چند رسانه ای
نگارستان

سمینار آموزشی سیستم مدیریت امنیت اطلاعات بر پایه سیاستهای استانداردهای BS7799 & BS15000

سمینار آموزشی اول

Part One

Information Security Management Systems

Dr. Sc. Houman Sadeghi Kaji

Spread Spectrum Communication System PhD. ,

Cisco Certified Network Professional Security Specialist

BS7799 LA

info@houmankaji.net

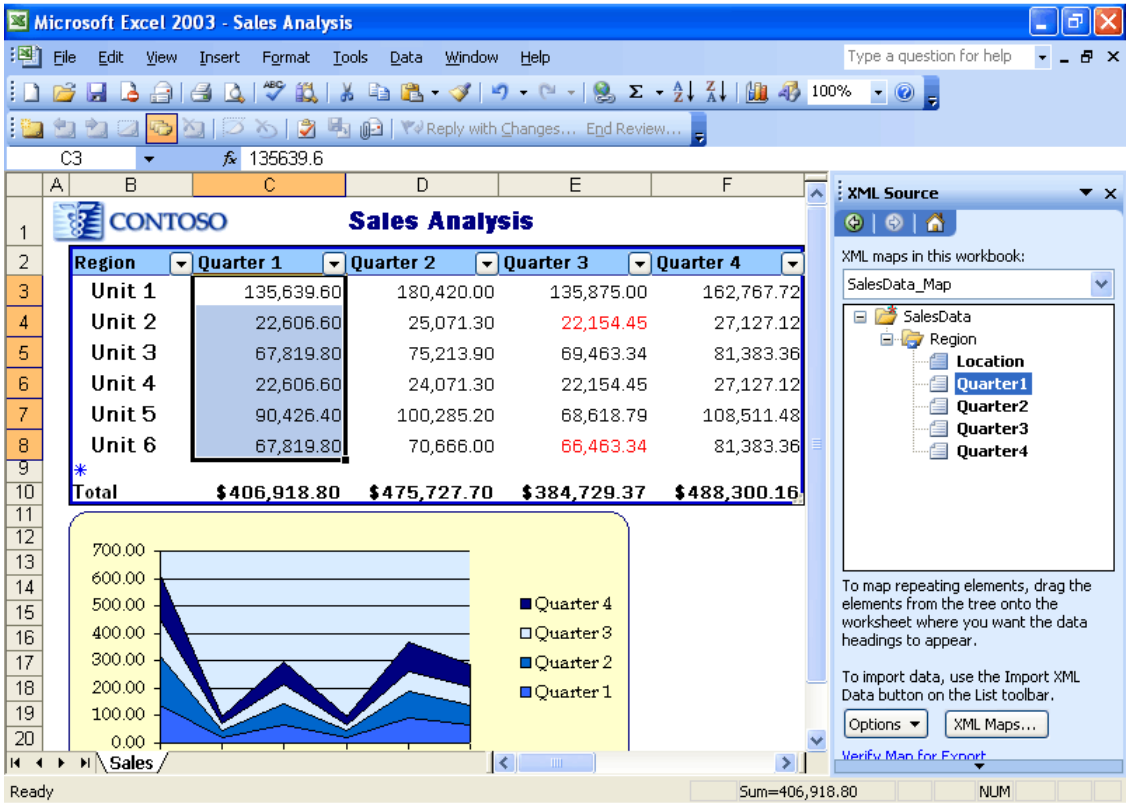
Information Security Management Systems

- **Objectives of this Session**
  - Provide the general history of Information Security Management Systems
  - Get an understanding on the need of Information Security Management Systems within Organizations
  - Get an introduction to the implementation of an Information Security Management System
  - Get an introduction to Risk Assessment and Security Level

What is Information and Information Security?

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

ISO 17799:2000



Types of Information

- Printed or written on paper
- Stored electronically
- Transmitted by mail or electronic means
- Shown on corporate videos
- Spoken in conversations

Why is information security needed?

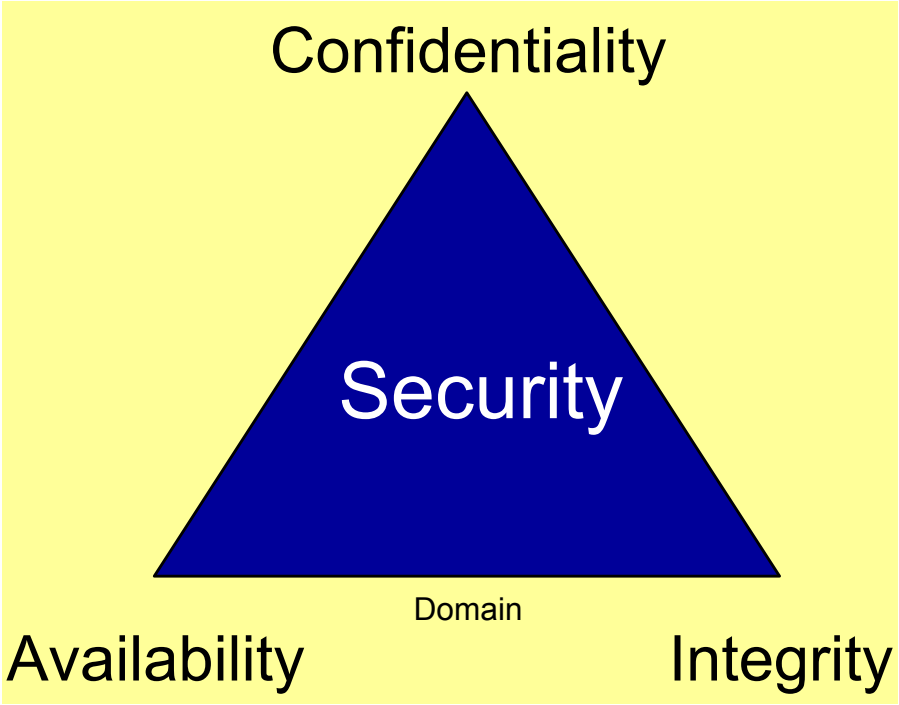
Information :

The key to the success and growth

- 15,000 hospital patient journal found in a waste bin
- 30,000 passwords to internet accounts published on the internet
- Early promotion pictures in the evening press
- Banks pay millions to blackmailing crackers
- 25 people in a development department moved to a competitor
- 300,000 credit cards numbers stolen, some published on www
- Suspected spy employed at ABB

What is Information Security?

- **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



Terms and Definitions

3.1 Availability

ensuring that authorized users have access to information and associated assets when required

3.2 Confidentiality

ensuring that information is accessible only those authorized to have access

3.3 Information security

security preservation of confidentiality, integrity and availability of information

Terms and Definitions

3.4 Information Security Management System (ISMS) that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review. maintain and improve information security

3.5 Integrity

safeguarding the accuracy and completeness of information and processing methods

3.6 Risk Acceptance

decision to accept a risk

Terms and Definitions

3.7 Risk Analysis

systematic use of information to identify sources and to estimate the risk

3.8 Risk Assessment

overall process of risk analysis and risk evaluation

3.9 Risk Evaluation

process of comparing the estimated risk against given risk criteria of determine the significance of risk

Terms and Definitions

3.10 Risk Management

Coordinated activities to direct and control an organization with regard to risk

Note: generally includes risk -assessment, -treatment, -acceptance and -communication.

3.11 Risk Treatment

Treatment process of selection and implementation of measures to modify risk

note 1: sometimes used for the measures themselves

note 2: can include avoiding, optimizing, transferring or retaining risk

Terms and Definitions

3.12 Statement of Applicability

Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and treatment process

How to identify the security requirements?

1. Form security risks

2. From legal and contractual requirements

3. From internal principles, objectives and requirements

CORRECT controls and required degree of flexibility from the START!

Security Level

Business needs

Threat, Probability & Consequence = Risk

Need for Protection

ISMS Implementation

Establish the context

−Define ISMS Scope

−Define policy

−Identify risks

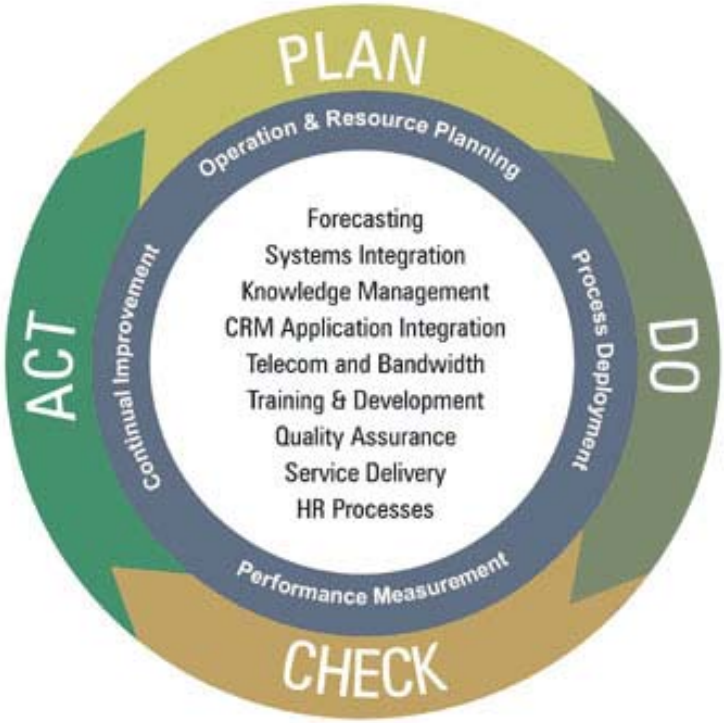
−Assess risks

−Select control objectives and control for treatment of risks

−Prepare a statement of applicability (SoA)

Implement and operate

-Formulate a risk
-Implement the risk treatment plan
-Implement controls selected to meet the control objectives



Maintain and improve

- Implement identified improvements
-Take appropriate corrective and preventive actions
-Communicate the result and actions and agree with all interested parties
-Ensure that improvements achieve their intended objectives

Monitor and review

Execute monitoring procedures
Undertake regular reviews of the effectiveness
Conduct internal audits at planned intervals

ISMS Implementation

Constraints

- Fear/Resistance to change
- Fear for external exposure
- Increased cost
- Inadequate knowledge as to approach
- Seemingly huge task

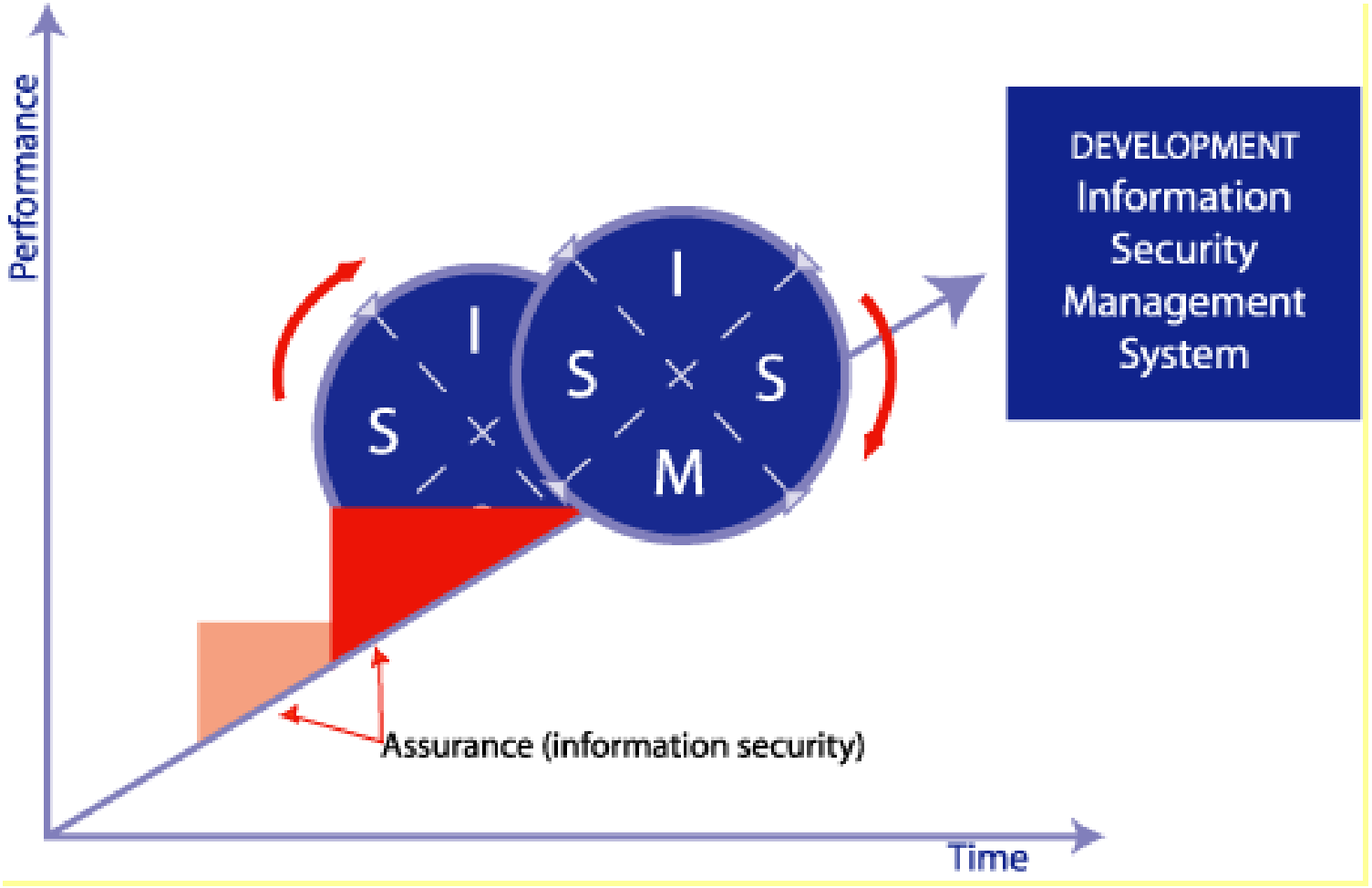
Benefits

- Risk and losses will be reduced
- Compliance to rules, legislation, company standards and practices
- Improved security
- Reliable operations

Benefits of Implementation

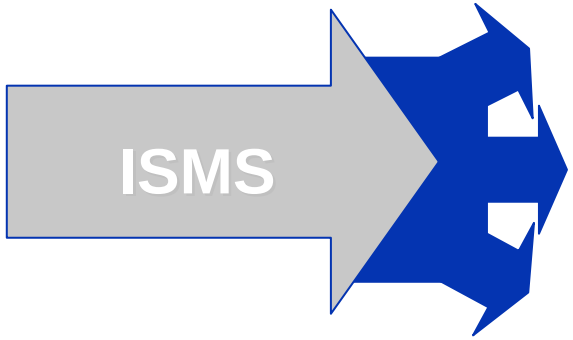
- Systematic approach
- Improved understanding of business aspects
- Reductions in adverse publicity
- Improved insurance liability rating
- Identify critical assets via the business risk assessment
- Provide a structure for continuous improvement
- Be a confidence factor internally as well as externally
- Enhance the knowledge and importance of security-related issues at the management level
- Ensure that "knowledge capital" will be "stored" and managed in a business management system

Continual Improvement



A three pronged ISMS approach

- Sets framework for:



•Management goal setting based on prioritized
•Setting up a structured system with essential elements and methods
•Enables internal and external evaluation for further system development (Improvement)

Implement and operate the ISMS

- Identify management actions and priorities for ISMS
- Implement control objectives and controls
- Implement a risk treatment and controls
- Training and awareness
- Manage the operations and resources
- Implement procedures for detection and response to incidents

Monitor and review the ISMS

- Monitor the processes write, errors, faults, breaches
- Reviews of effectiveness
- Review level of residual and acceptable risk
- Internal audits
- Training and awareness
- Management review
- Record events and actions

Maintain and Improve the ISMS

- Implementing identified improvements
- Take corrective and preventive actions
- Apply lessons learned (internal and external sources)
- Communicate results and actions and agree with parties involved
- Ensure that intended achieved

Documentation Requirements (General)

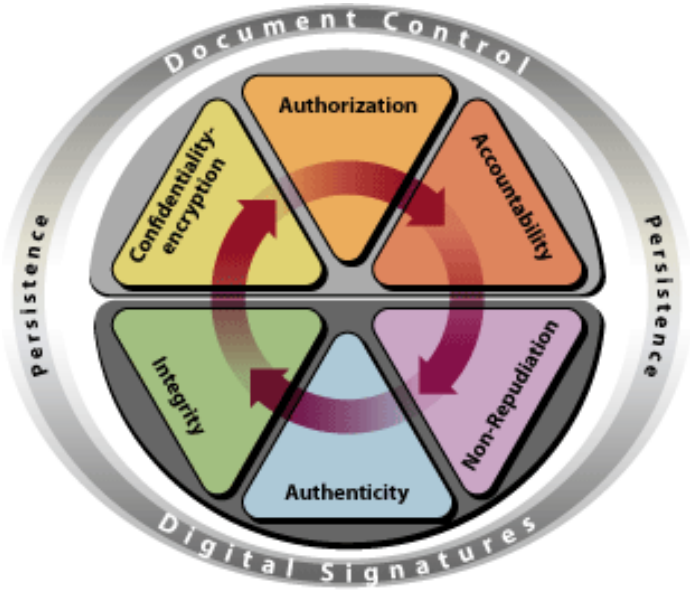
Documentation shall include:

- Statements of policy and control objectives
- Scope of the ISMS
- Procedures and controls in support of ISMS
- Risk assessment report
- Risk treatment plan
- Documented procedures needed by the organization
- Statement of applicability

Document Control

A documented procedure that comprises :

- Approval prior to use
- Review, update and re-approval
- Identification of changes
- Availability of relevant versions of applicable documents
- That documents remain legible and readily
- identifiable
- Identification of external documents
- Distribution of documents are controlled
- Prevent unintended use of obsolete documents
- Apply suitable identification if retained for any purpose



Persistent Document Security
Control that stays throughout the life of the document

Control of Records

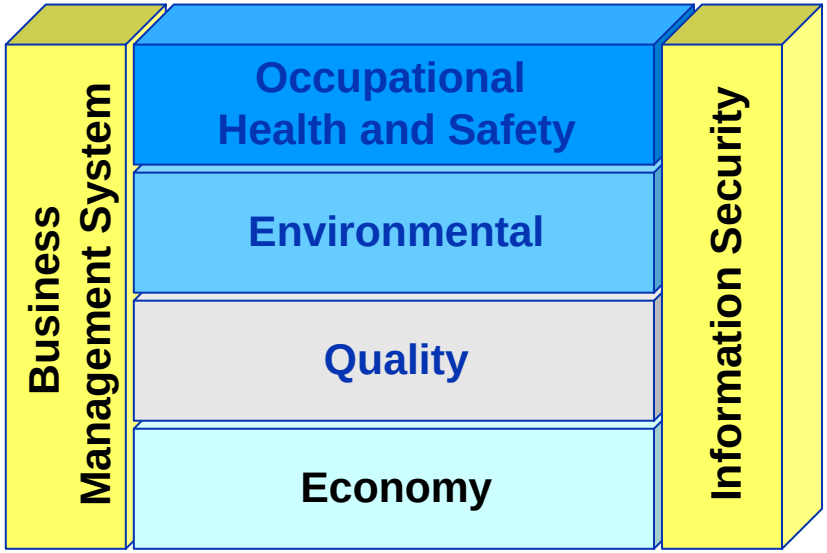
- Evidence
- Demonstrate compliance
- Procedures
- Legible, identifiable and traceable
- Stored and maintained

Identify and Evaluate options

- Apply appropriate controls
- Accept the risk
- Avoid risk
- Transfer risk

The Risk stays with the company , even if the activity is subcontracted !

Co-ordination with other audits



- Quality Management System
- Environmental Management System
- Occupational Health and Safety Management System
- Information Security Management System

Focus Area - Different Management Systems

ISMS

- Risk assessment
- Statement of Applicability
- Security Policy
  - The Complete ISMS
  - Penalty

EMS

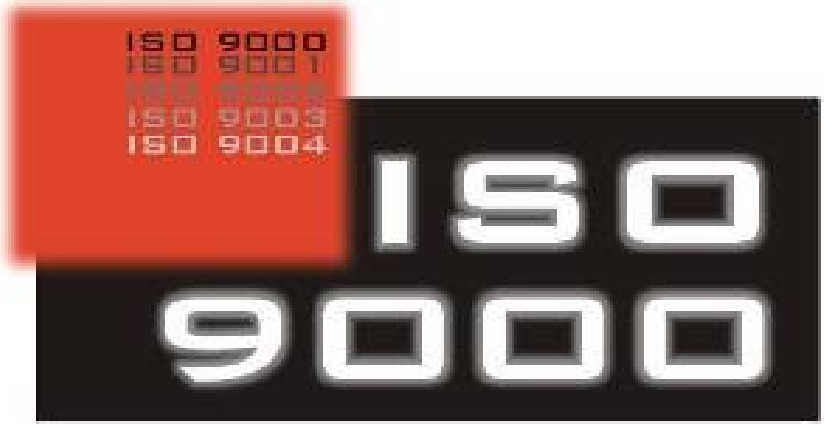
- Environmental aspects
- —
- Environmental Policy
  - Framework for Environmental objectives and targets

QMS

- —
- Application
- Quality Policy
  - Framework for Quality objectives
  - Commitment to comply with requirement

ISO 9000 - Similarities

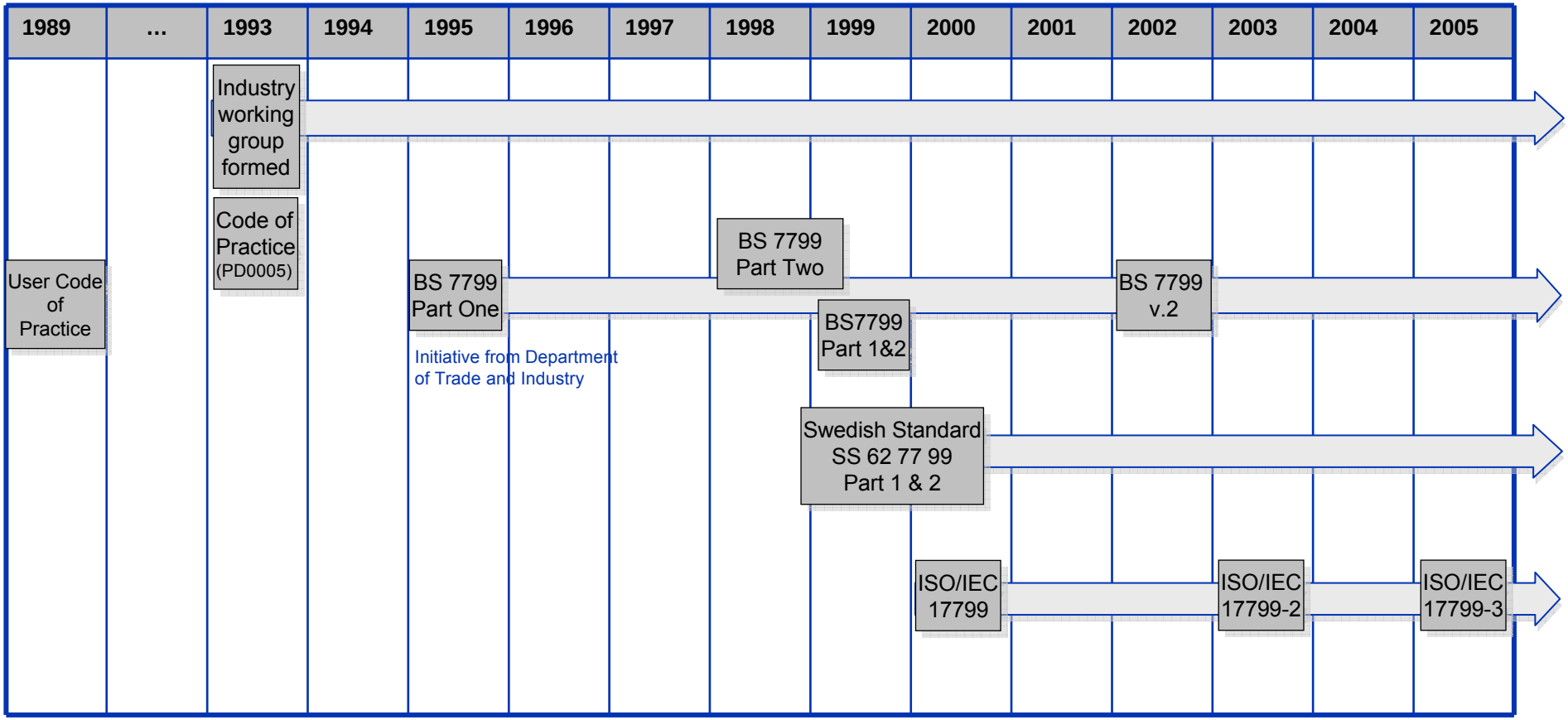
- Management commitment - Policy & Goal
- Organisation, incl. responsibility definition
- System Structure
- Procedures
- Document control
- Records management
- Training
- Management review
- Internal Audit
- Corrective and Preventive Action



ISO 9000 - Differences

- Evaluation of the risk assessment and the statement of applicability
- Assessment of the operation of the controls
- Verification of achievement of security objectives
- Validation of correct implementation of security products
- Verification of adherence to
- Procedures
  - That’s not different

History of Information Security Standards



Fast tracked by ISO / IEC – Feb - Aug 2000
Published – Dec 2000
UK number becomes BS ISO/IEC 17799:2000 / BS 7799-1:2000

The Basis for

Information Security Management Systems

Definition - Risk

- The dictionary defines risk as "***exposure to the chance of injury or loss.***"
- In terms of ***insurance*** it defines risk as "***the hazard or chance of loss.*** "

Risk is the ***perceived extent*** of possible loss.

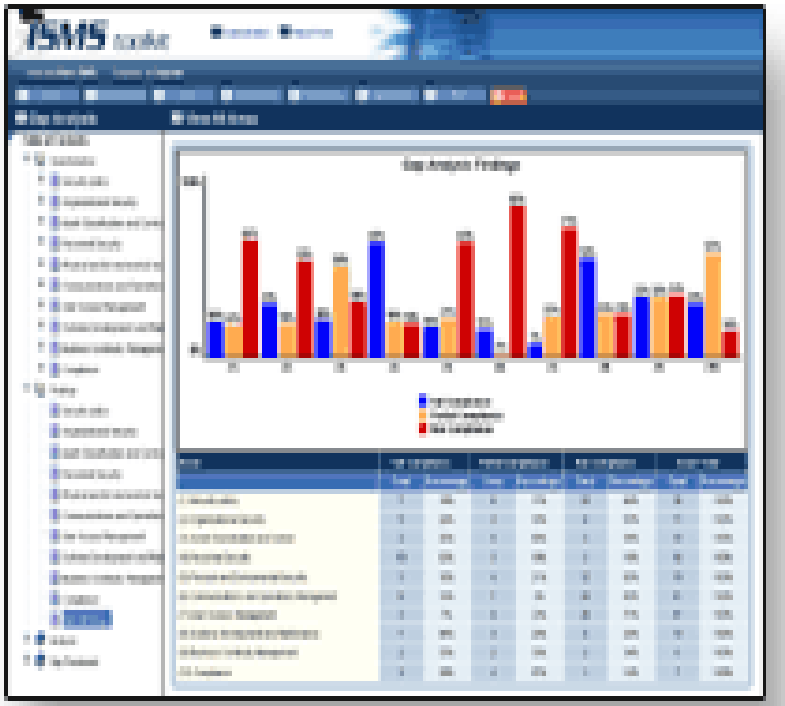
Definition - Business Risk

Business Risk

is the threat that an event or action will adversely affect an organization's ability to successfully achieve its business objectives and execute its strategies

Information

- Information can be an asset and a resource
- Information is knowledge
- Information exists in different shapes:
  - human capital
  - printed or written on paper
  - stored on data media
  - spoken
  - presented on film, video or overhead.



Analyzing Security Risks

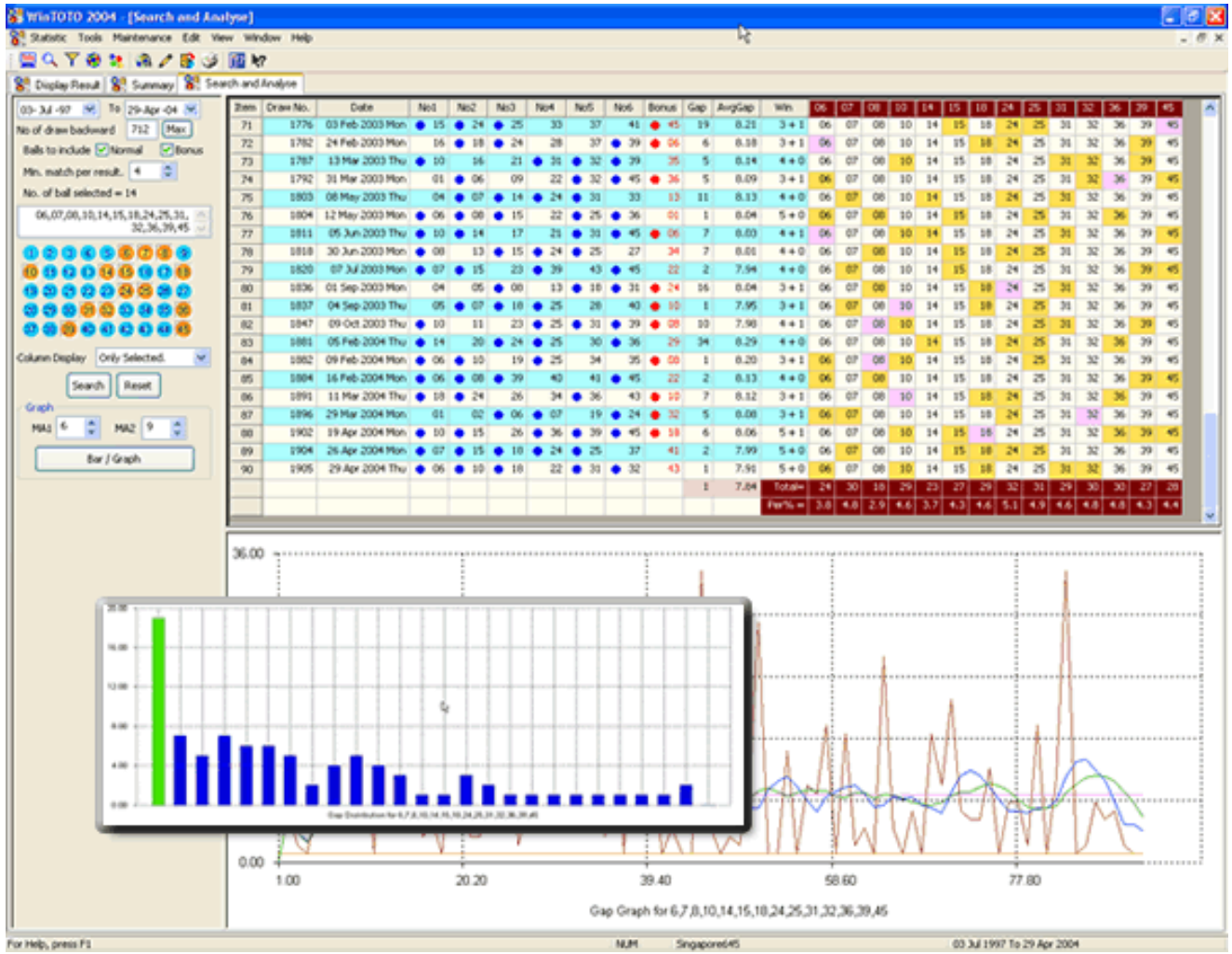
- Security requirements are identified through a methodical analysis of security risks
- Costs for controls must be weighed against the hazard or chance of loss resulting from flaws in security
- A Risk assessment can be performed for a complete organisation, for its different parts as well as for individual information systems or parts of those when this is practical and realistic

Risk Management Methodology

Risk Assessment Method

- What if analysis
- Operator
- Fault tree analysis
- GAP analysis
- Relative Ranking
- Reliability analysis
- Probability and Consequence analysis

Example – GAP analysis result



Basic Data

- Open Company Information
  - Business idea, goals, company presentation
  - Business area
  - Organisation chart ,personnel inventory , positions
  - Annual report and balance sheets
- Other Company Information
  - Strategic Plans
  - Inventory of suppliers
  - Customer inventory
  - Maps, building drawing
  - Assets inventory and their value

Basic Data (cont.)

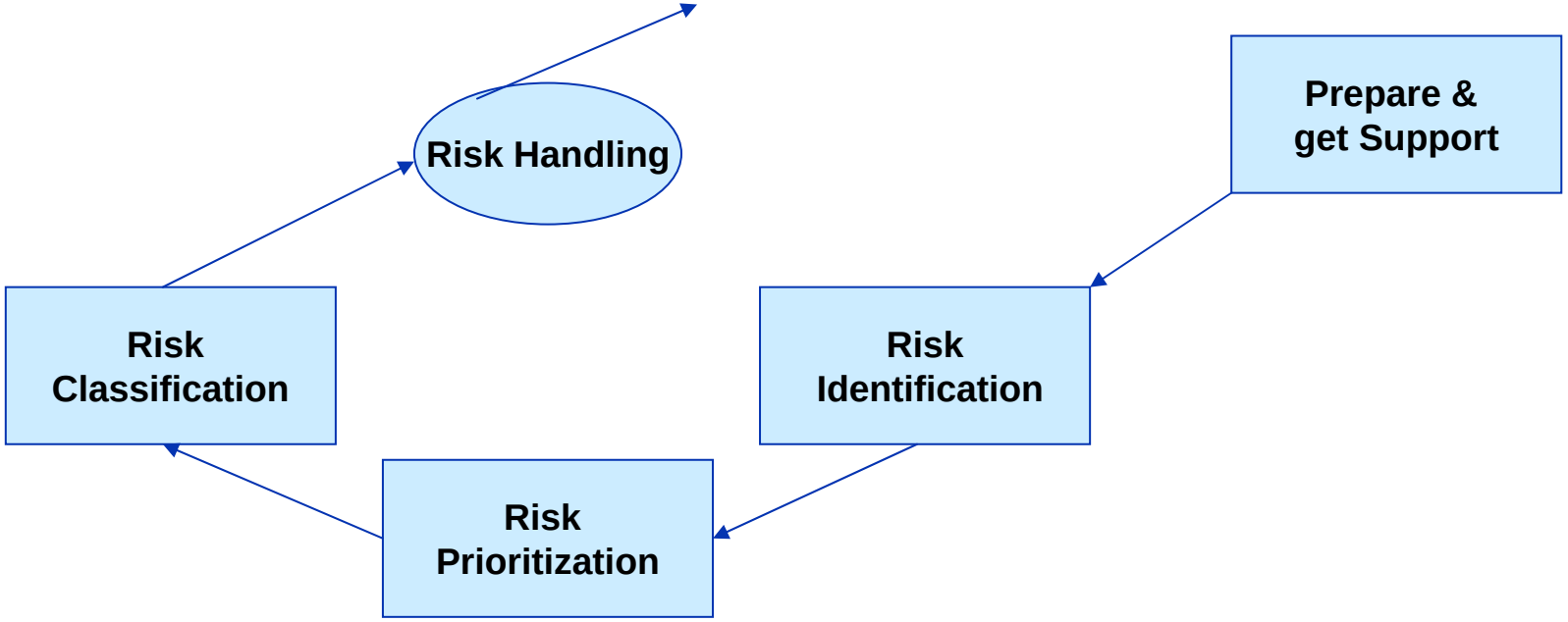
- Statistical Material
  - Near-accident reports and incidents
  - Insurance
  - Loss
  - Operations and maintenance
- Technical Descriptions
  - Supporting systems
  - Communications and network
  - Process, -production flows, systems
  - IT-Infrastructure

Group Members - Representing

- Management
- Business / Department responsible
- IT Operators
- System development
- Network / Communications
- Internal audit
- Security department
- End Users
- Consulting
- Outsourcing partners

Methodology – Threat Analysis to Risk handling

The Basic of Risk Handling in a Company



Understand the Business

Business Process

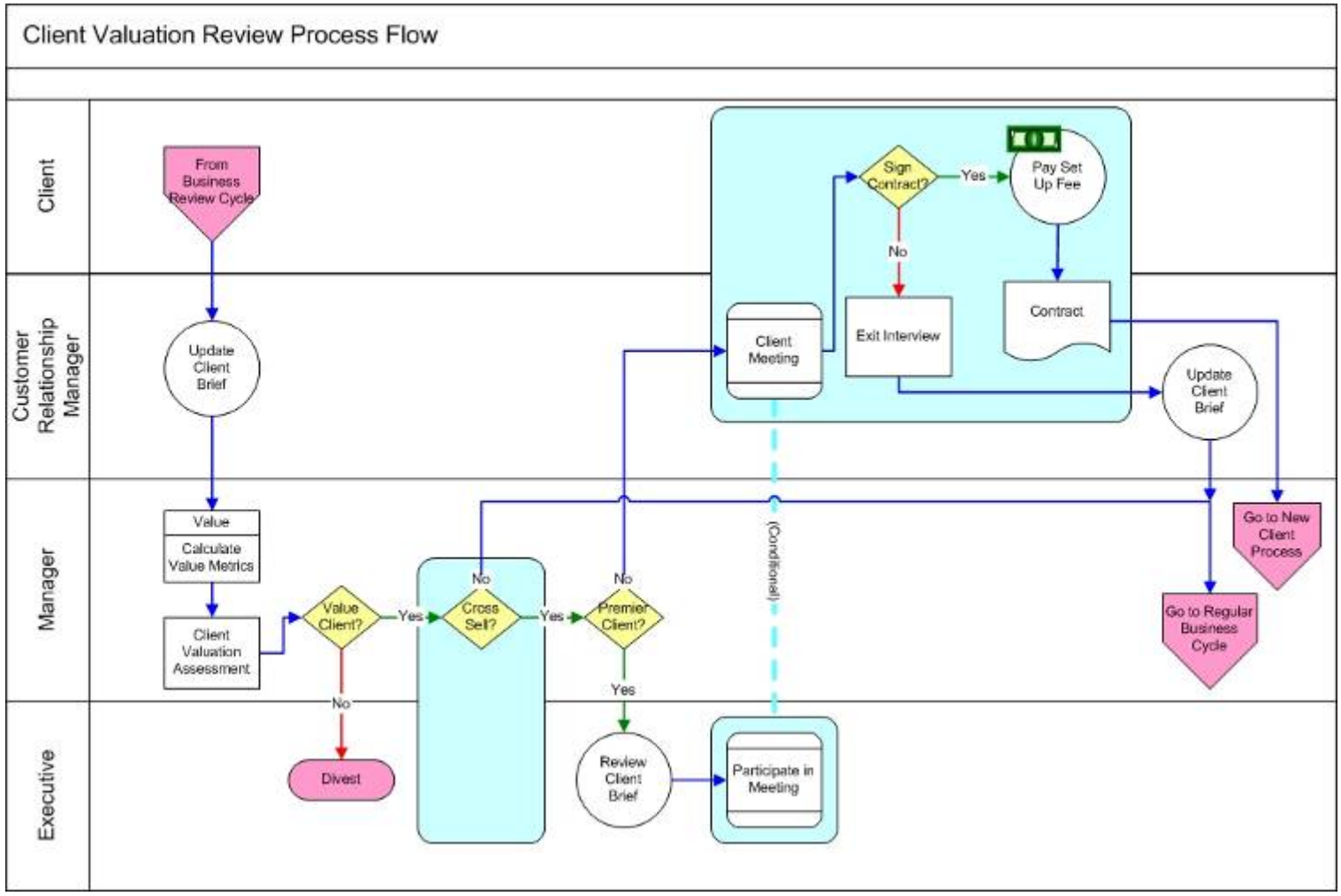
Information Flow

Infrastructure and Resources

Identify the main dependencies in the business and vulnerability points within the organization, from the top as well as from the bottom:

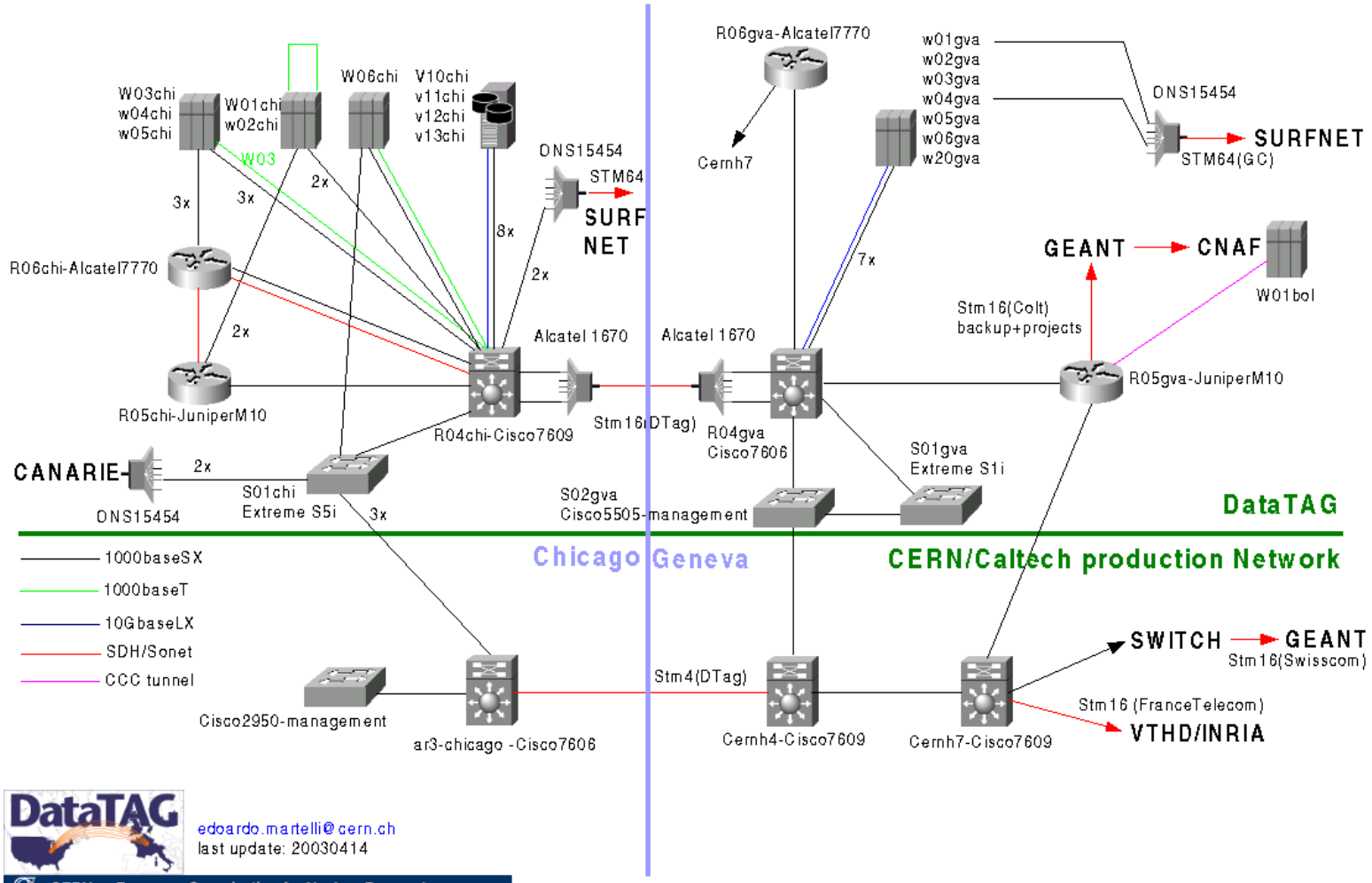
- **What is the organization dependent on to be successful?**
- **Which are the main process driving the business activity?**
- **Which are the vulnerabilities within those systems and business processes?**

Mapping of a business process



Understand the Business – Network Mapping

Datatag Testbed



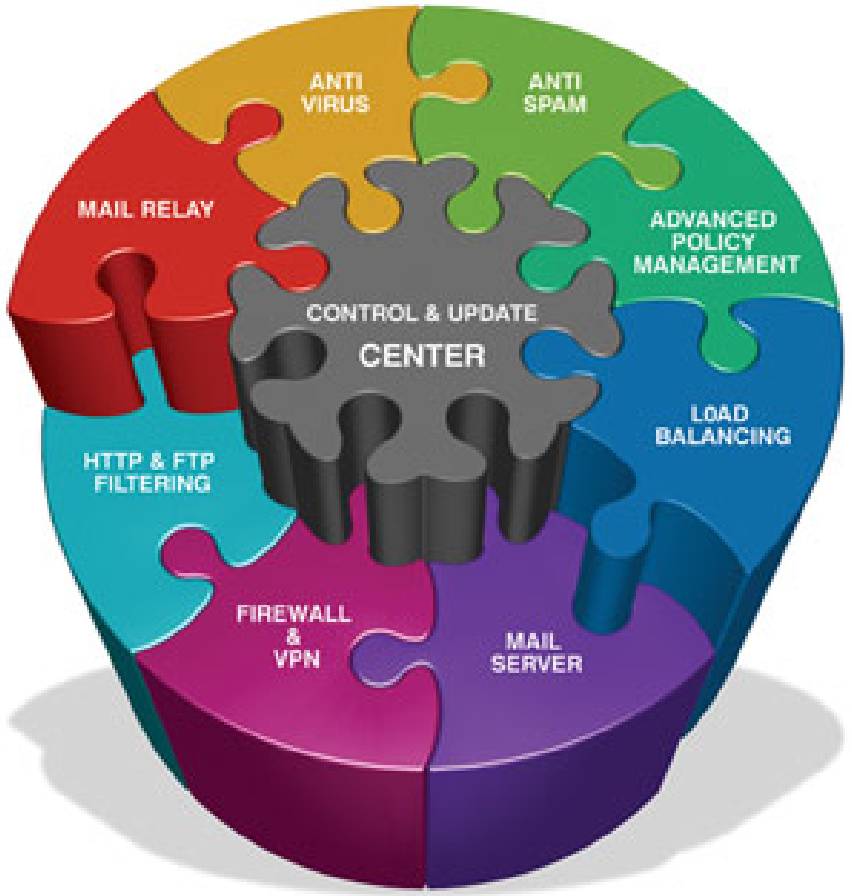
edoardo.martelli@cern.ch

last update: 20030414

CERN — European Organization for Nuclear Research

Threats and Anti-Threats

- **All Systems**
  - **Viruses** **85%**
  - **Insider abuse of Internet** **79%**
  - **Denial of Service** **27%**
- **Web sites**
  - **Vandalism** **64%**
  - **Denial of Service** **60%**
  - **Theft of transactional info** **8%**
  - **Financial Fraud** **3%**



Operational Threats

- Customer satisfaction
- Leadership
- Non marketable
- Product development
- Conformance
- Productivity
- Production shutdown
- Capacity
- Product and Service Quality
- Expectation gap
- Environmental
- Circulation time
- Occupational health and safety
- Supply of raw material
- Fire
- Raw material price

More potential Threats

- Leadership
- Authority
- Limits
- Performance incentive
- Communication
- Fraud (Management)
- Fraud (Employees)
- Unlawful handling
- Forbidden use
- Reputation

Risk Evaluation Factors

- **Probability**

The probability that an event occurs shall, if possible, be based on statistics, history and experience.

- **Consequence**

The consequences shall be drawn up in co-operation with appropriate company representative (s), and, if possible, be specified in financial terms.

Risk Evaluation Factors, Example

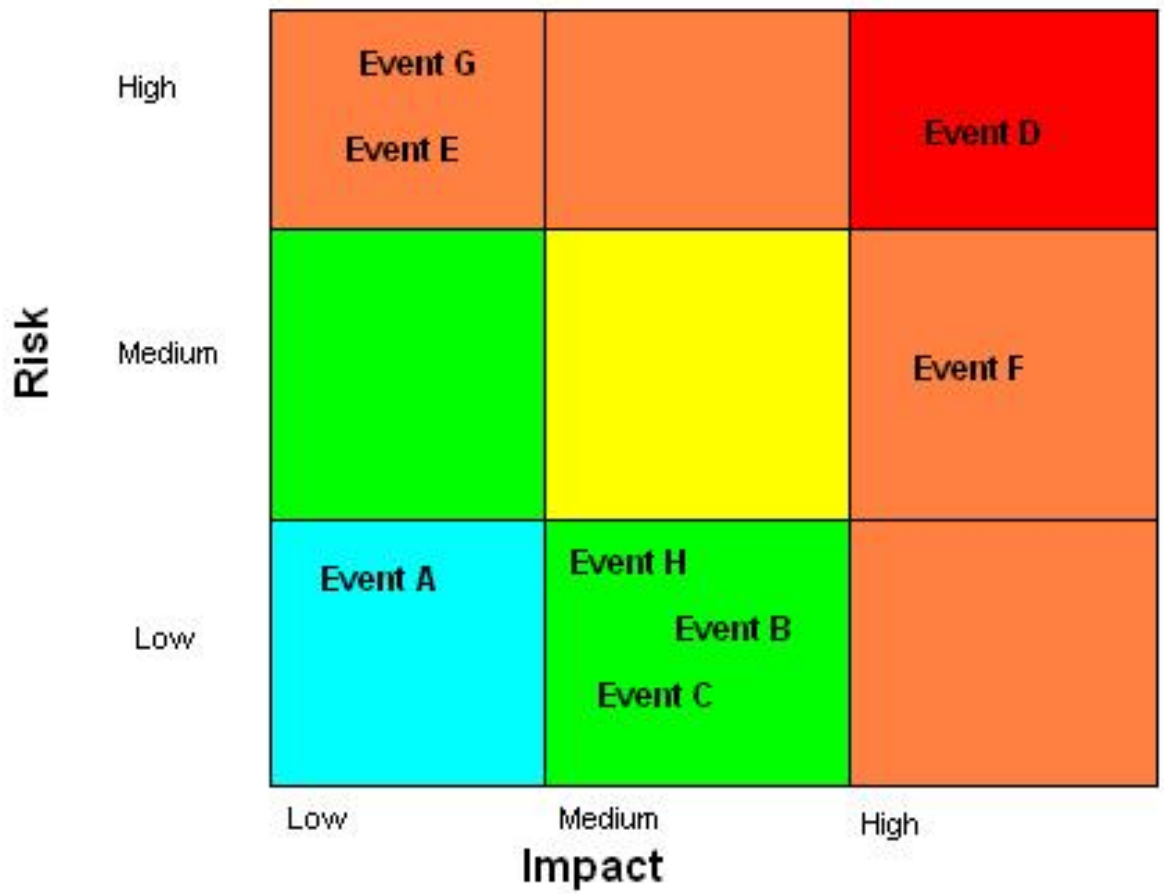
Probability

- High — Once a week
- Medium — Once a month
- Low — Once every 6th month

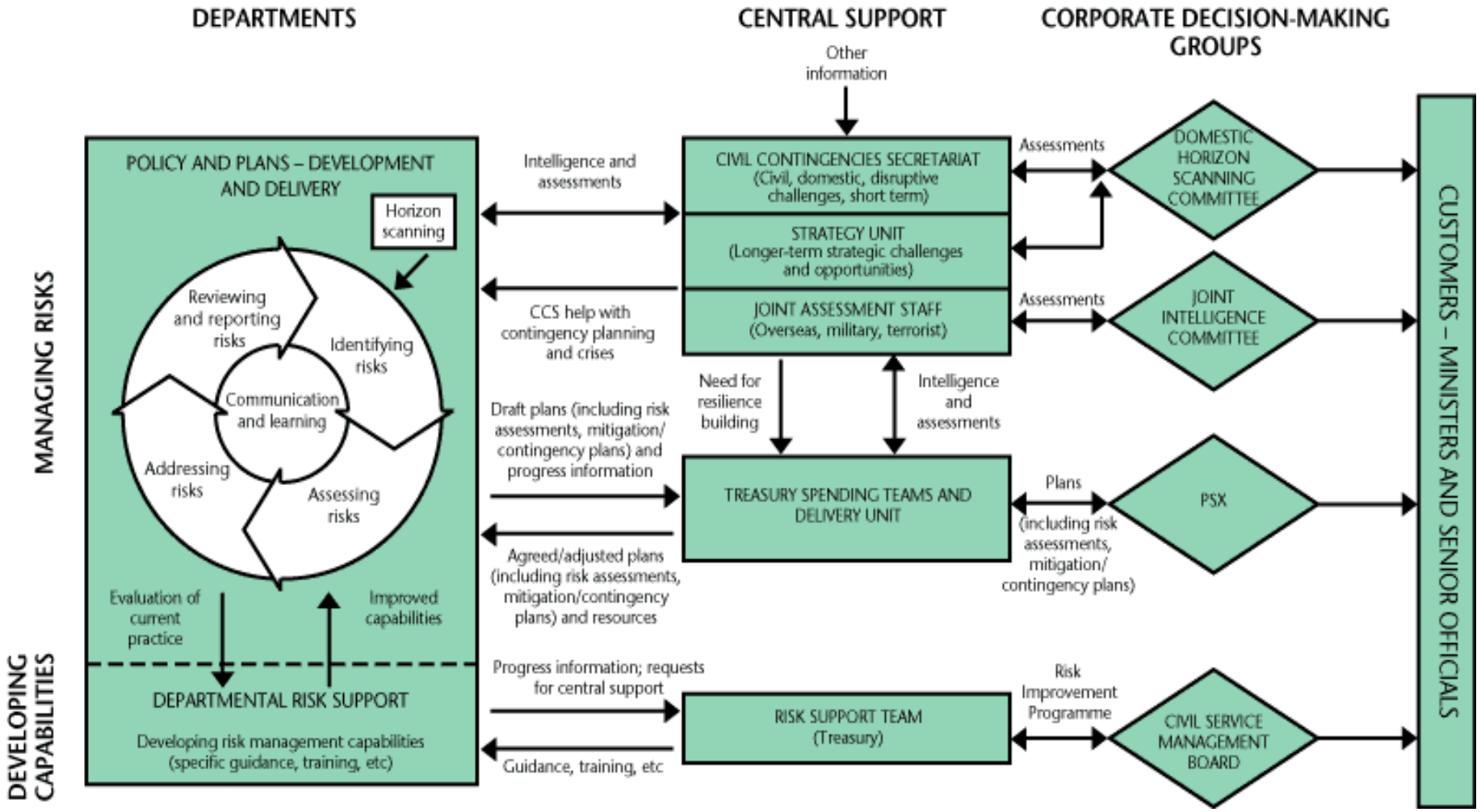
Consequence

- High — Bankruptcy
- Medium — Noticeable effect on the business result
- Low — No effect on the business within the budget

Risk Prioritization / Classification



Risk handling

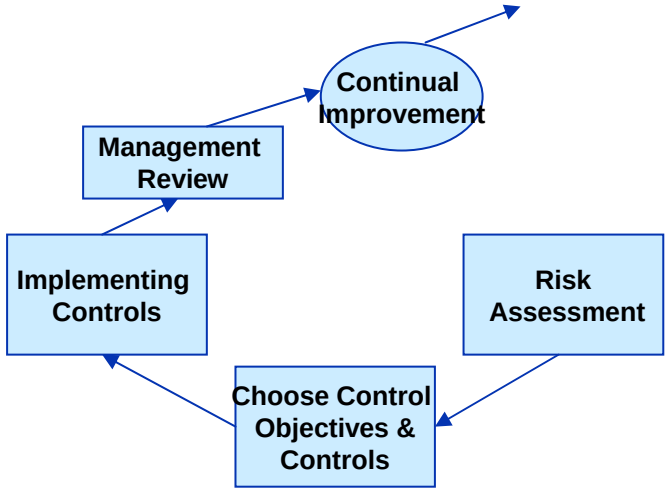


Risk handling

Identification	**Prioritization**	**Risk analysis**
Take away	**Reduce**	**Risk handling**
Lower	**Transfer**	
Insurance	**Excess**	**Risk financing**
Follow UP		

Security Controls - examples

- Security Controls
  - Anti Virus Software
  - Firewalls
  - Authentication
- Preventive Security Controls
  - Physical Access Cards
  - Training
  - Log in/out, Passwords
- Corrective Security Controls
  - Incident Report Analysis and Corrective Action



Software Tools

- COBRA
- Callio Secura
- ezRisk