Fundamentals of Information Security and Introduction to ISO 27001

About Qdot

www.qdot.ae

Qdot managed by a team of experienced professionals, is committed to promote quality & excellence culture in GCC (UAE, QATAR, KSA, Oman, Kuwait, Bahrain) by providing below mentioned services.

Management System Services

- ISO 9001, ISO 14001, ISO 45001, HACCP, ISO 22000, FSSC 22000, BRC GS, Halal, ISO 22716 (GMP),Organic Certification, ISO 27001, ISO 41001, ISO 37001, ISO 50001, ISO 55001, ISO 17020 & ISO 17025 etc

Training Services

- IRCA Approved Lead Auditor
- Awareness & Trainings on ISO Standards

Product Registration

- SABER, SQM, SFDA, CITC, IECEE, ECAS, EQM, RoSH, EESL, SLCP, G-Mark etc

Social Compliance

- SEDEX-SMETA, SA 8000, amfori BSCI, ISO 26001, WRAP, GRLI, ESG, CTPAT etc

Q

Qdot

The Changing Phase of Information Security

- **Traditional View**
  - The domain of a System Administrator
  - Task of Purchasing a Firewall
  - Implementing Security Controls was not a compulsion

Qdot

The Changing Phase of Information Security

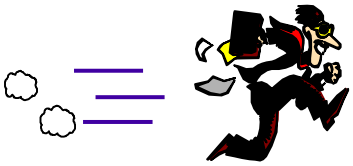
Qdot

- **Modern View**
  - The Domain of the Business Owner
  - Task of finding out what is AT RISK and finding right solutions for the same
  - Business and Security can't be separated
  - Security Team Consists of Top Management, IT Managers and a Dedicated Information Security Manager
  - Plan, Do, Check and Act Model
  - Integration of Quality Systems Like ISO, CMMI etc. with Information Security Models

SOME COMMON SECURITY CONCERNS TO INFORMATION ASSETS

Qdot

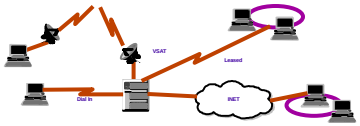
High User knowledge of IT sys.



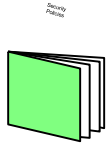
Theft , Sabotage, Misuse, Hacking

Version Control Problems

Unrestricted Access

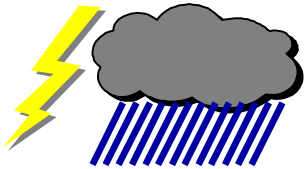


Systems / Network Failure



Lack of documentation

Virus



Natural calamities

Fire

WHY INFORMATION SECURITY?

- More and More Dependence on Information Systems
- Need for a long term and failure proof system for Securing every form of Information Asset
- Theft of Information can cause disasterous results for companies
- Companies have projects which force them to protect sensitive client information
- Projects are awarded to companies who have a sound system to protect Information
- International Laws like HIPPA and Data Protection law have set the benchmark for protecting information being stolen or tampered.

Q

Qdot

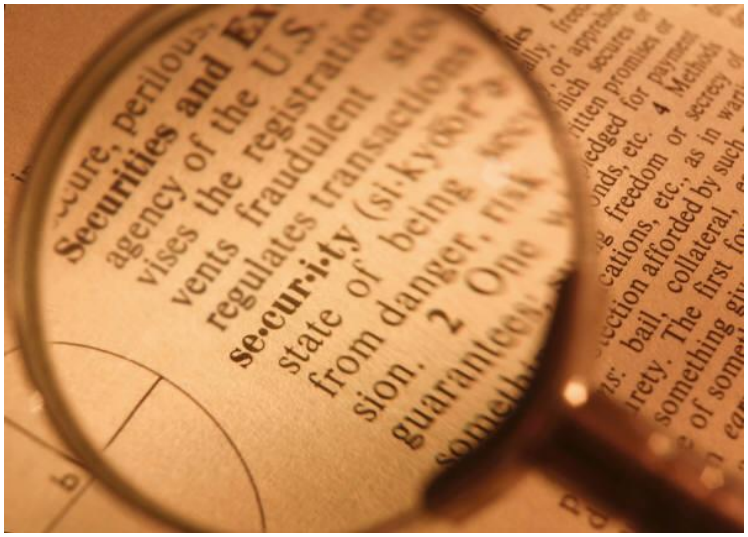
Who needs ISMS?

- Every organization which values information, needs to protect it e.g.
- Banks
- Call centers
- IT companies
- Government bodies
- Manufacturing concerns
- Hospitals
- Insurance companies

Q

Qdot

What is information?



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

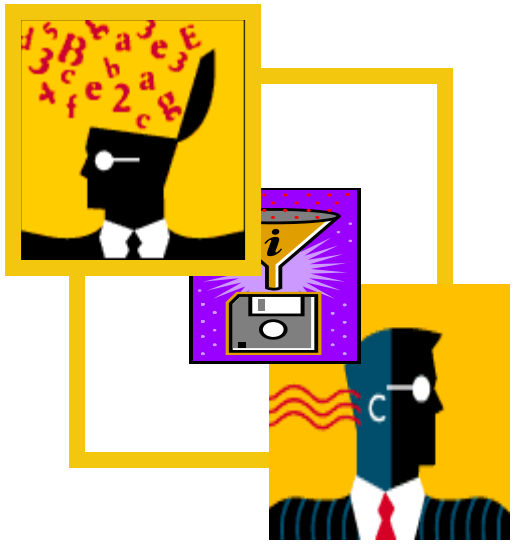
Asset: Anything that has value to the organization

Qdot

Information types

Information can be:

- Created
- Stored
- Used
- Transmitted
- Destroyed

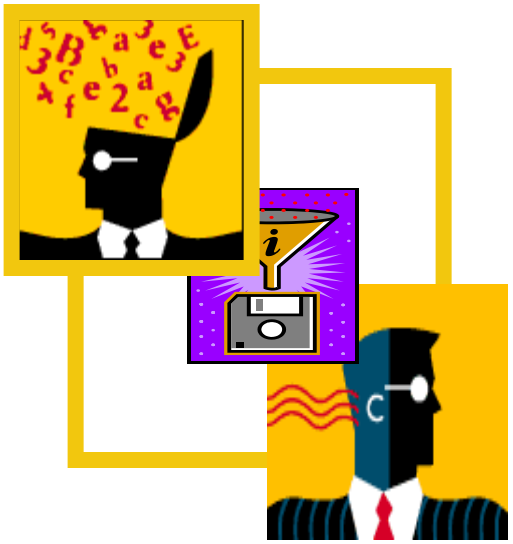


Qdot

Information types

Information format

- Paper
- Databases
- Disk(ette)s
- CD-ROMs
- Tapes
- (Design) drawings
- Films
- Conversations
- …

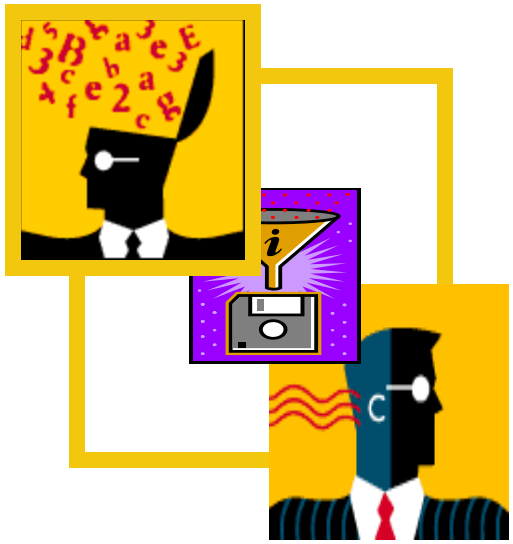


Qdot

Information types

Character of information

- Financial
- Strategic
- Operational
- Person dependent
- …



Qdot

WHAT CAN BE DONE WITH INFORMATION?

Qdot

Created

Stored

Destroyed?

Processed

Transmitted

Used - (for proper and improper purposes)

Lost!

Corrupted!

Business requirements for information security management:

- Commercial requirements
- Legal requirements
- Basic components
- Managing information boundries

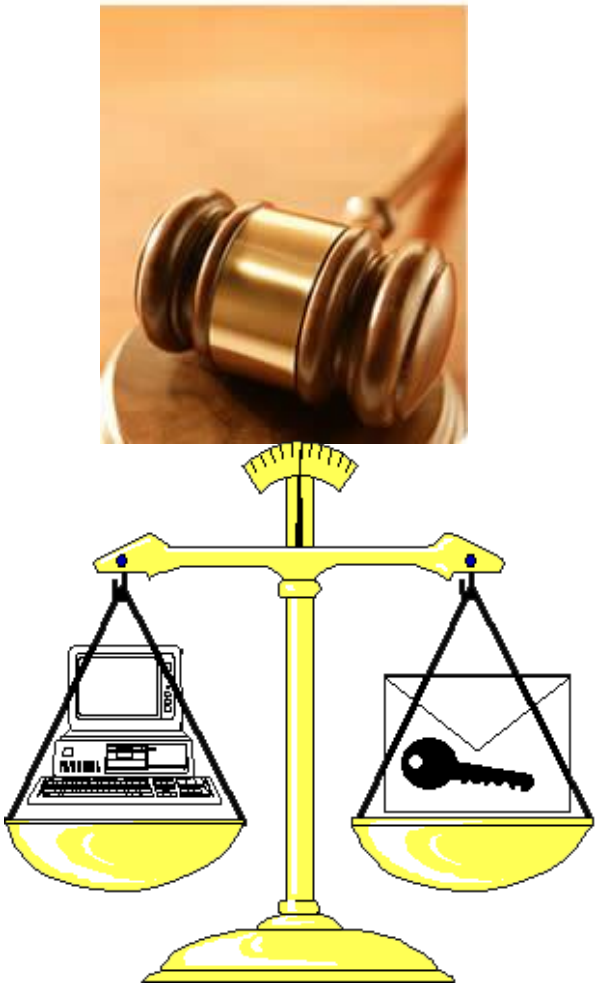
Qdot

Commercial Requirements:

Qdot

- Client / Customer / Stakeholder - requirement of contract / condition for Invitation to Tender.
- Marketing - seen as giving a competitive edge in marketing of product / service.
- Demonstration to Trading Partner of commitment to information security.
- Internal management tool - for control and confidence.

Legal Requirements:



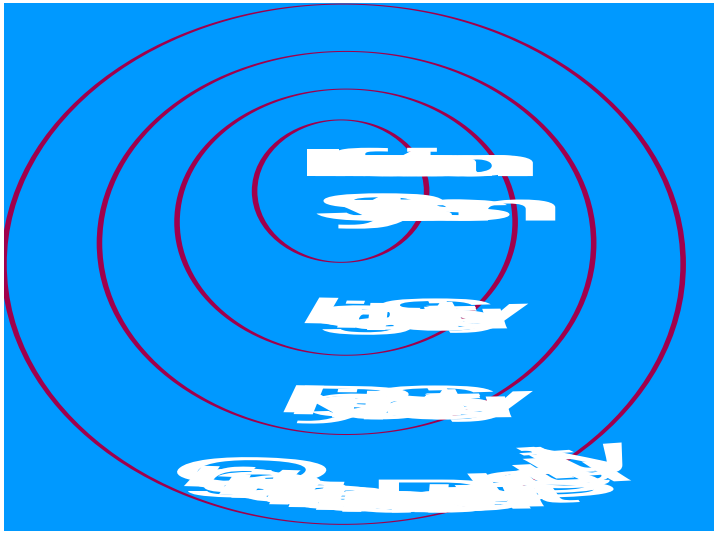
- Companies Trading Regulation
- Copyright, Designs and Patents Regulation
- Data Protection Requirements
- Computer Misuse
- Regulation of Investigatory Powers

What is information Security?

Qdot

Information Security is about protecting Information through selection of appropriate Security Controls

- ✓protects information from a range of threats
- ✓ensures business continuity
- ✓minimizes financial loss
- ✓ minimize business damage
- ✓maximizes return on investments and business opportunities



Basic components

Qdot

Confidentiality — Ensuring that information is accessible only to those authorised to have access.

Integrity — Safeguarding the accuracy and completeness of information and processing methods.

Availability — Ensuring that authorised users have access to information and associated assets when required.

Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected throughout its life cycle

Qdot

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

Managing information boundaries

Qdot

- Intranet connections to other business units,
- Extranets to business partners,
- Remote connections to staff working off-site,
- Virtual Private Networks (VPN's),
- Customer networks,
- Supplier chains,
- Service Level Agreements, contracts, outsourcing arrangements,
- Third Party access.

Information security management systems
iso 27001:2013

Q
Qdot

Preview of ISO International Organization for Standardization

Qdot

- The International Organization for Standardization widely known as ISO , is an international-standard-setting body composed of representatives from various national standards Organization.
- Founded on 23rd February 1947,
- The Organization promulgates worldwide proprietary industrial and commercial standards.
- It is headquartered in Geneva, Switzerland.
- ISO defines itself as a non-governmental organization. In practice, ISO acts as a consortium with strong links to governments.

WHY ISMS?

Q
Qdot

- **Information security that can be achieved through technical means is limited**
- **Security also depends on people, policies, processes and procedures**
- **Resources are not unlimited**
- **It is not a once off exercise, but an ongoing activity**

All these can be addressed effectively and efficiently only by establishing a proper Information Security Management System(ISMS)

What is ISO 27001?

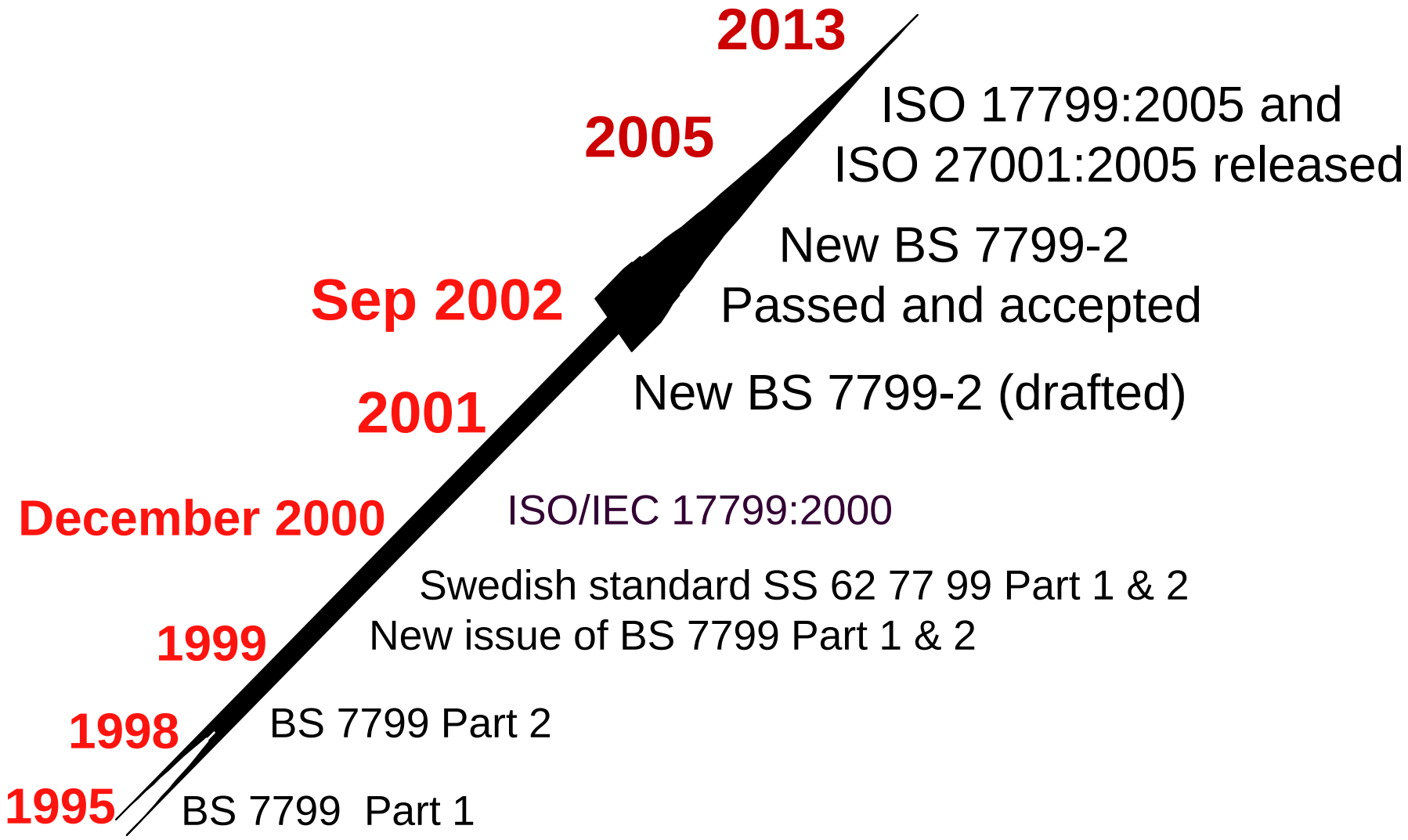
Q
Qdot

- It’s a International Standard for Information Security Management
- It consists of various Specification for information Security Management
- Code of Practice for Information Security Management
- Basis for contractual relationship
- Basis for third party certification
- Can be Certified by Certification Bodies
- Applicable to all industry Sectors
- Emphasis on prevention

History and Development of ISMS standard

(BS7799 – ISO 17799 - ISO27001)

Qdot



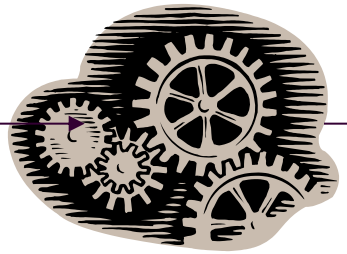
Information Security Management System (ISMS)

Qdot

- ISMS is that part of overall management system based on a business risk approach to
  - Establish
  - Implement
  - Operate
  - Monitor
  - Review
  - Maintain &
  - Improve *Information security*
- ISMS is a management assurance mechanism for security of information asset concerning its
  - availability
  - integrity and
  - Confidentiality

PROCESS FOR DEVELOPING AN ISMS

Qdot



Selection of controls (ISO/IEC 27001)

Legal Requirements

Business Requirements

Security Requirements

Risk Assessment

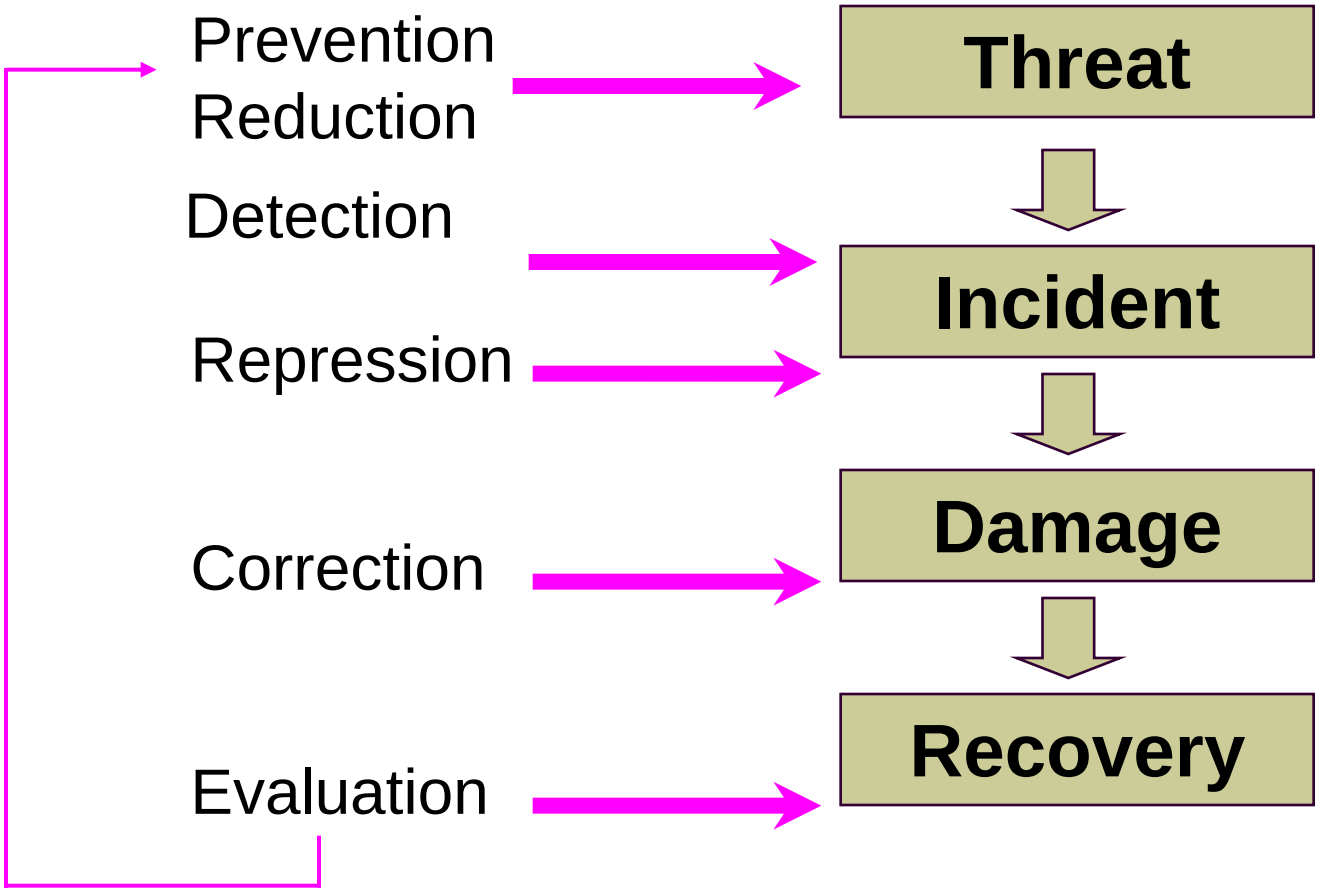
Threats & Vulnerabilities Assessment

Assets identification & valuation

Information Security Management System

Policy, Procedures & Controls

CHARACTERISTICS OF A GOOD ISMS



Qdot

ISMS STANDARDS

ISO/ IEC 27001 : 2013

- A specification (specifies requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS)
- Specifies the requirements of implementing of Security control, customised to the needs of individual organisation or part thereof.
- Used as a basis for certification

ISO/IEC 27002 : 2013

- A code of practice for Information Security management
- Provides best practice guidance
- Use as required within your business
- Not for certification

Qdot

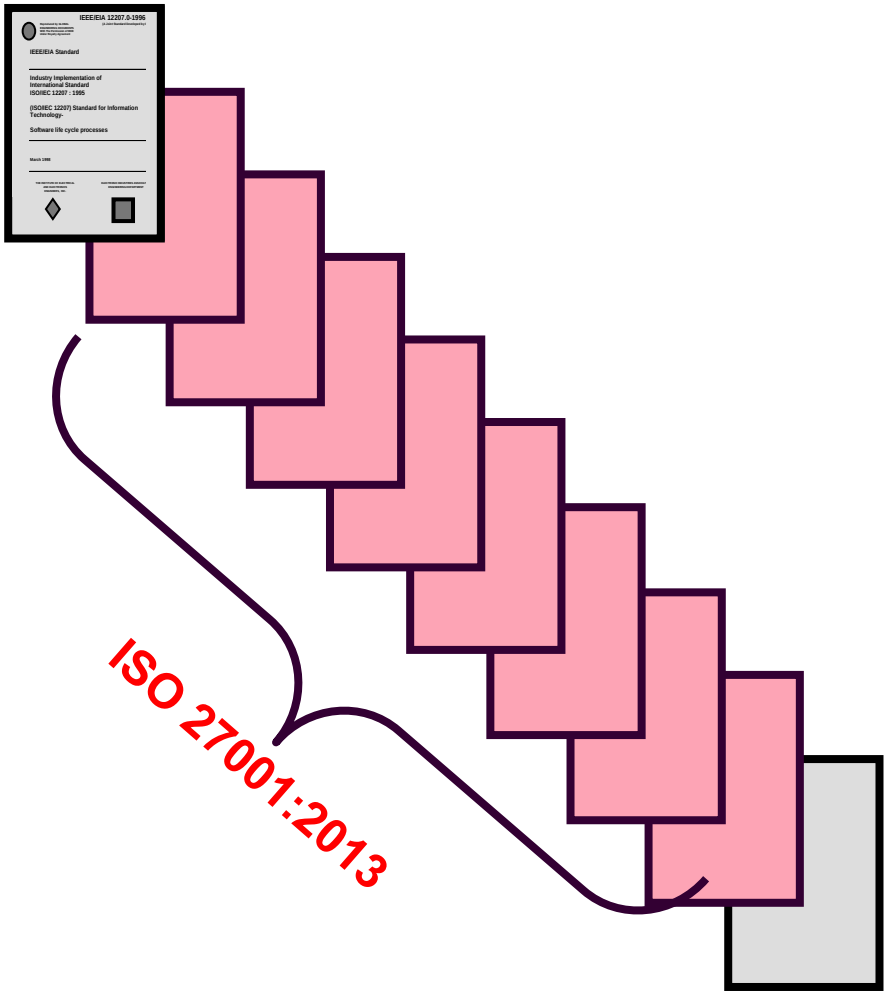
Toll Free: +971 800 QDOT9

info@qdot.ae

PLAN DO CHECK ACT CYCLE (PDCA)

Qdot

ISO 27001 Structure



0. Introduction
1. Scope
2. Normative References
3. Terms and Definitions
4. Context of Organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Annex A

Qdot

CLAUSE 1 – SCOPE

Qdot

SCOPE

- It is through the scope that you define what your Information Security Management System covers within your organization.

- The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
- Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

Q

Qdot

- CLAUSE 2 –
- NORMATIVE REFERENCES

Normative References

The following referenced document is indispensable for the application of this document.

- ISO/IEC 27000, Information technology — Security Techniques — Information security management systems – Overview and vocabulary

Q

Qdot

Clause 3 -Terms & Definitions

Qdot

Terms & Definitions

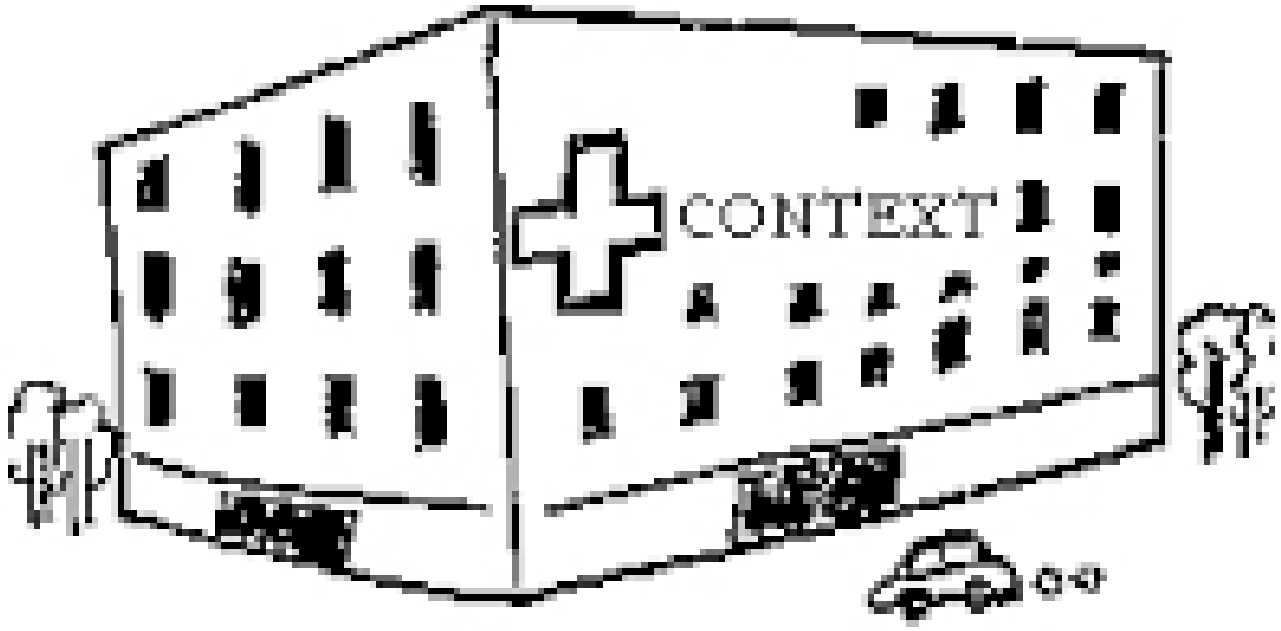
- For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

Q

Qdot

Clause 4 -Context of the Organization

Qdot



4 Context of the Organization

Qdot

4.1 Understanding the Organization & its Context

- The organization shall determine :
- external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

4.2 Understanding the needs & Expectations of Interested parties

Qdot

- The Organization shall determined.
- a) interested parties that are relevant to the information security management system; and
- b) the requirements of these interested parties relevant to information security.

NOTE: The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the Information Security Management System

Qdot

- The organization shall determine the scope of ISMS considering:
  - a) the external and internal issues referred to in 4.1;
  - b) the requirements referred to in 4.2; and
  - c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

- The scope shall be available as documented information.

4.4 Information Security Management System

Qdot

- The organization shall:
  - establish,
  - implement,
  - maintain and
  - continually improve
- an information security management system, in accordance with the requirements of this International Standard.

Clause 5 -Leadership

Qdot

Qdot

5 Leadership

Leadership & Commitment

Policy

Organizational
Roles
Responsibilities
Authorities

5 Leadership

Qdot

5.1 Leadership & Commitment

- Top Management shall demonstrate its commitment by ensuring that:

- Information Security Policy & Objectives are established.
- integration of the information security management system requirements into the
- organization's processes;
- the resources needed for the ISMS are available;
- communicating the importance of effective ISMS
- the ISMS achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the ISMS;
- promoting continual improvement

5.2 Information Security Policy

Qdot

- Top management shall establish Information Security policy
- Appropriate to the purpose of organization
- Includes information security objectives or provide frame work for setting the objectives
- Include commitment to satisfy applicable requirements
- Include commitment to improvement
- Policy shall be documented , communicated and available to interested parties as appropriate

5.3 Organization Roles, Responsibilities & Authorities

Qdot

- Top management shall ensure responsibility & authorities are assigned & communicated.
- Top management shall assign responsibility & authority for ISMS conforms to the requirement
- Processes are interact & Provide the intend output
- Reporting on the ISMS Performance

CLAUSE 6 -PLANNING

Qdot

6 Planning

Qdot

6.1 Actions to address risks & opportunities

6.1.1 General

- Organization shall consider 4.1 & 4.2 when planning
- Determine risks & Opportunities that need to be addressed
- Assure ISMS can achieve its intend outcomes
- Prevent & reduce undesired effect
- Achieve improvement

- The organization shall plan
- 1. actions to address these risks and opportunities, and
- 2. how to
- integrate and implement these actions into its ISMS processes; and
- evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

- The organization shall define an information security risk assessment process that:

a) establishes and maintains information security risk criteria, including the risk acceptance criteria;

b) determines the criteria for performing information security risk assessments; and

c) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

- The organization shall:
- d) Identify the information security risks.

1) Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS.

2) Identify the risk owners.

6.1.2 Information security risk assessment (contd….)

Qdot

- The organization shall:
- e) Analyze the information security risks.
  - 1) Assess the potential consequences that would result if the risks identified in 6.1.1 e) 1) were to materialize.
  - 2) Assess the realistic likelihood of the occurrence of the risks identified in 6.1.1 e) 1).
  - 3) Determine the levels of risk.
- f) Evaluate the information security risks.
  - 1) Compare the analyzed risks with the risk criteria established in 6.1.2 a) and establish priorities for treatment.

The organization shall retain documented information about the information security risk assessment process.

Qdot

6.1.3 Information security risk treatment

- The organization shall apply an information security risk treatment process to:
- a) select appropriate information security risk treatment options, taking account of the risk assessment results;
- b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
- c) compare the controls determined with those in Annex A and verify that no necessary controls have been omitted;
- d) produce a Statement of Applicability that contains the necessary controls and justification for inclusions/exclusion,
- e) formulate an information security risk treatment plan;
- f) obtain risk owner's approval of the information security risk treatment plan and the acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process

Qdot

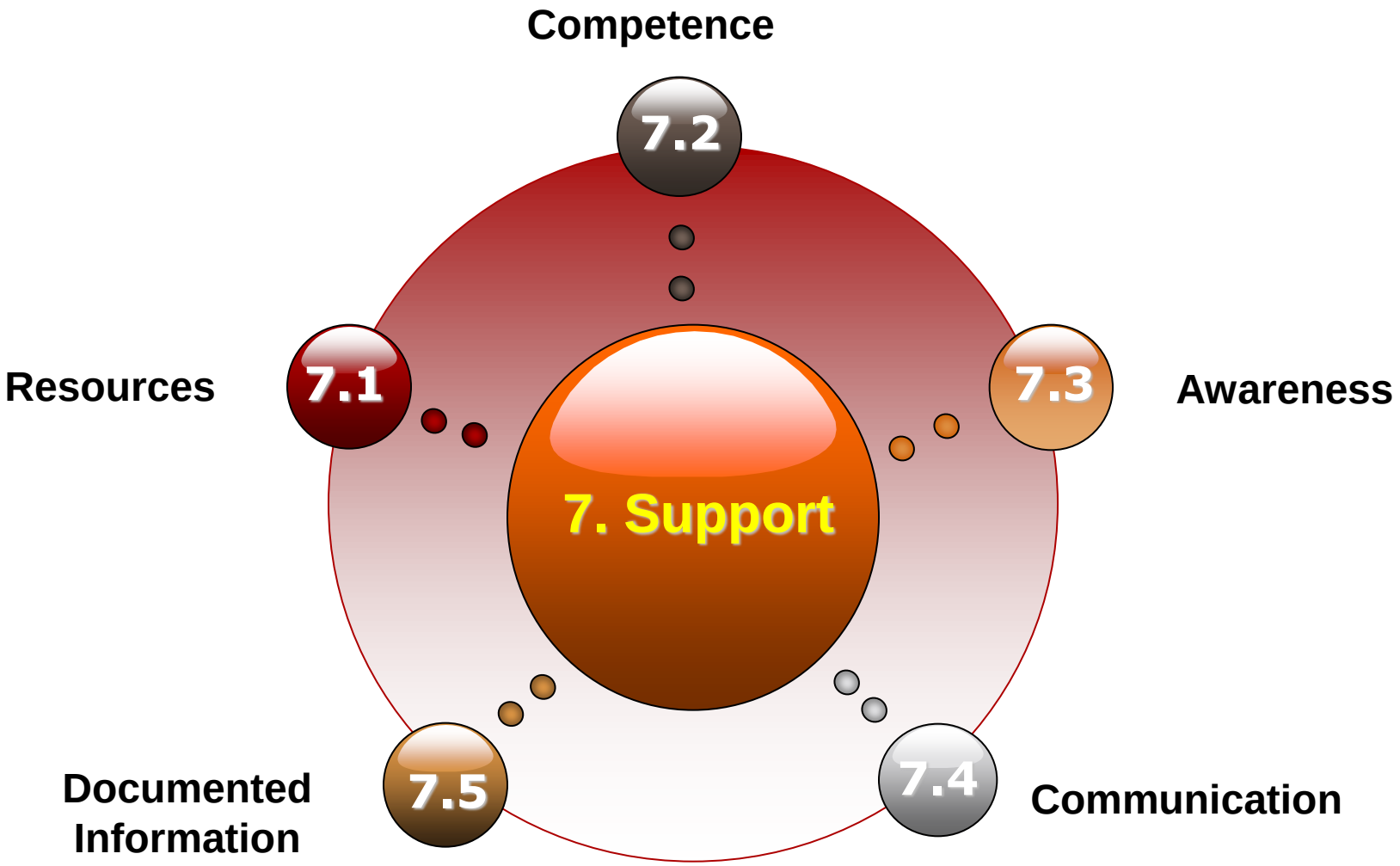
6.2 Information Security Objectives & Planning to Achieve them:

- The Organization shall establish Information Security Objectives
- take into account applicable information security requirements, and risk assessment and treatment results;
- Consistent with IS Policy, Measurable, documented, communicated and updated as required

- Planning to achieve shall include, what, how, who, when, etc.

Clause 7 -Support

Qdot


Competence
7.2
Resources
7.1
7.3
Awareness
7. Support
Documented Information
7.5
7.4
Communication

7.1 Resources

The organization shall determine and provide the resources needed for the:

- establishment,
- implementation,
- Maintenance, and
- continual improvement of the information security management system.

Q

Qdot

7.2 Competence

- Determine competence and ensure persons are competent
  - based on appropriate education,
  - training or experience

- Where required, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

- retain appropriate documented information as evidence of competence

Qdot

7.3 Awareness

Persons doing work under control of organization shall be aware of:

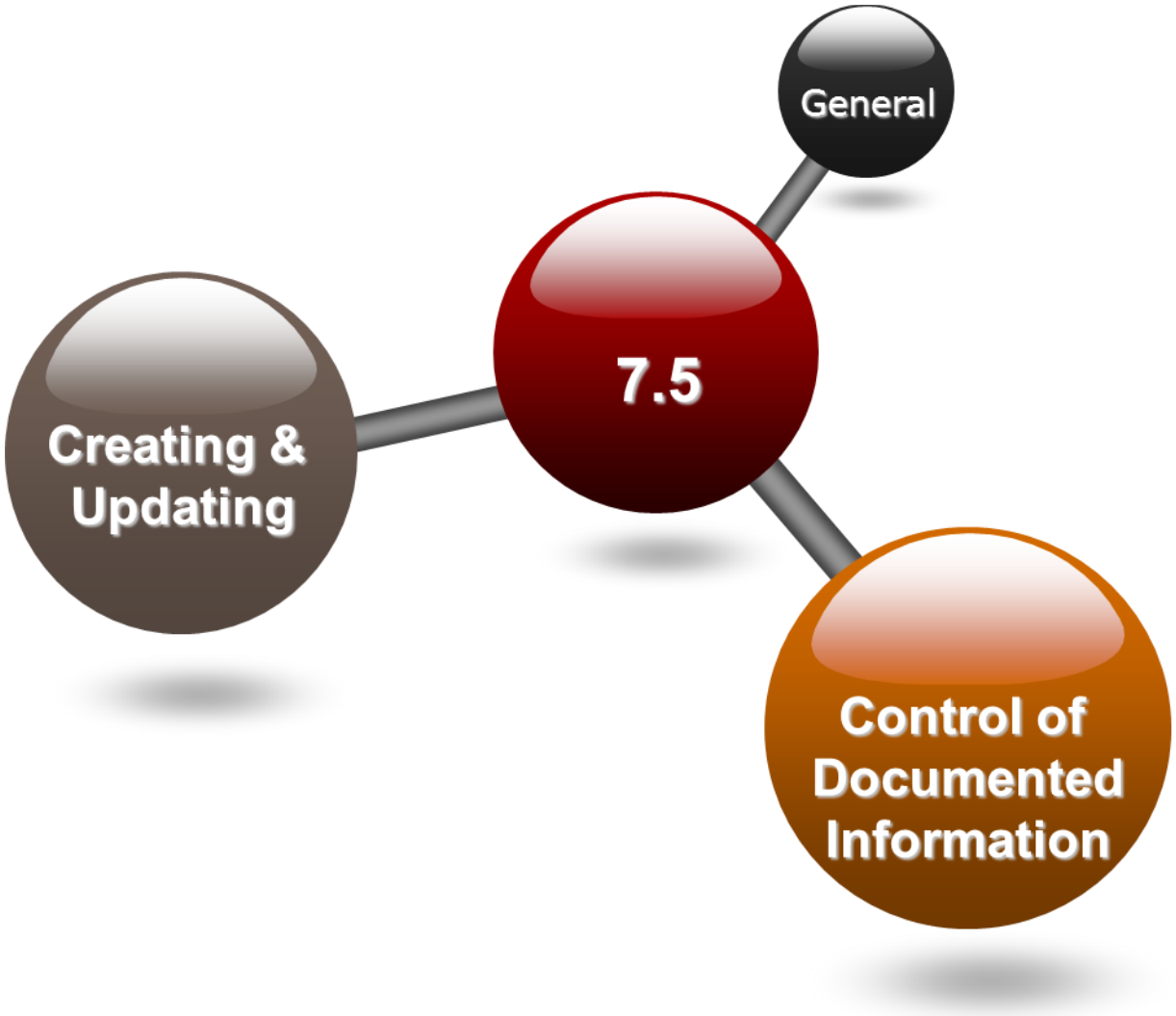
- Information Security Policy
- Their contribution of the effective management system
- The implication of not conforming with I

7.4 Communication

Qdot

- The Organization shall determine the Internal & External Communications relevant to Information Security Management System:

  - a) on what to communicate;
  - b) when to communicate;
  - c) with whom to communicate;
  - d) who communicates.
  - e) how to communicate;


General
7.5
Creating & Updating
Control of Documented Information

Q
Qdot

Qdot

7.5 Documented Information

- Document Information shall be maintained by considering
  - Requirements of this International Standard
  - Requirements of the organization

7.5 Documented Information

Qdot

TYPICAL ISMS DOCUMENT CLASSIFICATION

Security Policy Manual

- Summary of management framework including the information security policy and the control objectives and implemented controls given in the statement of applicability.

Procedures

- Procedures adopted to implement the controls required.

Operational Documents

- Explains details of specific tasks or activities.

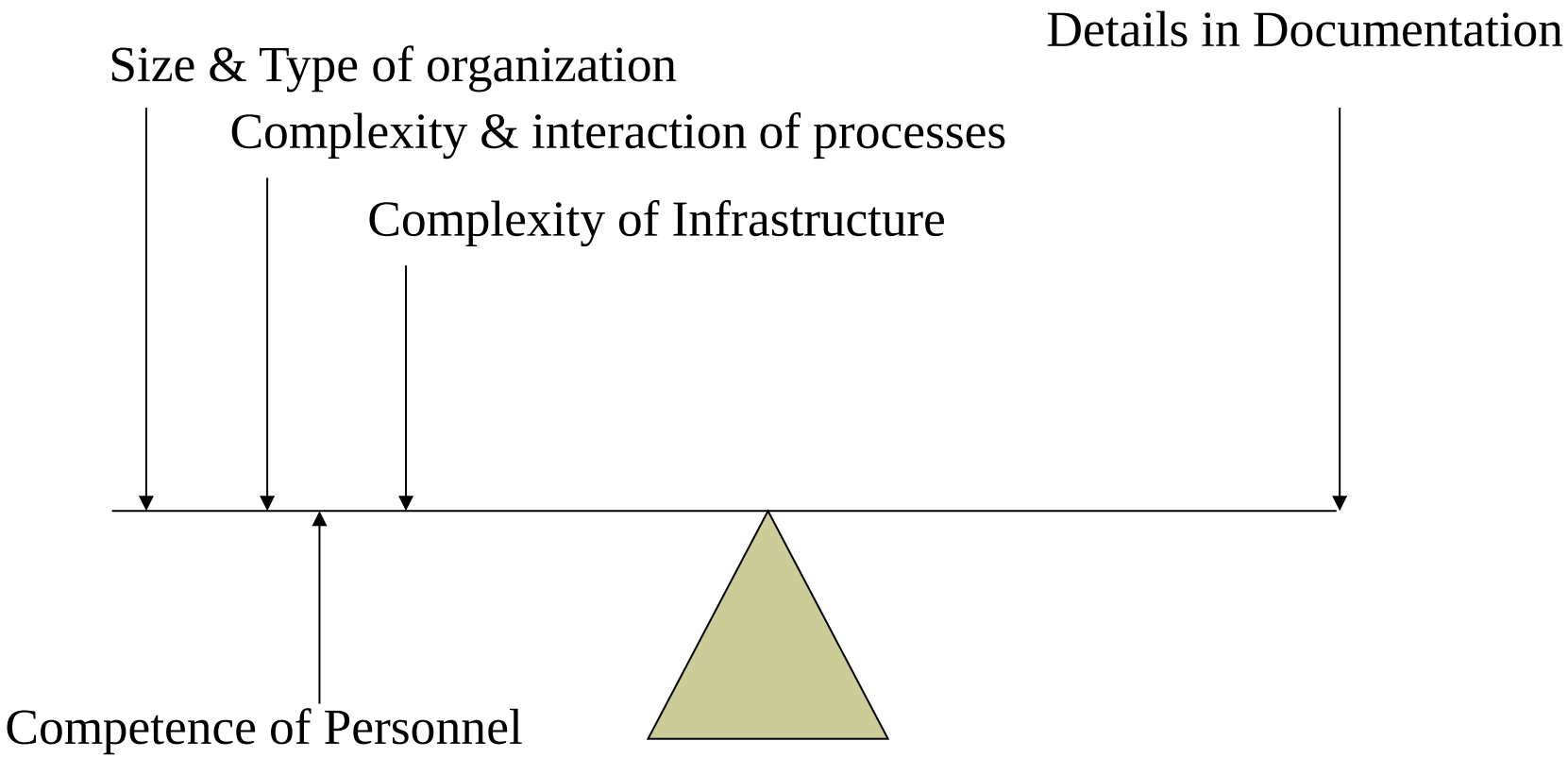
Records

- Evidence of activities carried out.

7.5 DOCUMENTED INFORMATION

Qdot

extent of documentation



7.5 Documented Information

Qdot

- Creating & Updating
- The organization shall ensure appropriate:
- a) identification and description (e.g. a title, date, author, or reference number);
- b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
- c) review and approval for suitability and adequacy.

7.5 Documented Information

Qdot

- Control of Documented Information

Documented Information shall be controlled:

a) available and suitable for use,

b) adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

- c) distribution, access, retrieval and use;
- d) storage and preservation, preservation of legibility;
- e) control of changes (e.g. version control); and
- f) retention and disposition.

Clause 8 -Operation

Qdot

8.1 – Operational Planning And Control

Qdot

- The organization shall :

- plan, implement and control the processes needed to meet information security requirements
- implement plans to achieve information security objectives
- maintain documented information to the extent necessary to have confidence that the processes have been carried out as planned
- control planned changes and review the consequences of unintended changes

8.2 – Information security risk assessment

Qdot

- The organization shall :

- perform information security risk assessments at planned intervals or when significant changes are there

- retain documented information of the results of the information security risk assessments

8.3 – Information security risk treatment

Qdot

- The organization shall :
  - implement the information security risk treatment plan
  - retain documented information of the results of the information security risk treatment

CLAUSE 9 -PERFORMANCE EVALUATION

Qdot

9.1 – Monitoring, measurement, analysis and evaluation

Qdot

- The organization shall determine :
  - what needs to be monitored and measured
  - the methods for monitoring, measurement, analysis and evaluation
  - when the monitoring and measuring shall be performed
  - who shall monitor and measure
  - when the results from monitoring and measurement shall be analyzed
  - who shall analyze and evaluate these results, and
  - retain appropriate documented information as evidence of the monitoring and measurement results

9.2 – Internal Audit

Qdot

- The organization shall conduct internal audits at planned intervals to ensure that ISMS:
- a) conforms to
  - the organization's own requirements for its information security management system; and
  - the requirements of this International Standard;
- b) is effectively implemented and maintained.

9.2 – Internal Audit

Qdot

- a- Plan, Establish, Maintain with defined Frequency, method, responsibilities, reporting
- b- Define the criteria and scope
- c- Use of Independent Auditors
- d- Reporting of Results to Management
- e- Taking Actions Without Undue Delay
- f- Maintain and Retain Documented Information

9.3 Management Review

Qdot

- Top management shall review the organization's information security management system, at planned intervals ,to ensure its continuing suitability, adequacy, effectiveness.

9.3 Management Review

Qdot

- The management review shall include:
- a) the status of actions from previous management reviews;
- b) changes in external and internal issues relevant to ISMS
- c) feedback on the IS performance, including trends in:
  - 1) nonconformities and corrective actions;
  - 2) monitoring and measurement results;
  - 3) audit results; and
  - 4) fulfillment of information security objectives;
- d) feedback from interested parties;
- e) results of risk assessment and status of risk treatment plan;
- f) opportunities for continual improvement.

9.3 Management Review

Qdot

- The outputs of the management review shall include:

  - decisions related to continual improvement opportunities,
  - any needs for changes to the information security management system.

- The organization shall retain documented information as evidence of the results of management reviews.

Clause 10-Improvement

Qdot

10.1 Nonconformity and Corrective Action

Qdot

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it; and

2) deal with the

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the information security management system,

- The organization shall retain documented information.

Qdot

10.2 Continual Improvement

- The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Annex A-Control Objective and Controls

Qdot

Annex A Consist of:

»14 Control Area : Core topic areas that Covered Most Aspects of Information Security

» 34 Control Objective : Objectives of Control

» 114 Control : Applicable Controls to be Implemented on ISMS Program

Annex A- Control areas

Qdot

A.5: Information Security Policies

Manage and Update of Organization Information Security Policies

A.6: Organization of Information Security

Manage of Organization Information including: Identified Role and Responsibilities, Segregation of Duties, Mobile Devices and teleworking

A.7: Human resources security

Manage of Organization Human Resource including: During, prior Employment Relationship

A.8: Asset management

Manage of Organization Assets

A.9: Access Control

Manage and Control Access of Organization Information

Annex A- Control areas

Qdot

A.10: Cryptographic

Control of Using Cryptographic inside Organization

A.11: Physical and environmental Security

Manage and Control of Organization Physical and environmental Access

A.12: Operations security

Manage and control all Operation security including : Operational Procedure and Responsibilities , logging and Monitoring , Technical vulnerability management and information systems audit

A.13: Communications Security

Manage and control Organization Communication Security including: Network security management and information transfer Controls

Annex A- Control areas

Qdot

A.14: System acquisition, development, and maintenance

Manage and control System Development Cycle Including: identified and enforce security requirements, Secure of development system

A.15: Supplier Relationship

Manager suppliers relationship including : apply information security for supplier relationship and service

delivery management

A.16: Information Security Incident management

Manage information security incident

Annex A- Control areas

Qdot

A.17: Information Security aspects of Business Continuity Management

Manage information security Continuity and Redundancies

A.18: Compliance

Manage organization compliance with legal and contractual requirements

Annex A-Control Objective and Controls

Qdot

A12	Operations security	14
A8	Asset management	10
A16	Information Security Incident management	7
A6	Organization of Information Security	7
A14	System acquisition, development, and maintenance	13
A10	Cryptographic	2
A18	Compliance	8
A5	Information Security Policies	2
A13	Communications Security	7
A9	Access Control	14
A17	Information Security aspects of Business Continuity	4
A7	Human resources security	6
A15	Supplier Relationship	5
A11	Physical and environmental Security	15

Qdot

1. Security Policy

- Objective:
  - Information security policy.
- Covers:
  - Information security policy document
  - Review of Informational Security Policy

1. Security Policy

Tech Mahindra Security
Document Library

Current Location
- Home
- BMS
- Capability and Support
- Tech Mahindra Security

Select a View
- All Documents
- Explorer View

Actions
- Add to My Links
- Alert me
- Export to spreadsheet
- Modify settings and columns

New Document | Upload Document | New Folder | Filter | Edit in Datasheet

Type	Name	Ref. Id	Version	Created On
	TML Security Function Manual	IS000	1.0	5/14/2004
	Incident Management Procedure	IS001	1.1	1/25/2005
	User Guidelines	IS003	1.0	12/27/2004
	MIS Template IDU information	IS004A	1.0	2/6/2006
	MIS Template TIM - Central Services	IS004B	1.0	2/6/2006
	MIS Template TIM - Operations	IS004C	1.0	2/6/2006
	Anti-Virus Policy	IS00B	1.0	7/1/2004
	Compliance Policy	IS00C	1.0	7/1/2004
	Desktop Security Policy	IS00D	1.0	7/1/2004
	Email Security Policy	IS00E	1.0	7/1/2004
	Application Security Policy	IS00F	2.0	12/27/2004
	Incident Management Policy	IS00G	1.0	8/5/2004
	Information and Asset Classification Policy	IS00H	1.0	7/1/2004
	Internet Usage Policy	IS00I	1.0	7/1/2004
	Laptop Security Policy	IS00J	1.0	7/1/2004
	Logical Access Management Policy	IS00K	1.0	7/1/2004
	Equipment and Media Handling Policy	IS00L	1.2	2/6/2006
	Third Party Agreement	IS00M	1.0	8/5/2004
	Guidelines for Third Party Agreement Policy	IS00M3	1.0	8/5/2004
	Network Security Policy	IS00N	1.0	7/1/2004
	Security Monitoring Policy	IS00O	1.0	7/1/2004
	Personnel Security Policy	IS00P	1.0	8/5/2004
	Physical Security Policy	IS00Q	1.0	5/13/2004
	Server Security Policy	IS00R	1.0	7/1/2004
	System Development and Maintenance Policy	IS00S	1.0	8/5/2004
	Malicious Code Security Policy	IS00T	1.0	12/27/2004
	Acceptable Usage Policy	IS00U	1.0	2/6/2006
	Visitor Escort and Access Control Policy	IS00V	1.0	3/31/2006
	Bomb Threat Procedure	IS00W	1.0	7/21/2006

2. Organization of information security

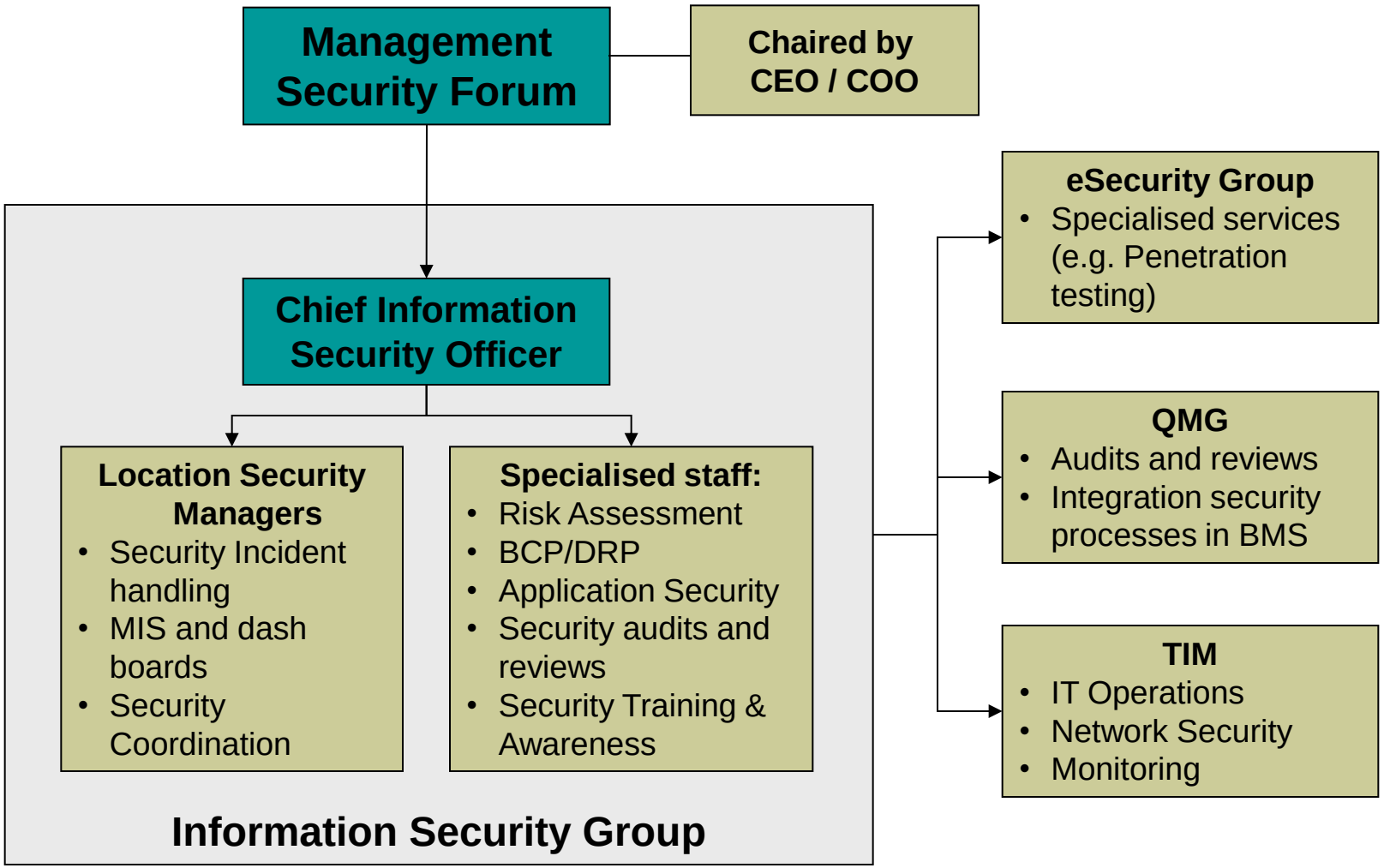
Qdot

- Objective:
  - Internal Organization
  - External Parties

- Covers:
  - Management commitment to information security
  - Information security coordination
  - Allocation of information security responsibilities
  - Authorization process for information processing facilities
  - Confidentiality agreements
  - Contact with authorities
  - Contact with special interest groups
  - Independent review of information security
  - Identification of risks related to external parties
  - Addressing security when dealing with customers
  - Addressing Security in third party agreements

2. Organization of information security - Example

Qdot



3. Asset Management

Qdot

- Objective:
  - Responsibility for assets
  - Information classification
- Covers:
  - Inventory of assets
  - Ownership of assets
  - Acceptable use of assets
  - Classification guidelines
  - Information labelling and handling

Information Asset

Qdot

- Inventory of Information Assets are categorized & classified as below

Sr	Asset Category	Classification
1	Paper Assets	Client Confidential
2	Electronic Data	Company Confidential
3	Hardware	Commercial in Confidence
4	Software	Restricted
5	People	Critical & Non Critical

- Valuation of Information Assets – Scale
  - Very High, High ,Medium ,Low , Negligible

- Other Attributes of Inventory
  - Asset Group, Asset Classification, Value, Storage Area, Storage location ,
  - Asset Owner, Asset Retention, Remarks

4. Human Resource Security

Qdot

- Objective:
  - Prior to employment
  - During employment
  - Termination or change of employment

- Covers:
  - Roles and responsibilities
  - Screening
  - Terms and conditions of employment
  - Management responsibilities
  - Information security awareness, education and training
  - Disciplinary process
  - Termination responsibilities
  - Return of assets
  - Removal of access rights

5. Physical and Environmental Security

Qdot

- Objective:
  - Secure Areas
  - Equipment Security

- Covers:
  - Physical Security Perimeter
  - Physical entry Controls
  - Securing Offices, rooms and facilities
  - Protecting against external and environmental threats
  - Working in Secure Areas
  - Public access delivery and loading areas
  - Cabling Security
  - Equipment Maintenance
  - Securing of equipment off-premises
  - Secure disposal or re-use of equipment
  - Removal of property

6. Communications & Operations Management

Qdot

- Objective:
  - Operational Procedures and responsibilities
  - Third party service delivery management
  - System planning and acceptance
  - Protection against malicious and mobile code
  - Backup
  - Network Security Management
  - Media handling
  - Exchange of Information
  - Electronic Commerce Services
  - Monitoring
- Covers:
  - Documented Operating procedures
  - Change management
  - Segregation of duties

6. Communications & Operations Management (contd..)

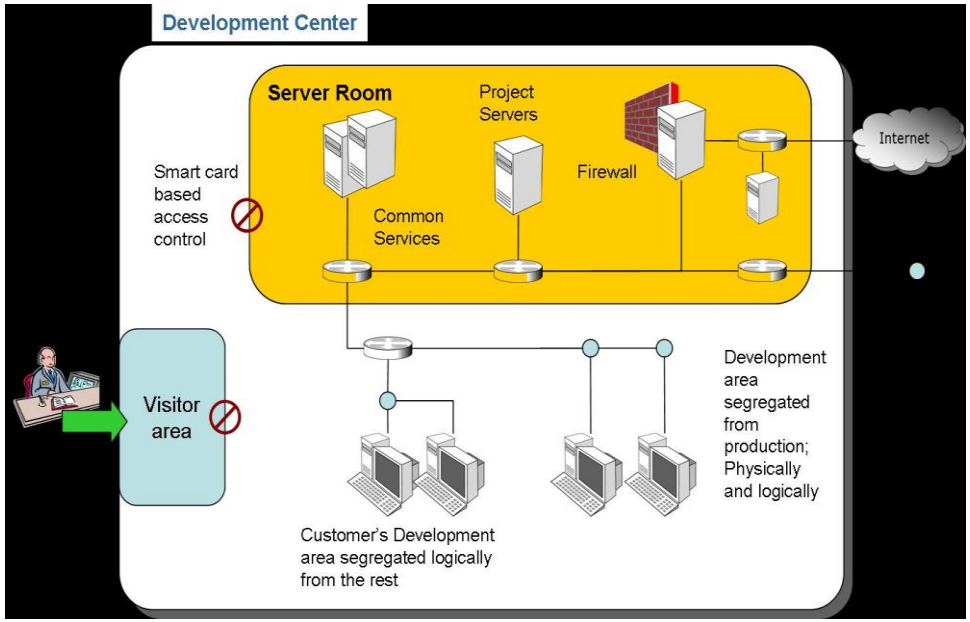
Qdot

- Separation of development, test and operational facilities
- Service delivery
- Monitoring and review of third party services
- Managing changes to third party services
- Capacity Management
- System acceptance
- Controls against malicious code
- Controls against mobile code
- Information backup
- Network Controls
- Security of network services
- Management of removable media
- Disposal of Media
- Information handling procedures
- Security of system documentation
- Information exchange policies and procedures
- Exchange agreements

6. Communications & Operations Management (contd..)

Qdot

- Exchange agreements
- Electronic Messaging
- Business information systems
- Electronic Commerce
- On-Line Transactions
- Publicly available information
- Audit logging
- Monitoring system use
- Protection of log information
- Administrator and operator logs
- Fault logging
- Clock synchronisation



7. ACCESS CONTROLS

Qdot

- Objective:
  - Business Requirement for Access Control
  - User Access Management
  - User Responsibilities
  - Network Access Control
  - Operating system access control
  - Application and Information Access Control
  - Mobile Computing and teleworking

- Covers:
  - Access Control Policy
  - User Registration
  - Privilege Management
  - User Password Management
  - Review of user access rights
  - Password use

7. Access Controls (contd..)

Qdot

- Unattended user equipment
- Clear desk and clear screen policy
- Policy on use of network services
- User authentication for external connections
- Equipment identification in networks
- Remote diagnostic and configuration port protection
- Segregation in networks
- Network connection control
- Network routing control
- Secure log-on procedures
- User identification and authentication
- Password management system
- Use of system utilities
- Session time-out
- Limitation of connection time
- Information access restriction
- Sensitive system isolation
- Mobile computing and communications
- Teleworking

8. Information systems acquisition, development and maintenance

Qdot

- Objective:
  - Security requirements of information systems
  - Correct processing in applications
  - Cryptographic controls
  - Security of system files
  - Security in development and support processes
  - Technical Vulnerability Management

- Covers:
  - Security requirements analysis and specification
  - Input data validation
  - Control of internal processing
  - Message integrity
  - Output data validation
  - Policy on use of cryptographic controls
  - Key management
  - Control of operational software
  - Protection of system test data

8. Information systems acquisition, development and maintenance (contd)

Qdot

- Access Control to program source code
- Change control procedures
- Technical review of applications after operating system changes
- Restriction on changes to software packages
- Information leakage
- Outsourced software development
- Control of technical vulnerabilities

9. Information Security Incident Management

Qdot

- Objective:
  - Reporting information security events and weaknesses
  - Management of information security incidents and improvements
- Covers:
  - Reporting information security events
  - Reporting security weaknesses
  - Responsibilities and procedures
  - Learning from information security incidents
  - Collection of evidence

10. Business Continuity Management

Qdot

- Objective:
  - Information security aspects of business continuity management

- Covers:
  - Including information security in the business continuity management process
  - Business continuity and risk assessment
  - Developing and implementing continuity plans in information security
  - Business continuity planning framework
  - Testing, maintaining and re-assessing business continuity plans

11. Compliance

Qdot

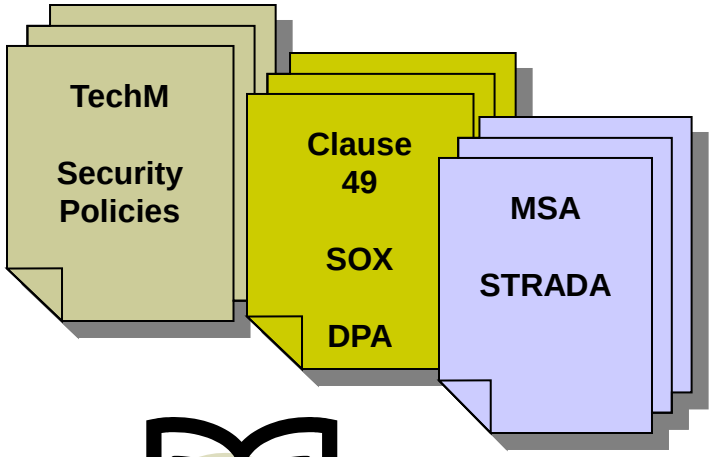
- Objective
  - Compliance with legal requirements
  - Compliance with security policies and standards, and technical compliance
  - Information Systems audit considerations

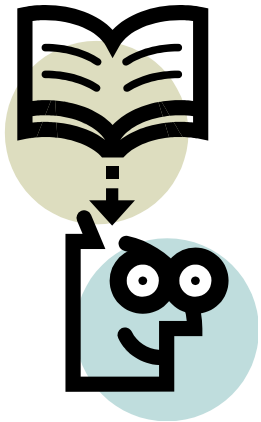
- Covers:
  - Identification of applicable legislation
  - Intellectual property rights (IPR)
  - Protection of organizational records
  - Data protection and privacy of personal information
  - Prevention of misuse of information processing facilities
  - Regulation of cryptographic controls
  - Compliance with security policies and standards
  - Technical compliance checking
  - Information systems audit controls
  - Protection of information system audit tools

Compliance Management

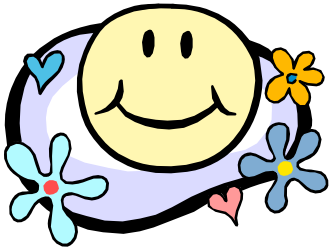
Qdot

- Tech M policies
- Regulatory concerns
- Contractual requirements
- Distribution and awareness
- Enforcement
  - Deterrence
  - Technology means





Qdot



Thank You!!

Contact us:

www.qdot.ae, info@qdot.ae
Toll Free: +971 800 QDOT9
Call / Whatsapp: +971 800 QDOT9, +971 50 133 5432

Qdot

Dubai (Head Office)

Office 16, 6th Floor, Business Village-B,
Clocktower Roundabout, Deira, Dubai, UAE.
info@qdot.ae
+971 800 QDOT9 (73689)
+971 56 502 1526

Qatar (Regional Office)

Quality Dot International Consultancy QFZ LLC
Office 62, Ras Bufontas Admin Building
Building 43, Street 517, Zone 49 Ras Bufontas
Free Zone, Doha Qatar
info@qdot.ae
+974 5560 2152

KSA Office

Fatima Tul Zahra Street, District Jarir, Riyadh
12837-4139, Kingdom of Saudi Arabia.
info@qdot.ae
+966 57 236 5783

Oman Office

info@qdot.ae
+971 800 QDOT9 (73689)

Kuwait Office

info@qdot.ae
+971 800 QDOT9 (73689)

Bahrain Office

info@qdot.ae
+971 800 QDOT9 (73689)

Pakistan (Regional Office)

info@qdot.ae
+92 304 0749364

USA Office

info@qdot.ae
+971 800 QDOT9 (73689)

UK Office

info@qdot.ae
+971 800 QDOT9 (73689)