impact (asset) B	Likelihood of Threat Occurrence	Measure of Risk D = BxC	Threat Ranking E
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Distinction Between Tolerable and Intolerable Risks

Damage Value	0	1	2	3	4
Frequency Value					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Tools and Methods for Risk Assessment

Q: What tool does BS 7799 recommend?

A: The risk assessment shall identify threats to assets, vulnerabilities and impacts on the organization and shall determine the degree of risk

Risk Treatment - Plan

- The risk treatment plan is a coordination document defining the actions to reduce unacceptable risks and implement the required controls to protect information

Risk Treatment - Plan

	BS 7799-2 Clause	Type of change	Finding	Proposed Remedy	Level of Effort	Notes	Threat Level: H/M/L	Risk Level: H/M/L	*Overall Risk*	Will we mitigate this risk?	Will we buy off on this risk?	If "yes", why?	Responsible Party
1	A11.1	BC/DR	No contingency plan document has been prepared for the GSOC Research Network	BIA (first step) in progress; generate BC/DR plan	**80.0**		**L**	**M**	**M**	**Yes**	**No**		Casti
2	A11.1	BC/DR	Procedures for recovery of the network and continuity of business operations are not defined or documented	BC/DR plan based on corporate network BC/DR	**40.0**	x 5 people	**L**	**M**	**M**	**Yes**	**No**		Casti
3	A11.1	BC/DR	No alternate site has been identified for recovery in the event of a disaster.	Follow Herndon plan or corporate plan as appropriate	**0.0**		**H**	**H**	**H**	***No***	***Yes***	***Inadequate respources for compliance***	Sr. Mgmt
4	A11.1	BC/DR	There is no contingency planning process, and no plans for business continuity, disaster recovery or emergency operations have been developed	Existing Herndon plans for BC/DR? may need specific operations plan for research network, perhaps similar to DowNet or corporate network	**0.0**		**L**	**M**	**M**	**Yes**	**No**		Casti

Risk Treatment - Directions

- Accepting the residual risk
- Avoiding the risk
- Transferring the risk
- Reducing the risk to an acceptable level

Levels of Acceptable Risk

- It is not possible to achieve total security
- There will always be residual risk
- What degree of residual risk is acceptable?

Risk Treatment Determinants

- Location
- Existing security
- Number of attackers
- Facilities available
- Cumulative opportunity
- Level of publicity
- Continuity of Operations Planning

Risk

- Controls must reflect the organization’s risk management strategy
- Must consider the impact of security risks on the business
- How important is it to us for “this” to be available in order to continue our business processes?

Risk Treatment

- Define an acceptable level of residual risk
- Constantly review real and potential threats and vulnerabilities
- Review existing security controls
- Applying additional security controls in accordance with BS 7799-2
- Introduce and revise/eliminate policies and procedures in order to manage information security against the evolving business needs

Control Selection

- Which control is the right one to apply?
- Which is right against our business requirements?

Control Selection Determinants

- Risk
- Degree of assurance required
- Cost
- Ease of implementing
- Servicing
- Legal and regulatory requirements
- Customer and other contractual requirements

Cost Determinants

- Budget limitations
- Does the cost of applying the control outweigh the value of the asset?
- May have to select “imperfect but best value” range of controls

Ease of implementing controls

- Does the work environment or infrastructure support “this” control?
- How long will the control take to implement?
- Is the control readily available?
- Does this control complement or reduce the value of other controls?

Servicing controls

- Are the skills available internally to manage control?
- Are upgrades readily available?
- Is the equipment supported by local engineers/suppliers?

Controls for Best Practice

- Our Information Security Management Plan
- Our Roles and Responsibilities document
- Information Security Education and Training
- Reporting our Information Security Incidents
- Our Continuity of Operations Overview and COO Procedure documents
- Leverage our ISO 9001:2000 registered QMS as needed to reduce reinventing the wheel

Customer and Other Contractual Requirements

- Security Screening
- Restricted Access
- Physical perimeters
- Data storage
- Encryption
- Digital signatures

Where to get the standards

- ✓ ISO and BS standards are copyrighted and have to be purchased; they should not be available for free on the Internet (if they are, someone is violating copyright).
- ✓ ISO standards from http://www.iso.ch or http://www.asq.org
- ✓ ISO and BS standards from BSI Americas http://www.bsitraining.com/standards.asp
- ✓ Both standards are available from BSI Americas on a CD in a searchable PDF format for $230.00

Questions?

Contact information:

Bill Casti, CQA

SPPS Delivery Excellence Manager

GSOC ISO Quality & BS 7799-2 InfoSec Manager

EDS Corporation

Herndon VA

Cell: 571-283-1802

Email: bill.casti@eds.com

Alternate email: help@quality.org http://www.quality.org

EDS

eds.com

Bill Casti, CQA

bill.casti@eds.com cell: 571-283-1802