ISO 27799: Security management in health using ISO/IEC 17799

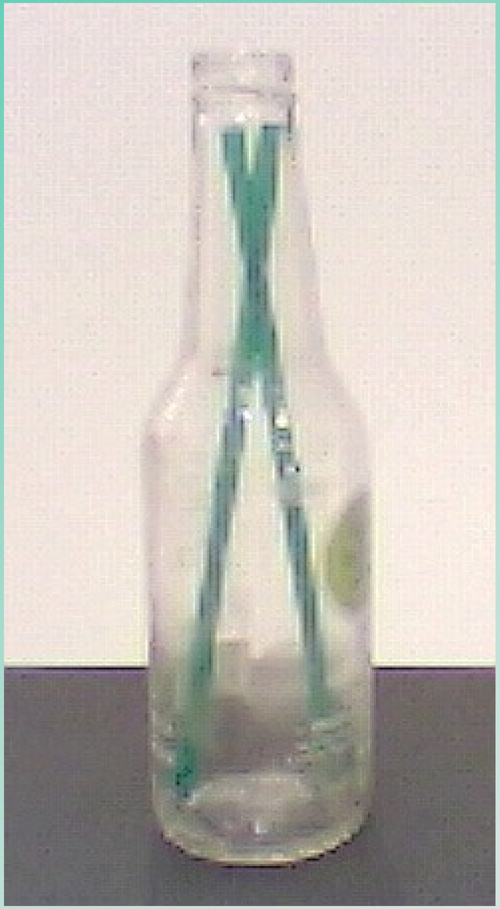
CIHI Partnership Conference
June 6, 2006

Ross Fraser
International Convenor of the ISO health informatics security working group (TC215 WG4)

Agenda

- Information Security Mgmt:
  - Need for standards
  - Goals and context
  - Threats, Vulnerabilities, Risks
- ISO 27799 – Security management in health using ISO 17799
  - Rationale, history and structure of 17799
  - Rationale, history and structure of 27799
  - Structure of 27799
- Questions

Need for standards

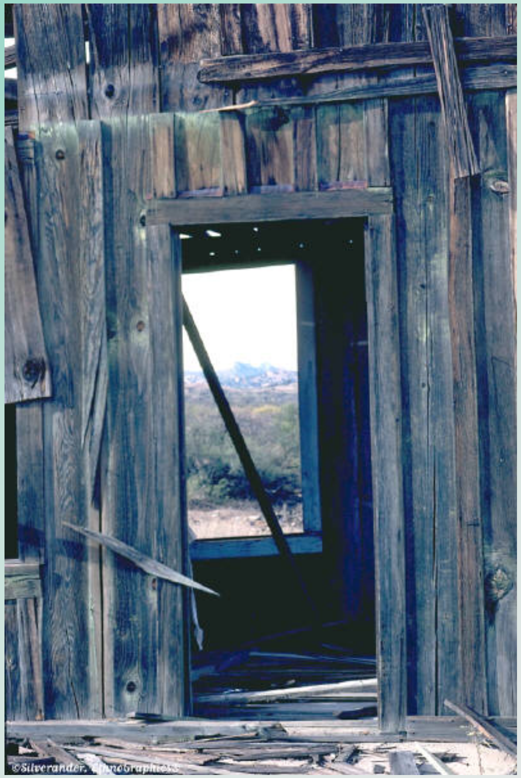


Canadian drinking straw
in a US soft drink bottle

Need for security standards

Front Door

Side Door



©Silverander, Cinnographics

Back Door

Need for e-health

2006 World Congress on Information Technology, Austin Texas
CNET News.com, Published: May 4, 2006

“Around 90,000 people died in the U.S. last year [2005] as the result of medical errors caused by fatigue or sloppiness that could have been prevented with better technology.”

Tommy Thompson
Former secretary of Health and Human Services

"The reality is that a good many of the problems have to do with lack of coordination between one system or another," she said. Records kept by one doctor won't necessarily show up in a different doctor's record-keeping system, never mind across different countries.”

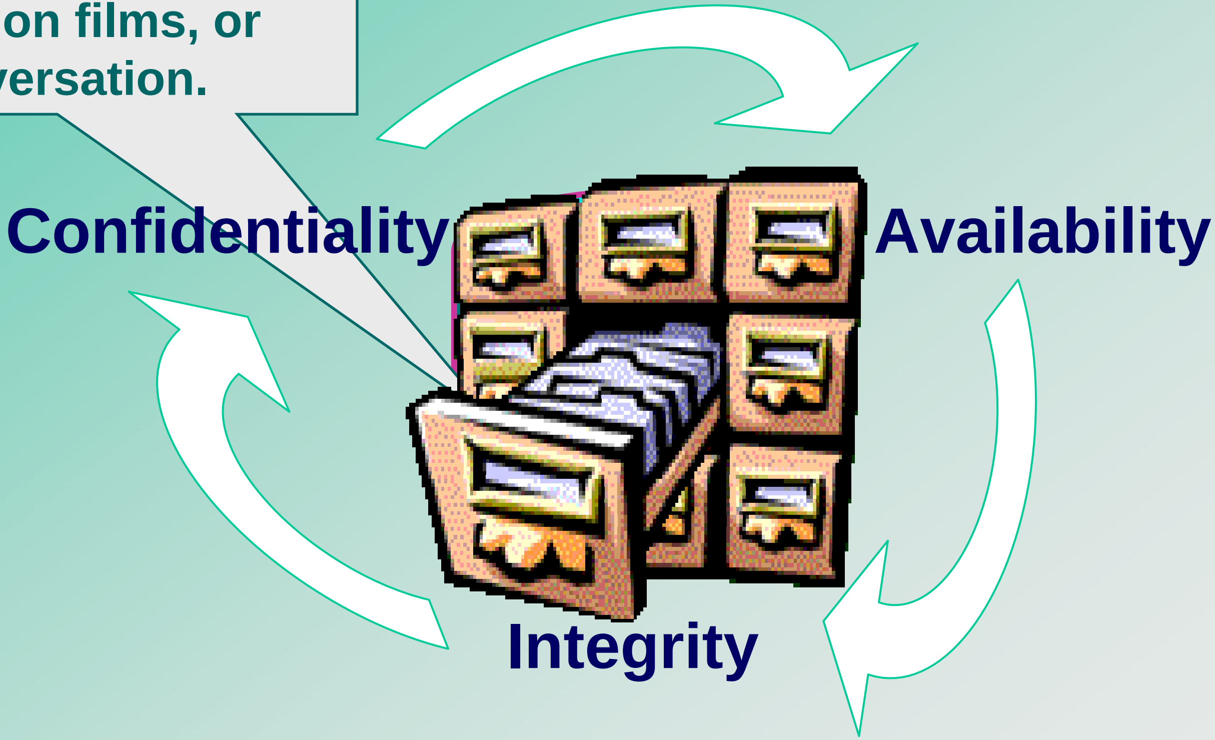
Karen Bell
Acting Deputy, US Office of the National Coordinator for Health Information Technology

"Anybody who waits for the standards bodies before implementing e-health will be waiting a long time,“

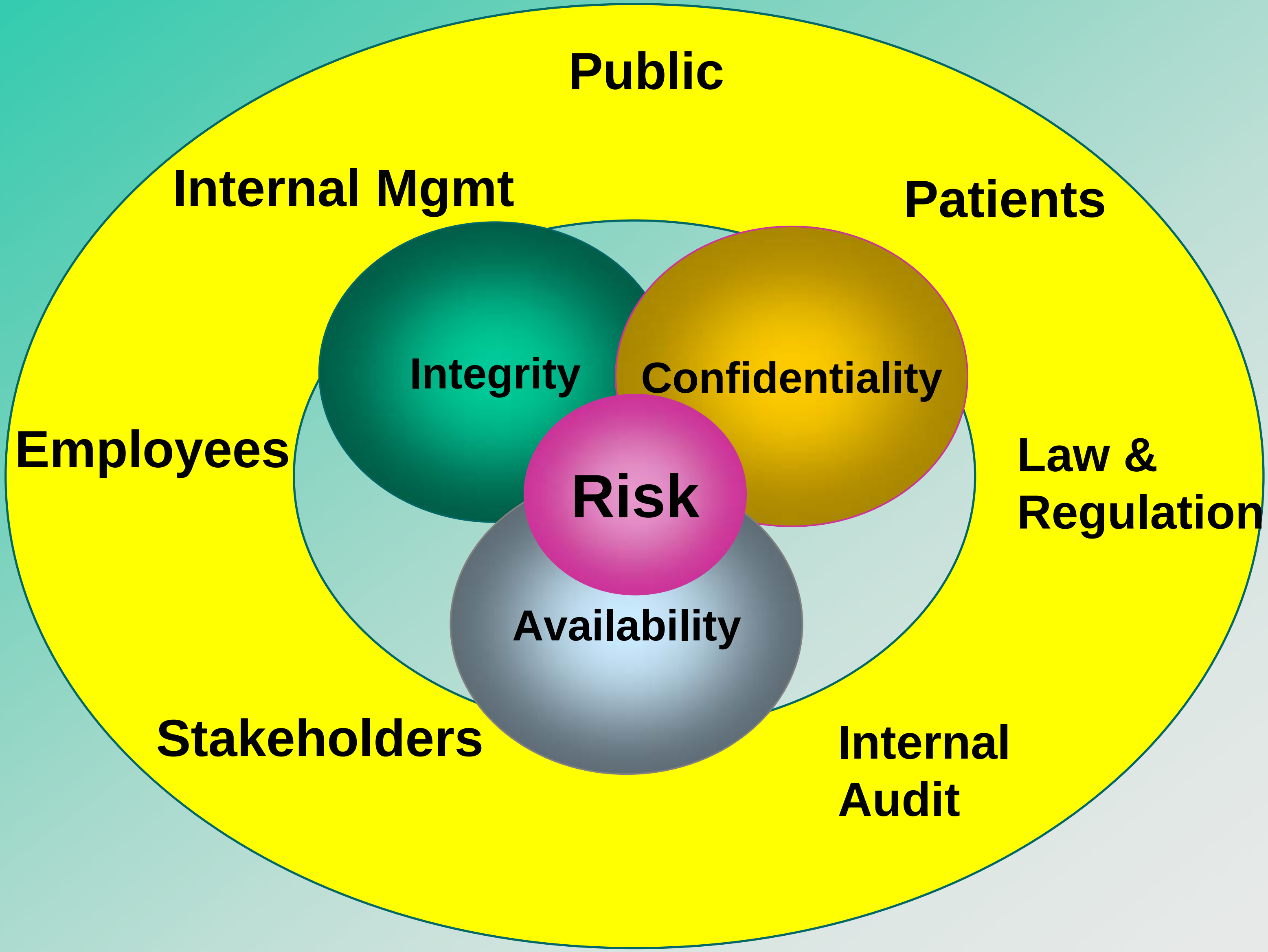
Ian Reinecke, Chief Executive Officer,
Australian E-Health Transition Authority

Goals of Info Security Management:

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.



Context for Info Security Management



Public

Internal Mgmt

Patients

Employees

Integrity

Confidentiality

Risk

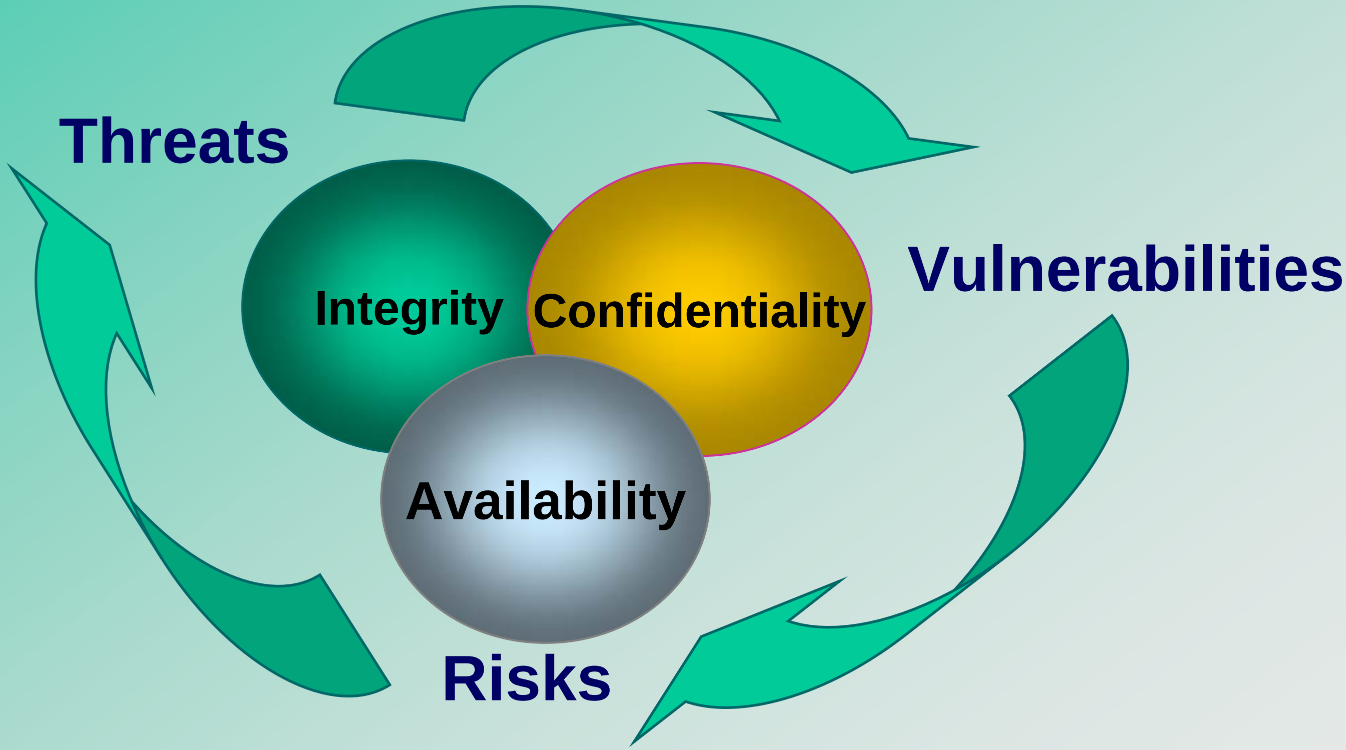
Law & Regulation

Availability

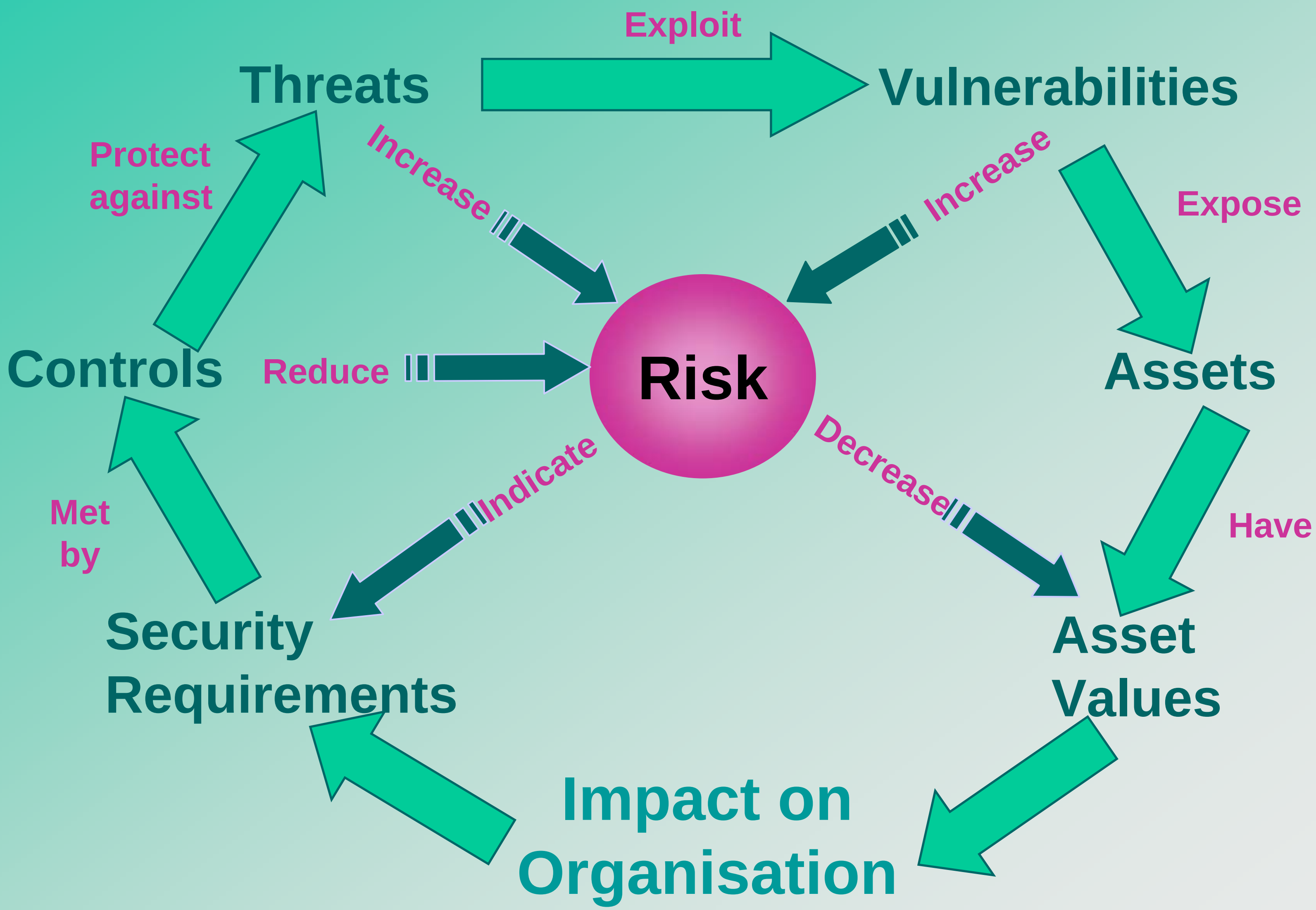
Stakeholders

Internal Audit

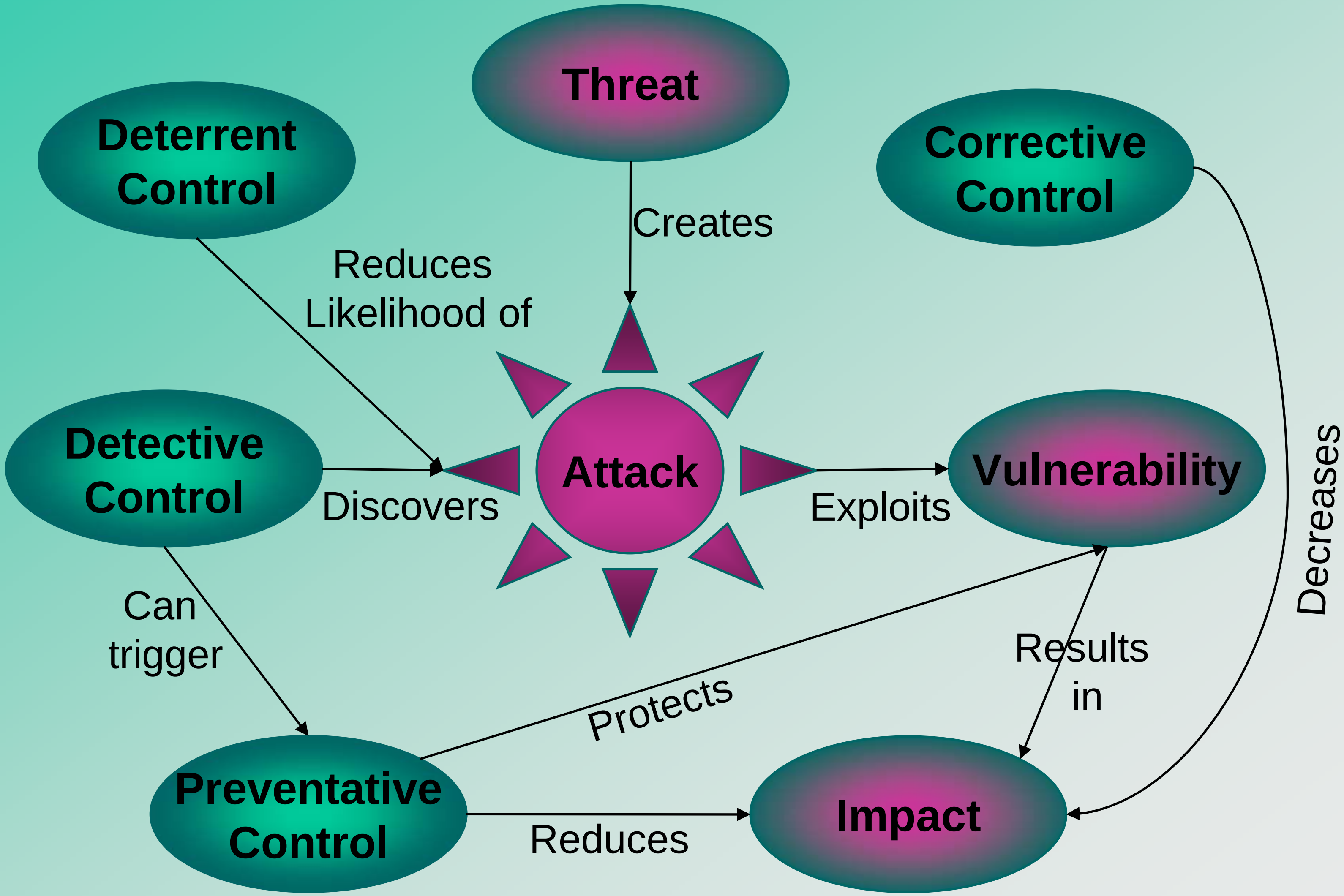
Threats, Risks & Vulnerabilities



Threats, Risks & Vulnerabilities



Security Controls



Agenda

- Information Security Mgmt:
  - Need for standards
  - Goals and context
  - Threats, Vulnerabilities, Risks
- ISO 27799 – Security management in health using ISO 17799
  - Rationale, history and structure of 17799
  - Rationale, history and structure of 27799
  - Structure of 27799
- Questions

ISO 17799:2000 Code of Practice for Information Security Management

What is it?

- “A comprehensive set of controls comprising best practices in information security”
- Basically… an internationally recognised generic information security standard

Purpose:

- “It is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce”
- Facilitation of information flow in a trusted environment

ISO 17799 contains:

- 11 control areas essential to Information Security Management System
- More than 130 controls

ISO 17799: History

British Standards Institute (BSI)

- formed in 1901, develops British industry policies and standards
- supports over 3,000 technical committees and 16,000 standards projects
- member of ISO and European standards organization (CEN)

In early 1990's, BSI recognized need for a practical guide for information security management

- Group of leading companies (BOC, BT, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever) combined to develop a Code of Practice for Information Security Management (now BS 7799 Part 1 Code of Practice)
- Published as BS7799 "Code of Practice for Information Security" in Feb 1995
- BS 7799 Part 2 "Specification for Information Security Management Systems" commission by UK government Dept. of Trade and Industry and published in Feb 1998

ISO 17799: History

Early Days (mid 1990's):

Other countries started to publish it as a national standard:

- Netherlands (SPE20003)
- Australia/New Zealand (AS/NZS 4444)
- Denmark and Sweden (SS627799)

Initially NOT widely embraced by industry, for various reasons:

- not flexible enough
- simplistic 'key control' approach
- other more pressing issues (e.g.: Y2K)

Major revision of BS7799:

- version 2 published in May 1999
- formal certification and accreditation schemes launched same year
- support tools started to appear
- fast tracked as an ISO standard
- published as ISO standard, December 2000

ISO 17799: Current Status

By 2000, there was significant uptake

- many organizations intended to implement
- some well on route to certification
- some organizations already certified
- significant international uptake
- massive increase in interest in the issue of security

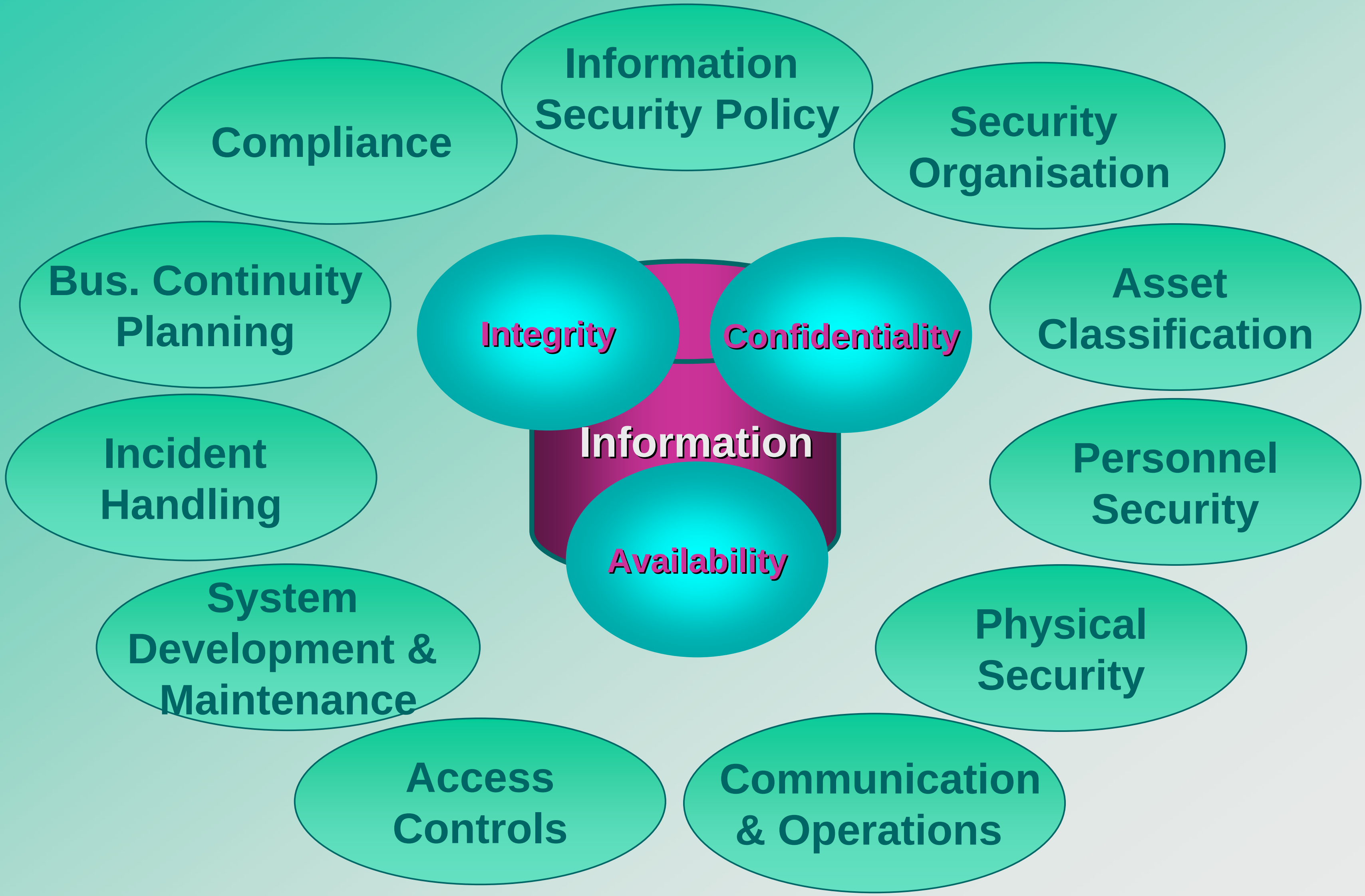
Why the sudden interest?

- Companies doing e-business sought security assurance
- Major consultancies invested very heavily in training of certified auditors (potential major income generator)
  - consultants therefore act indirectly as sales agents
- Quality of the standard improved significantly
- Y2K and other competing issues had been completed or scaled down

ISO 17799: Approach

- ISO 17799 based on assuring confidentiality, integrity, availability of information assets and integrity and availability of supporting systems
- Assurance is attained through *controls* that management creates and maintains within the organisation.
- Eleven key control areas are identified by 17799
    - All 11 are needed for the implementation of a successful information security program
- Control areas are broken down into a total of 39 main security categories. For each category, the standard states:
    - a control objective
    - one or more controls

Eleven Key Control Areas of ISO 17799



Compliance

Information Security Policy

Security Organisation

Bus. Continuity Planning

Integrity

Confidentiality

Asset Classification

Information

Incident Handling

Personnel Security

Availability

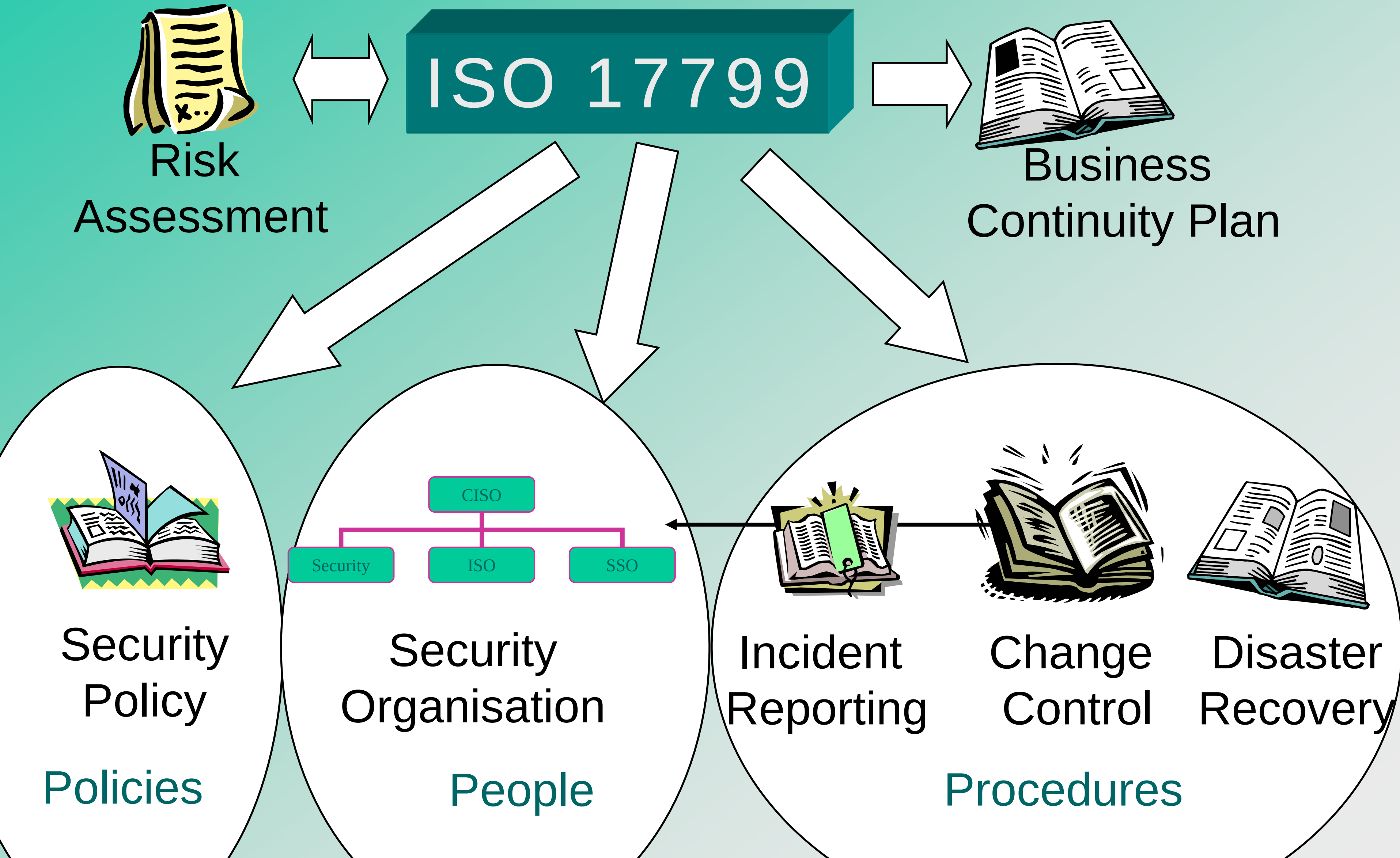
System Development & Maintenance

Physical Security

Access Controls

Communication & Operations

Output:



Risk Assessment

ISO 17799

Business Continuity Plan

CISO

Security

ISO

SSO

Security Policy

Security Organisation

Incident Reporting

Change Control

Disaster Recovery

Policies

People

Procedures

Agenda

- Information Security Mgmt:
  - Need for standards
  - Goals and context
  - Threats, Vulnerabilities, Risks
- ISO 27799 – Security management in health using ISO 17799
  - Rationale, history and structure of 17799
  - Rationale, history and structure of 27799
  - Structure of 27799
- ISO 17090 – Public Key Infrastructure (PKI)
  - Goals
  - Part 1 – Overview of digital certificate services
  - Part 2 – Certificate profile
  - Part 3 – Policy management of certification authority
- Questions

ISO 27799: Security Management in Health using ISO/IEC 17799

What is it?

- a guide to applying ISO 17799 when securing health information systems or protecting personal health information
- A minimum set of requirements that must be met in order to ensure proper information security in healthcare

Purpose:

- “provides guidance to health organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 17799 ”
- “addresses the special security management needs of the health sector and its unique operating environments”
- gives healthcare specific guidance on each of the 11 control objectives in 17799.
- specifies some minimum requirements

ISO 27799: History

"Not all 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 organisation." ISO 17799

By 2003, the need was recognised for a practical guide for information security management in healthcare

Work of creating this guideline fell to ISO Technical Committee 215 and began in autumn of 2003

ISO Technical Committee 215 – Health Informatics

- **Technical Committee 215 first met in 1998**
- **develops standards related to healthcare information (data models, communications for medical devices, terminologies, security, health cards, e-prescribing and more**
- **supports 8 working groups**
- **has published almost 30 standards, specifications and reports**

Task group meetings held in Aarhus Denmark, Toronto, Washington, San Francisco, Delft, Berlin, Hamamatsu Japan, and Jeju Korea

ISO 27799: Current Status

Current draft is under ballot as a Draft International Standard

Ballot closes in October, 2006

How you can contribute

Obtain the current draft from your national delegation to ISO TC 215 or email me at rossfraser@aol.com

Send your comments to your national delegation or email them to me at rossfraser@aol.com

Agenda

- Information Security Mgmt:
  - Need for standards
  - Goals and context
  - Threats, Vulnerabilities, Risks
- ISO 27799 – Security management in health using ISO 17799
  - Rationale, history and structure of 17799
  - Rationale, history and structure of 27799
  - Structure of 27799
- Questions

Structure of ISO 27799

- Health information security overview

1. Information security within information governance
2. Information governance within corporate and clinical governance
3. Health information to be protected:
   - personal health information
   - pseudonymised data derived from personal health information
   - statistical and research data, including anonymised data derived by removal of personally identifying data
   - clinical / medical knowledge not related to specific patients (e.g., data on adverse drug reactions)
   - data on health professionals and staff
   - information related to public health surveillance
   - audit trail data that are produced by health information systems containing personal health information or data about the actions of users in regard to personal health information
   - system security data, e.g.: access control data and other security related system configuration data for health information systems.
4. Threats and vulnerabilities in health information security
   - 25 threats to health info security are described

Structure of ISO 27799

- Practical action plan for implementing ISO/IEC 17799

1 Taxonomy of the 17799 and 27001 standards

2 Management commitment to implementing ISO/IEC 17799

3 Establishing, operating, maintaining and improving the information security management system (ISMS)

Planning: establishing the ISMS

Doing: implementing and operating the ISMS

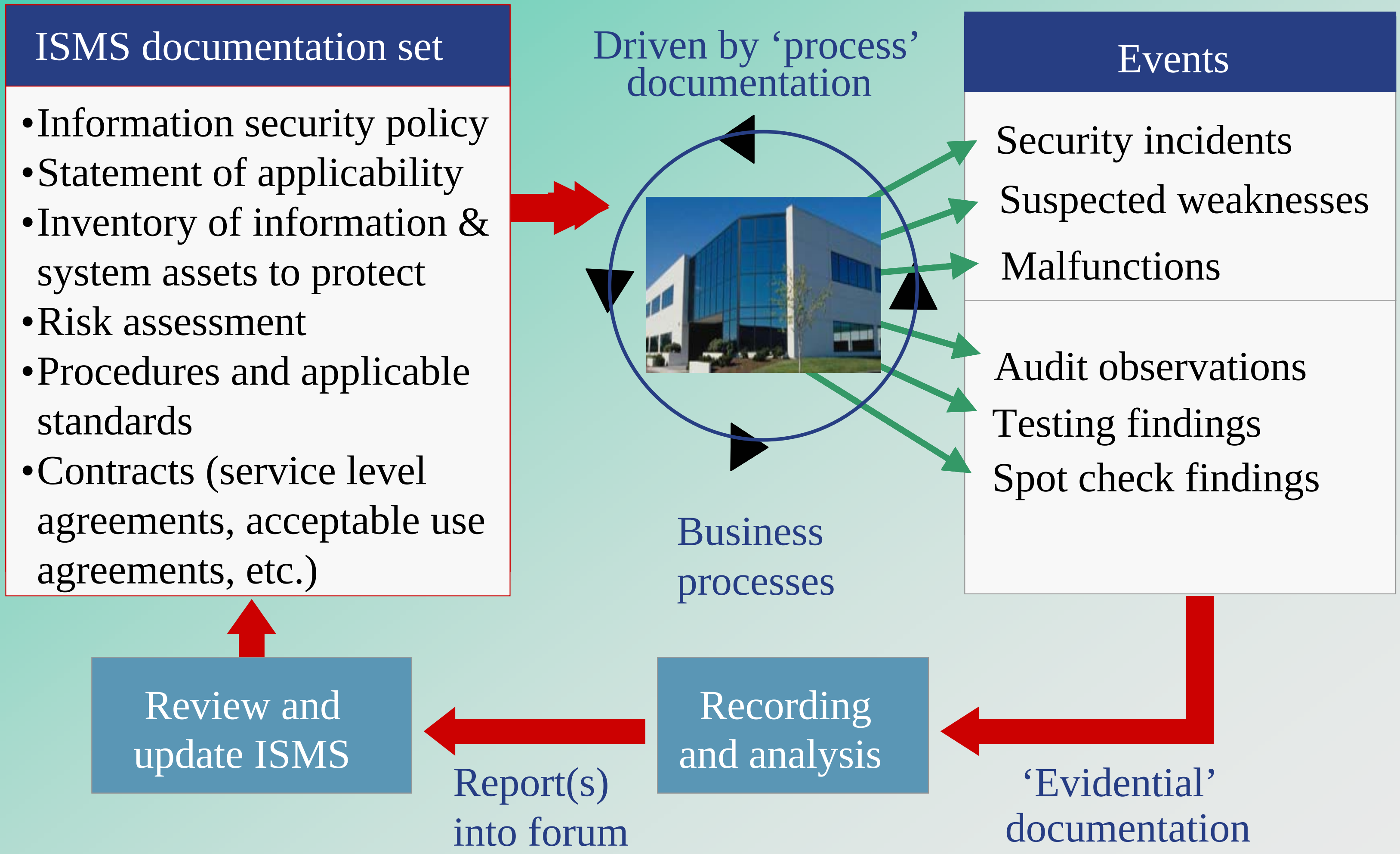
Checking: monitoring and reviewing the ISMS

Acting: maintaining and improving the ISMS

…continued

Structure of ISO 27799

- Information Security Management System



ISMS documentation set

- Information security policy
- Statement of applicability
- Inventory of information & system assets to protect
- Risk assessment
- Procedures and applicable standards
- Contracts (service level agreements, acceptable use agreements, etc.)

Driven by 'process' documentation

Business processes

Events

Security incidents

Suspected weaknesses

Malfunctions

Audit observations

Testing findings

Spot check findings

'Evidential' documentation

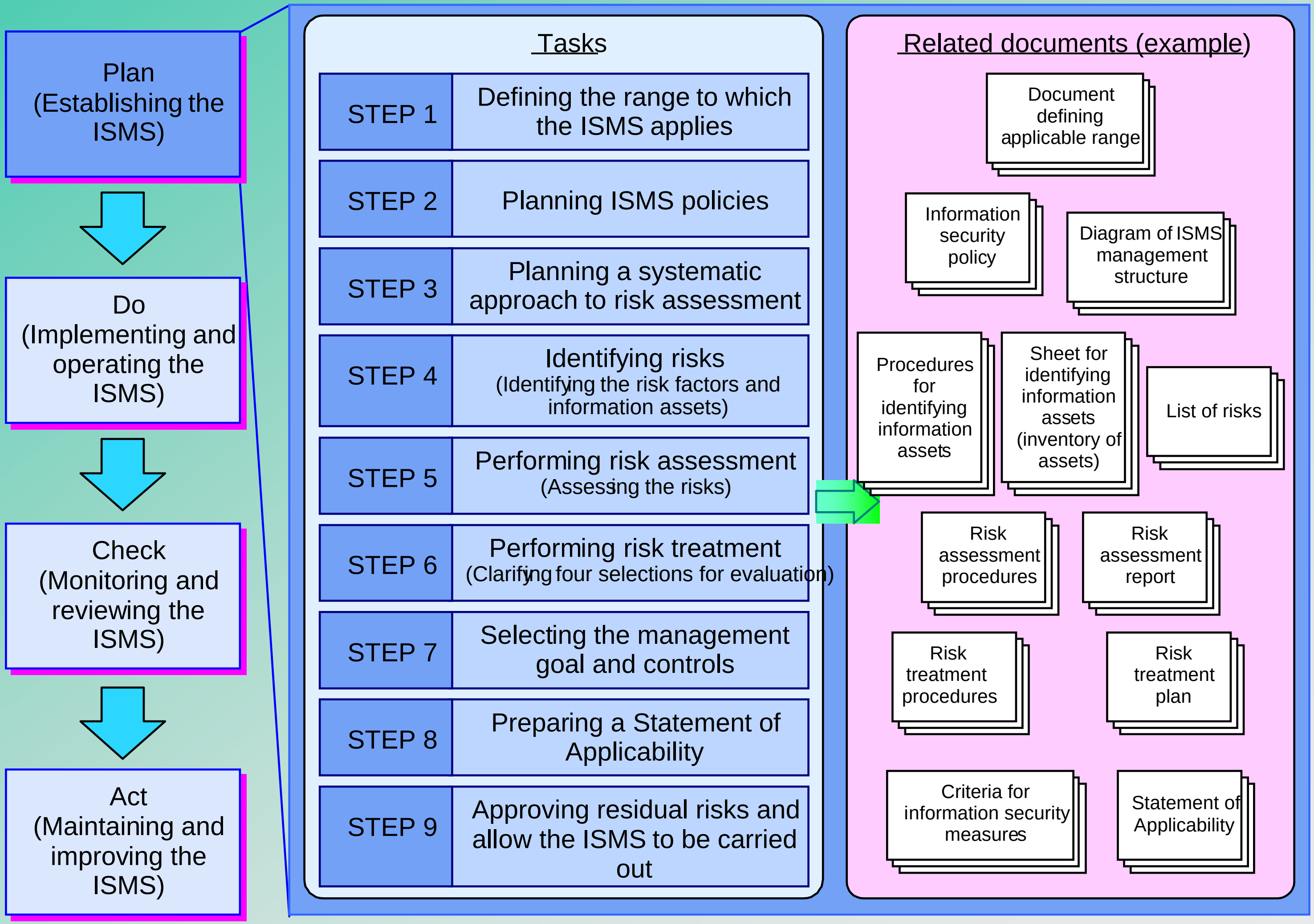
Recording and analysis

Report(s) into forum

Review and update ISMS

Structure of ISO 27799

- Tasks and related documents of the Information Security Management System:



Plan (Establishing the ISMS)

Do (Implementing and operating the ISMS)

Check (Monitoring and reviewing the ISMS)

Act (Maintaining and improving the ISMS)

Tasks

STEP 1	Defining the range to which the ISMS applies
STEP 2	Planning ISMS policies
STEP 3	Planning a systematic approach to risk assessment
STEP 4	Identifying risks (Identifying the risk factors and information assets)
STEP 5	Performing risk assessment (Assessing the risks)
STEP 6	Performing risk treatment (Clarifying four selections for evaluation)
STEP 7	Selecting the management goal and controls
STEP 8	Preparing a Statement of Applicability
STEP 9	Approving residual risks and allow the ISMS to be carried out

Related documents (example)

Document defining applicable range

Information security policy

Diagram of ISMS management structure

Procedures for identifying information assets

Sheet for identifying information assets (inventory of assets)

List of risks

Risk assessment procedures

Risk assessment report

Risk treatment procedures

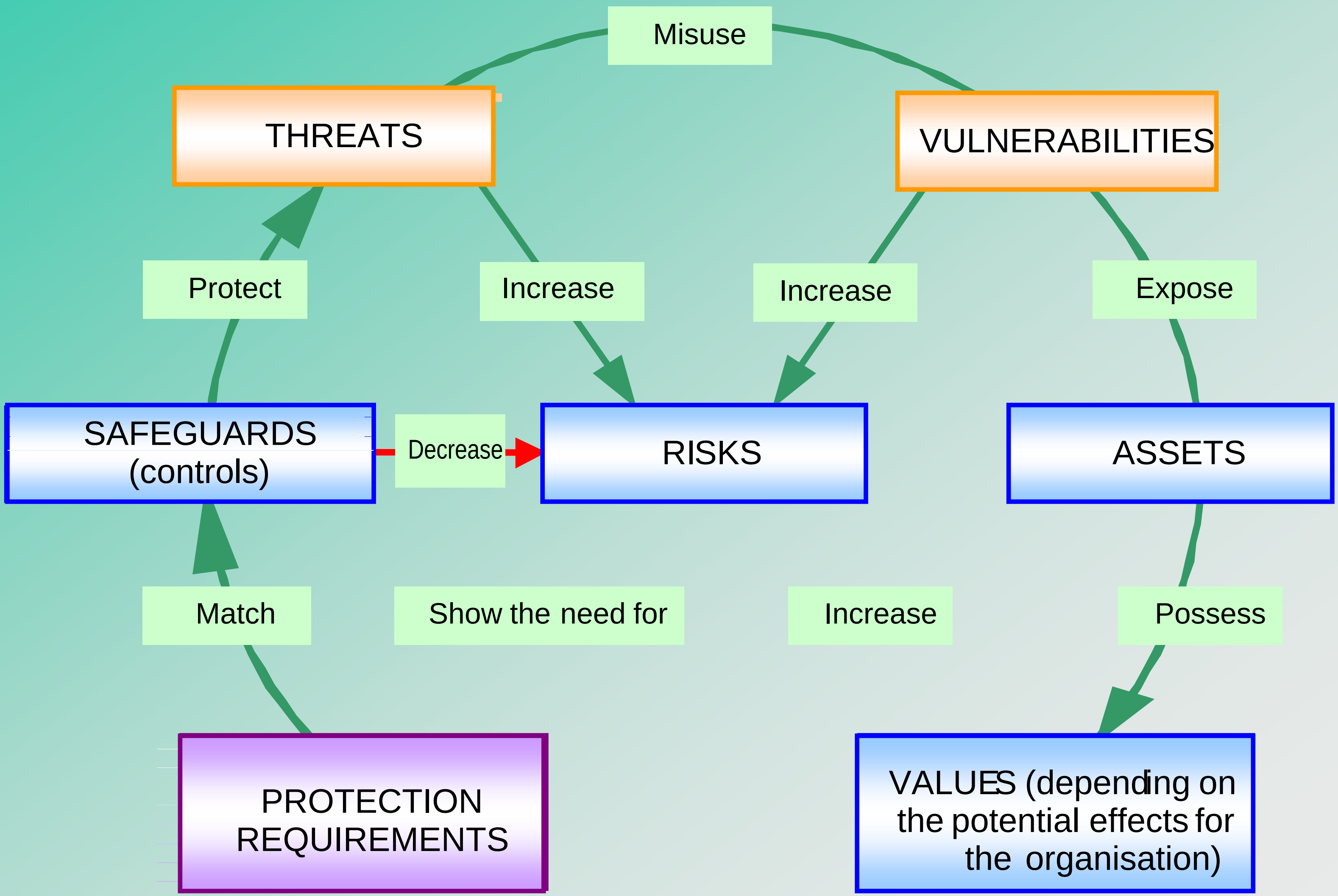
Risk treatment plan

Criteria for information security measures

Statement of Applicability

Structure of ISO 27799

- Managing risks



Structure of ISO 27799

- Healthcare implications of ISO/IEC 17799

  1 Information security policy
    - Information security policy document
    - Review of the information security policy document

  2 Organizing information security
    - Internal organization
      - Management commitment to information security, information security co-ordination, and allocation of security responsibilities
      - Authorization process for information processing facilities
      - Confidentiality agreements
      - Contact with Authorities, contact with special interest groups, and independent review of security
    - Third parties
      - Identification of risks related to external parties
      - Addressing security when dealing with customers
      - Addressing security in third party agreements

…continued

Structure of ISO 27799

3 Asset management

- Responsibility for health information assets
- Health information classification
  - Classification Guidelines
  - Information labelling and handling

4 Human resources security

- Prior to employment
  - Roles and responsibilities
  - Screening
  - Terms and conditions of employment
- During employment
  - Management responsibilities
  - security awareness, education and training
  - Disciplinary process
- Termination or change of employment
  - Termination of responsibilities and return of assets
  - Removal of access rights

…continued

Structure of ISO 27799

5 Physical and environmental security

- Secure areas
  - Physical security perimeter
  - Physical entry controls; securing offices, rooms and facilities; protecting against external and environmental threats; and working in secure areas
  - Public access, delivery and loading areas
- Equipment security
  - Equipment siting and protection
- Supporting utilities, cabling security, and equipment maintenance
- Security of equipment off-premises
- Secure disposal or reuse of equipment
- Removal of property

…continued

Structure of ISO 27799

6 Communications and operations management

- Operational procedures and responsibilities
  - Documented operating procedures
  - Change management
  - Segregation of duties
  - Separation of development, test and operational facilities
- Third-party service delivery management
- System planning and acceptance
  - Capacity management
  - System acceptance
- Protection against malicious and mobile code
  - Controls against malicious code
  - Controls against mobile code
- Backup
  - Health information backup
- Network security management
  - Network controls
  - Security of network services

…continued

Structure of ISO 27799

6 Communications and operations management continued...

- Media handling
  - Management of removable computer media
  - Disposal of media
  - Information handling procedures
  - Security of system documentation
- Exchanges of information
  - Health information exchange policies and procedures, and exchange agreements
  - Physical media in transit
  - Electronic messaging
  - Health information systems
- Electronic health information services
  - Electronic commerce, and online transactions
  - Publicly available health information
- Monitoring
  - Audit logging
  - Protection of log information
  - Clock synchronization

Structure of ISO 27799

7 Access control

- Requirements for access control in health
  – Access control policy
- User access management
  – User registration
  – Privilege management
  – User password management
  – Review of user access rights
- User responsibilities
- Network access control, and operating system access control
- Application and information access control
  – Information access restriction
  – Sensitive system isolation
- Mobile computing and teleworking
  – Mobile computing and communications
  – Teleworking

…continued

Structure of ISO 27799

8 Information systems acquisition, development, maintenance

- Security requirements of information systems
  - Security requirements analysis and specification
- Correct processing in applications
  - Uniquely identifying subjects of care
  - Input data validation
  - Control of internal processing
  - Message Integrity
  - Output data validation
- Cryptographic controls
  - Policy on use of cryptographic controls, and key management
- Security of system files
  - Control of operational software
  - Protection of system test data
  - Access control to program source code
- Security in development and support processes, and technical vulnerability management

…continued

Structure of ISO 27799

9 Information Security incident management

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

10 Business continuity management

- Information security aspects of business continuity management

…continued

Structure of ISO 27799

11 Compliance

- Compliance with legal requirements
  - Identifying applicable legislation, intellectual property rights, and protection of organizational records
  - Data protection and privacy of personal information
  - Prevention of misuse of information processing facilities, and regulation of cryptographic controls
- Compliance with security policies and technical compliance
- Information systems audit considerations in a health environment

…continued

Structure of ISO 27799

- Informative Annexes:
- Threats to health information security
- Tasks and related documents of the Information Security Management System:

  1 establishing the ISMS (Plan)

  2 implementing and operating the ISMS (Do)

  3 monitoring and reviewing the ISMS (Check)

  4 maintaining and improving the ISMS (Act)
- Potential benefits and required attributes of support tools

  1 Potential benefits of support tools

  2 Required attributes of support tools

  3 Tool support for ISO/IEC 17799 process

  4 Tool support for risk analysis process
- Related standards in health information security

Agenda

- Information Security Mgmt:
  - Need for standards
  - Goals and context
  - Threats, Vulnerabilities, Risks
- ISO 27799 – Security management in health using ISO 17799
  - Rationale, history and structure of 17799
  - Rationale, history and structure of 27799
  - Structure of 27799
- Questions

Questions

Bug Me

- Email address:

  ross.fraser@sextantsoftware.com
- Phone:

  (Country Code 1) 416-960-5872