Understanding Management Systems Concepts

Boğaç ÖZGEN

Lead Auditor

管理

- 计划 – 初始化
- 做 – 实施
- 检查 – 控制过程
- 行动 – 改善活动
- 系统监视

Management

- (PLAN) Planning and Organizing
- (DO) Implementing and realization of plans
- (CHECK) Checking and evaluation
- (ACT) Corrective and preventive actions

- Continual Improvement

Today’s programme

13:00 Management Systems – General Concepts

13:20 TickIT

13:50 Break (10 min)

14:00 Information Security Management System

14:35 Break (5 min)

14:40 IT Service Management

15:15 Questions

15:25 Free time

15:50 Expressing our feelings to meet each other again

BSI – British Standards Institution

A Global Market Leader

- Leading global certification body with over 68,000 certified locations and clients in over 120 countries
- A leader in the assessment and certification of:
  - Information Security – ISO/IEC 27001
  - IT Service Management – ISO/IEC 20000
  - Quality – ISO 9001
  - Quality – ISO 9001 - TickIT
  - Business Continuity – BS 25999

BSI – British Standards Institution

Services

- Information and guidance
- Customer events
- Training
- Second and third-party auditing and verification
- Registration and certification
- Continual assessment and strategic reviews
- Business improvement tools, performance benchmarking and software solutions

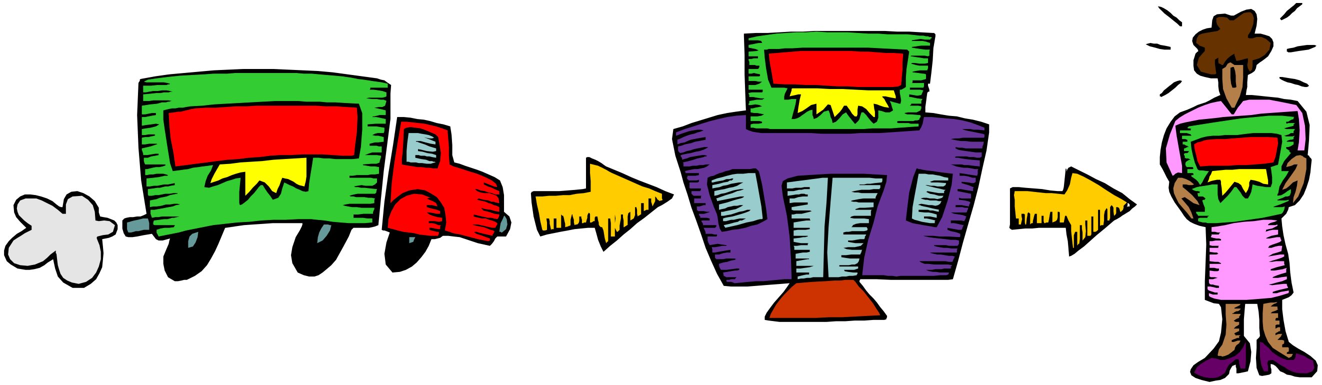
Boğaç ÖZGEN

- Industrial Engineer
- Master of Science degree on “Engineering Management”
- Interest Areas:
  - Software Development
  - Business Intelligence
  - Process Improvement
  - Management Systems
  - IT Governance
  - Risk Management
- Lead Auditor, Consultant and trainer

Management Systems – General Concepts

Management Systems – General Concepts

- Policy
- Scope
- Processes
- Process Management



Management Systems – General Concepts

- Required processes and procedures:
  - Control of Documents
  - Control of Records
  - Internal Audits
  - Corrective Actions
  - Preventive Actions
  - HR – Competency Management
  - Management Review Meetings

Management Systems – General Concepts

- Management Commitment
  - Management Principles
    - Customer focus
    - Leadership
    - Involvement of people
    - Process approach
    - System approach to management
    - Continual improvement
    - Factual approach to decision making
    - Mutually beneficial supplier relationships
  - Resource Management
  - Defining Goals and Targets

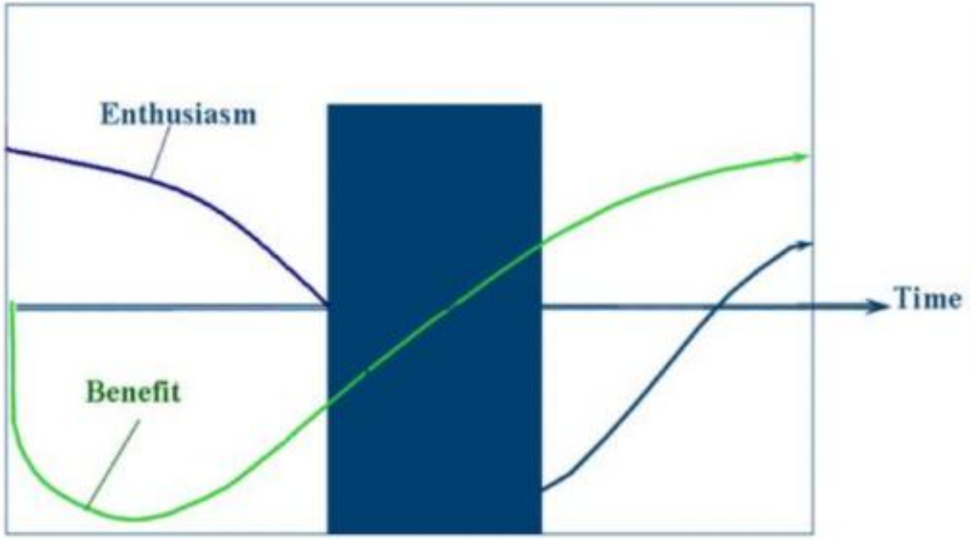
Goals & Targets

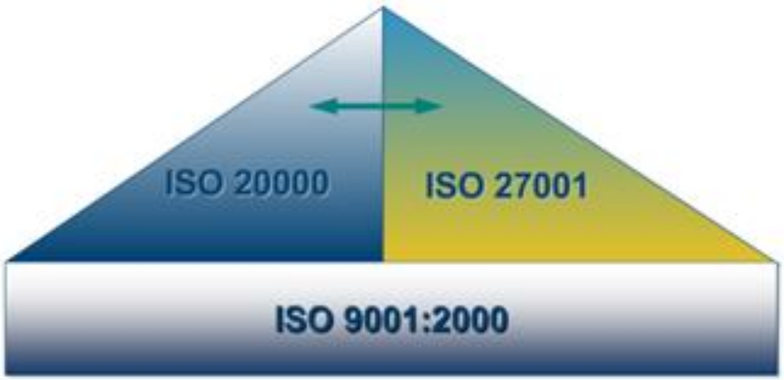
- **Balanced targets**
  - Financials
  - Customer
  - Training
  - Internal Processes
- **SMART Objectives**
  - Specific
  - Measurable
  - Achievable
  - Realistic
  - Time bases

- **Cascading down to activity level**
  - Business Objectives
    - Operational Objectives
      - Process Objectives
        - Activity Objectives

Please be patient, be strategic...!

Allow time!

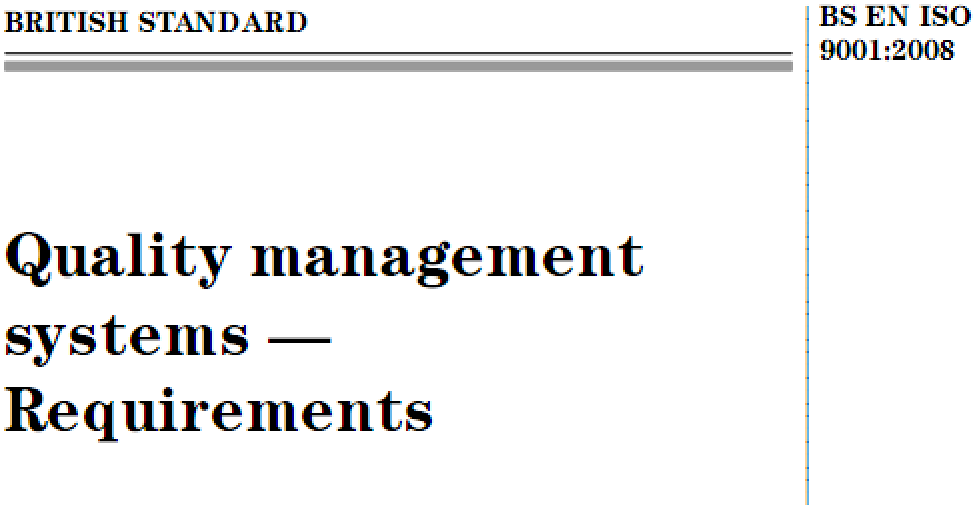




Summary of
Management Systems General Concepts

- Policy and Scope
- Process Management
- Management Commitment
- Goals and Targets
- Internal audits
- Continual Improvement
- HR – Competency Management

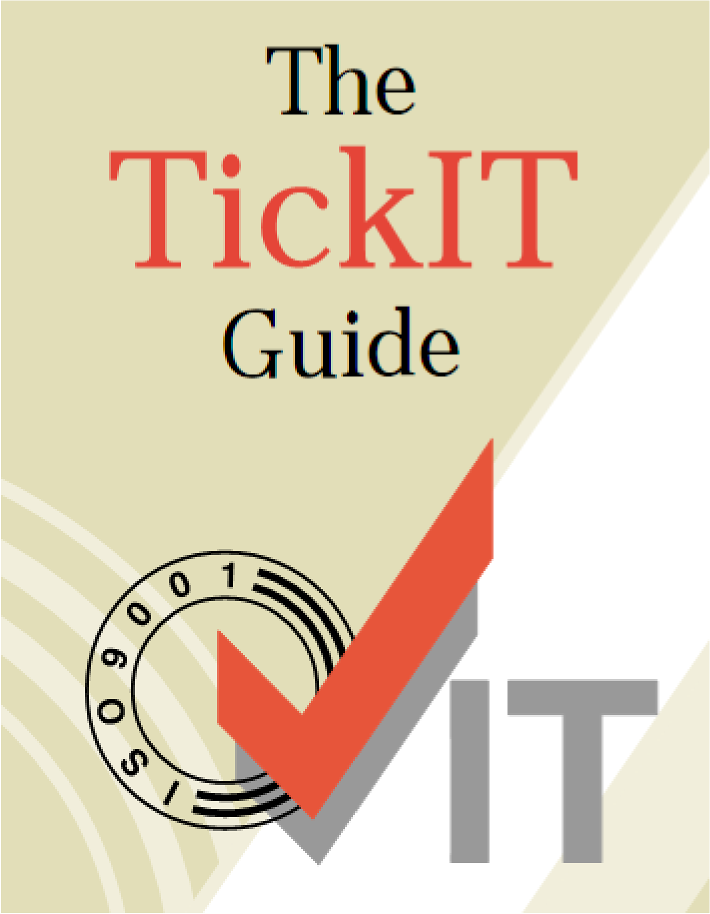
ISO9001:2008 – TickIT Scheme



BRITISH STANDARD

BS EN ISO
9001:2008

Quality management systems — Requirements



The TickIT Guide

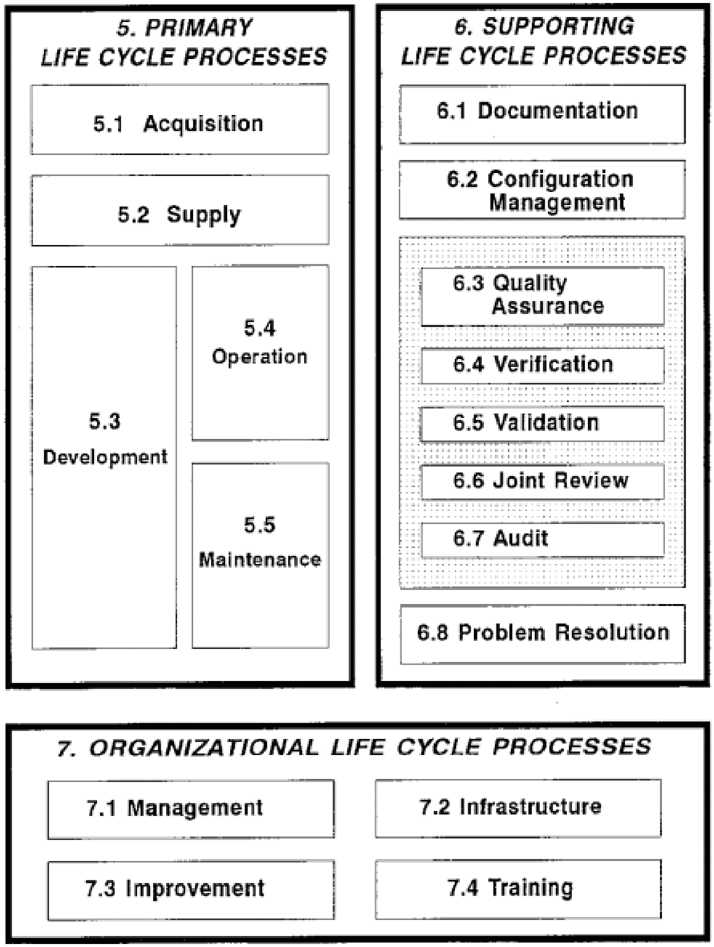
TickIT

- What is TickIT?
  - TickIT is implementation of **ISO9001** Standard onto the systems providing Software Development processes.
    - Desktop applications
    - Web applications
    - Portal development
    - Linux, Unix or other OS dependent systems
    - Linux run refrigerators
    - SCADA Systems
    - ...

TickIT Guidance

- Software sector guidance is available in
  - ISO 90003
    - Software engineering — Guidelines for the application of ISO 9001:2000 to computer software
  - TickIT Guide
    - TickIT Guide Section E and ISO 90003:2004 overlapping at some degree
    - Organisations are not required to satisfy guidance
  - ISO 12207
    - Information technology— Software life cycle processes

ISO12207 - Information technology Software life cycle processes



5. PRIMARY LIFE CYCLE PROCESSES

5.1 Acquisition

5.2 Supply

5.3 Development

5.4 Operation

5.5 Maintenance

6. SUPPORTING LIFE CYCLE PROCESSES

6.1 Documentation

6.2 Configuration Management

6.3 Quality Assurance

6.4 Verification

6.5 Validation

6.6 Joint Review

6.7 Audit

6.8 Problem Resolution

7. ORGANIZATIONAL LIFE CYCLE PROCESSES

7.1 Management

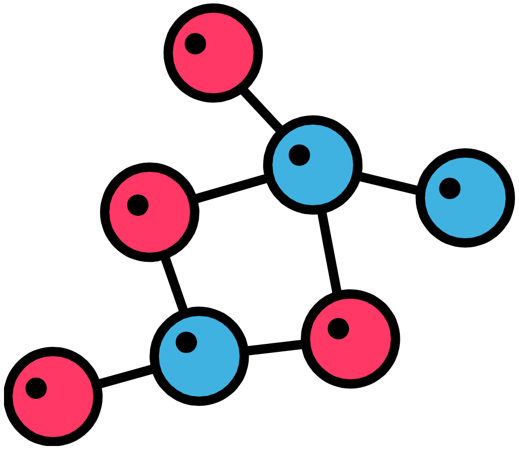
7.2 Infrastructure

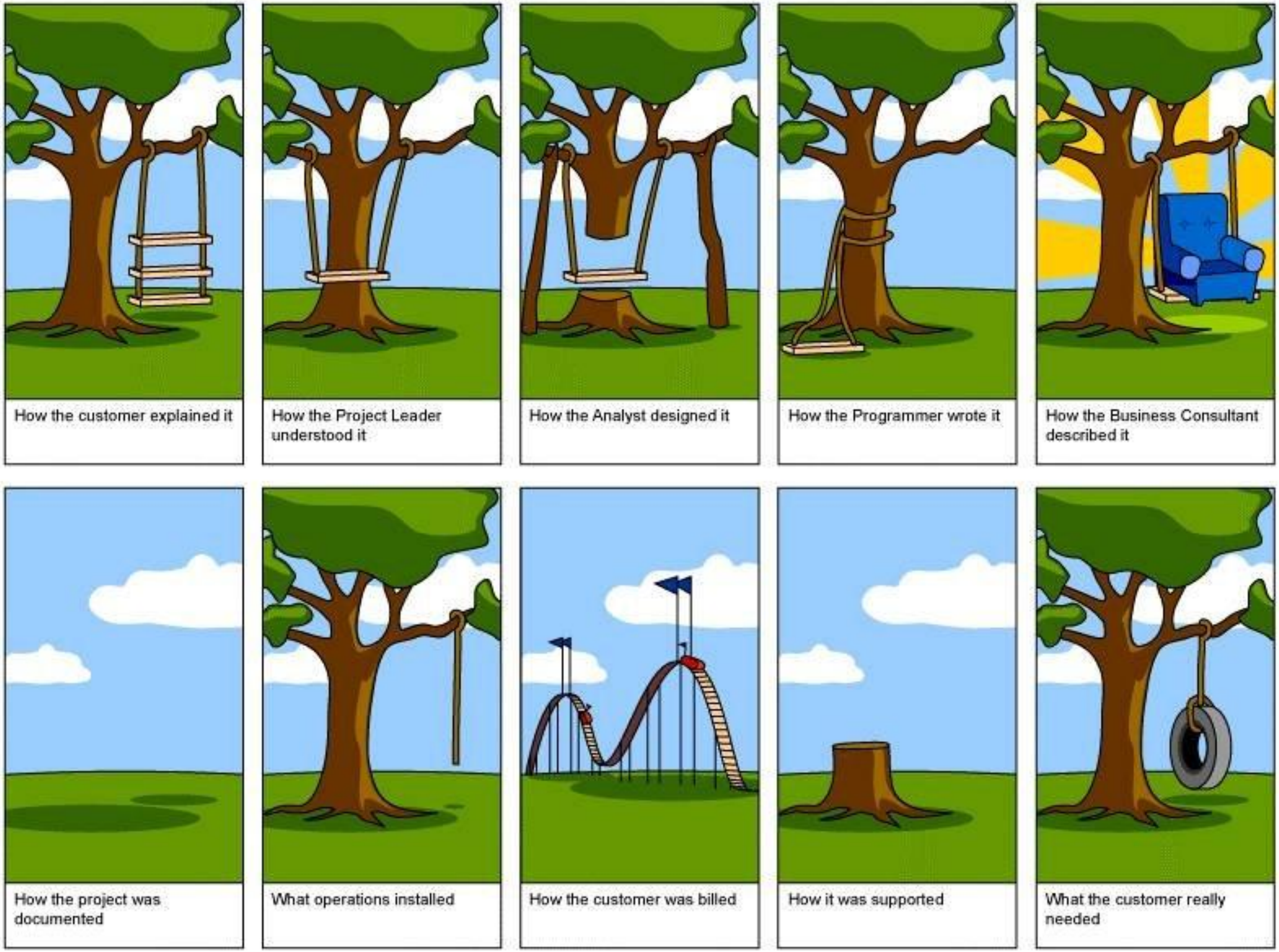
7.3 Improvement

7.4 Training

Software Development Models

- Instinctive (no structured testing)
- Creative (there is unit testing)
- Waterfall (starting of standard development models)
- V Model
- Spiral
- Prototyping
  - Agile (an approach)
  - RUP
  - eXtreme Programming
  - RAD/JAD
  - DSDM
  - ...




How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed

TickITPlus – A new approach Capability Dimension

- Level 2 : **Bronze**: Managed

  (Starting point to transfer from current TickIT)
- Level 3 : **Silver** : Established
- Level 4 : **Gold** : Predictable
- Level 5 : **Platinum** : Optimising
  - Based on ISO/IEC 15504-2 – SPICE

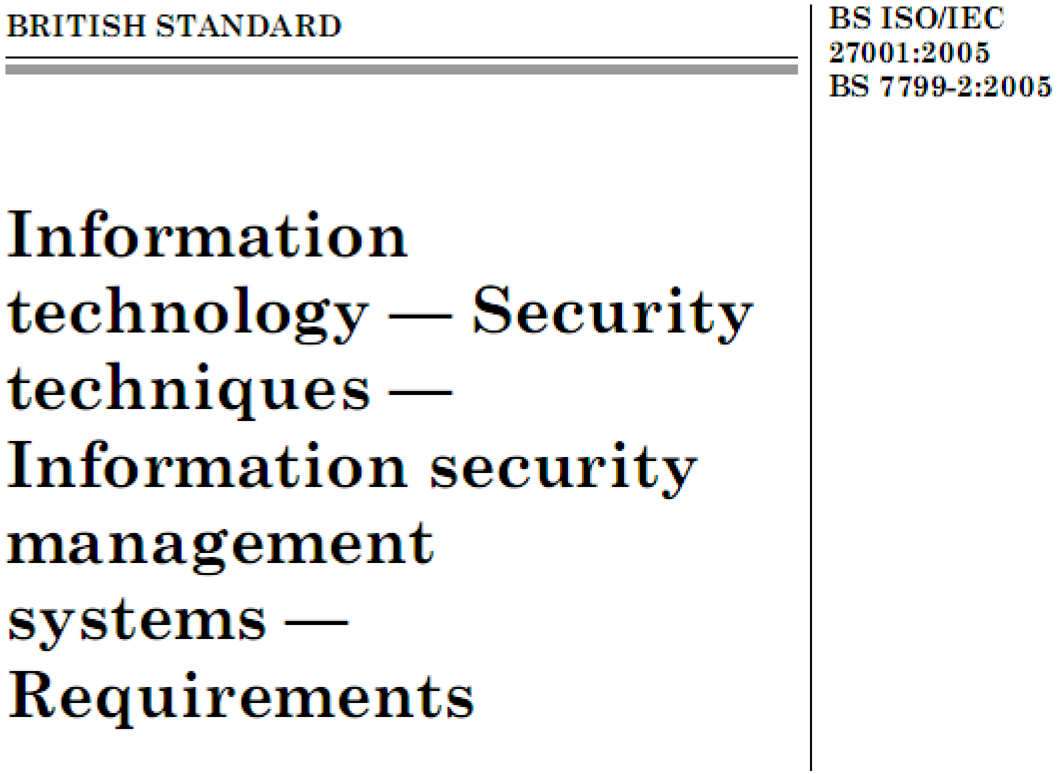
http://www.TickITPlus.org

Summary of **TickIT**

- Implementation of ISO9001
- Guidance Documents
  - TickIT Guide
  - ISO90003
  - ISO12207
- Software Development Models
- Software Development Processes
- TickITPlus is coming

Break – 10 min.

ISO27001:2005
Information Security Management System



BRITISH STANDARD

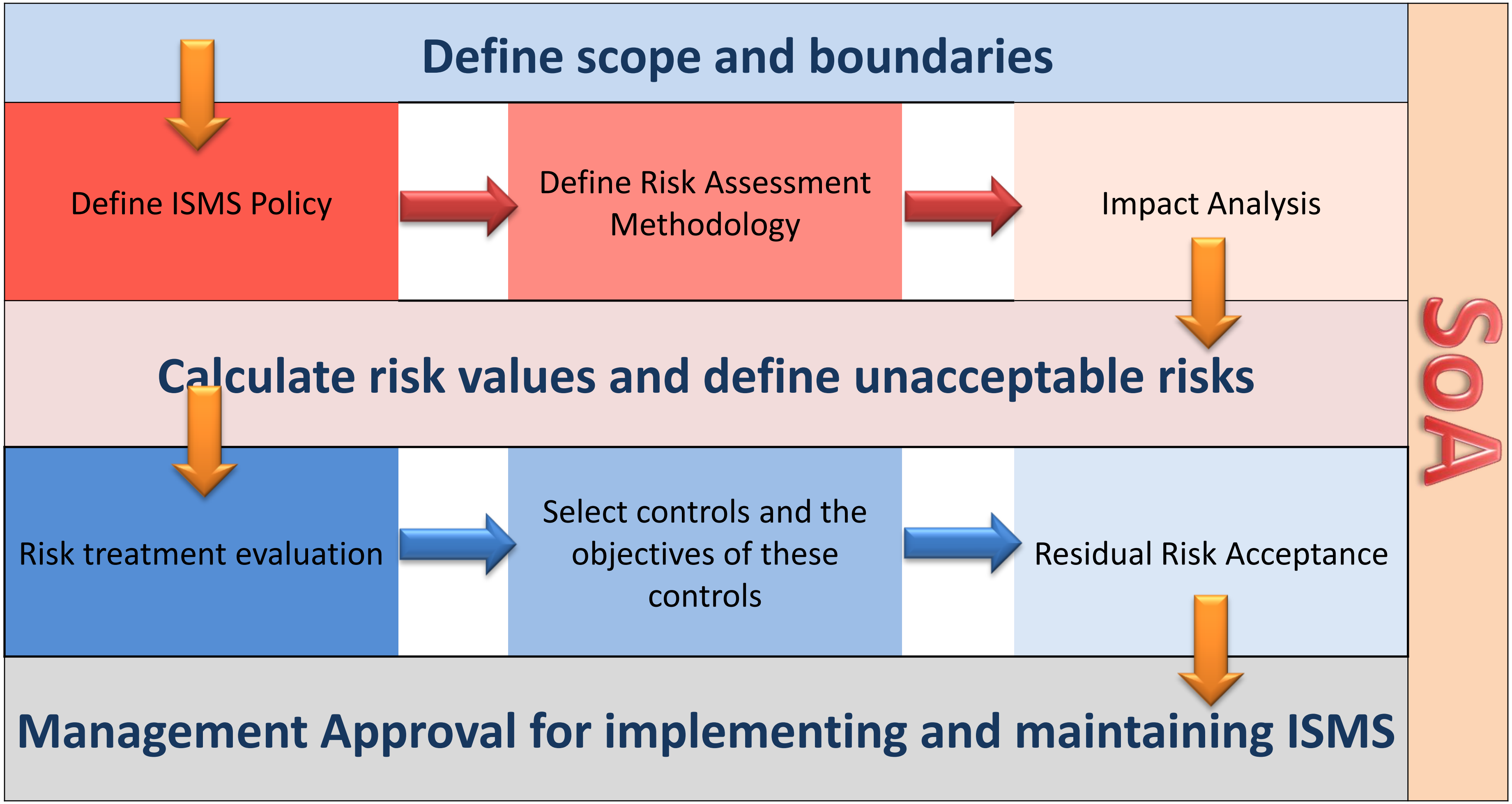
BS ISO/IEC
27001:2005
BS 7799-2:2005

Information technology — Security techniques — Information security management systems — Requirements

ISMS

- What is Information Security?
- What is Information Security Management System?
- What are assets?
- What are threats?
- What are vulnerabilities?
- What is impact analysis on CIA?
- What is risk?

ISMS Implementation



Define scope and boundaries

Define ISMS Policy

Define Risk Assessment Methodology

Impact Analysis

Calculate risk values and define unacceptable risks

Risk treatment evaluation

Select controls and the objectives of these controls

Residual Risk Acceptance

Management Approval for implementing and maintaining ISMS

Statement of Applicability (SoA)

- A.5 Security policy
- A.6 Organization of information security
- A.7 Asset management
- A.8 Human resources security
- A.9 Physical and environmental security
- A.10 Communications and operations management
- A.11 Access control
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management
- A.14 Business continuity management
- A.15 Compliance

Aspects of Corporate Information Security

- Privacy issues
- Identity Theft
- Web pages
- Firewalls
- Employee surveillance
- Electronic commerce
- Digital signatures
- Computer viruses
- Encryption
- Contingency planning
- Logging controls
- Internet
- Intranets
- Corporate Governance
- Outsourcing security functions
- Computer emergency response teams
- Microcomputers
- Local area networks
- Voice Over IP
- Password selection
- Electronic mail
- SPAM Prevention
- Data Classification
- Telecommuting
- Telephone systems
- Portable computers
- User security training
- Information Security Related Terrorism
- …

Summary of **ISO27001 – ISMS**

- Risk Management
- Asset Register
  - Threats
  - Vulnerabilities
  - Impact
- Risk Treatment and Controls
- Statement of Applicability
- Risk acceptance and Residual risk
- Effectiveness

Break – 5 min.

ISO20000:2005
IT Service Management

BRITISH STANDARD

BS ISO/IEC
20000-1:2005

Information technology — Service management —

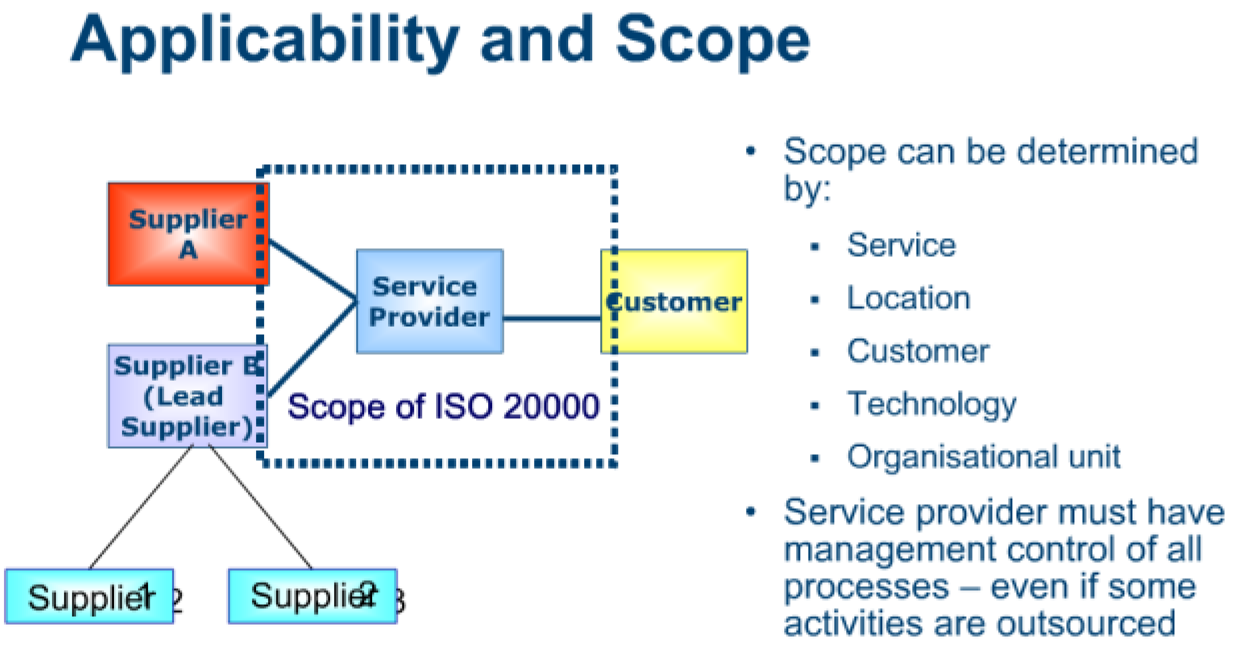
Part 1: Specification

What is IT Service Management?

IT Service Management System

- ISO20000-1:2005; Specification
- ISO20000-2:2005; Code of practice
- It is not ITIL (IT Infrastructure Library).
- PDCA Cycle is applicable.

IT Service Management - Scope



Applicability and Scope

- Scope can be determined by:
  - Service
  - Location
  - Customer
  - Technology
  - Organisational unit
- Service provider must have management control of all processes – even if some activities are outsourced

IT Service Management - Processes

- **Service Management and Improvement**
  - Planning and implementing service management
  - Implement service management and provide the services
  - Planning and implementing new or changed services
- **Service Delivery**
  - Service level management
  - Service reporting
  - Service continuity and availability management
  - Budgeting and accounting for IT services
  - Capacity management
  - Information security management
- **Relationship processes**
  - Business relationship management
  - Supplier management
- **Resolution processes**
  - Incident management
  - Problem management
- **Control processes**
  - Configuration management
  - Change management
- **Release process**
  - Release management process

Service Management Processes

- Planning and implementing service management
  - Plan service management
- Implement service management and provide the services
  - Policy
  - Management Plans
  - Activities
  - Monitoring, measuring and reviewing
  - Continual improvement
  - Management of improvements
- Planning and implementing new or changed services

Service Delivery Processes

- Service level management
- Service reporting
- Service continuity and availability management
- Budgeting and accounting for IT services
- Capacity management
- Information security management

Relationship Processes

- Business relationship management
- Supplier management

Resolution processes

- Incident management

  (Correction in ISO9001)

- Problem management

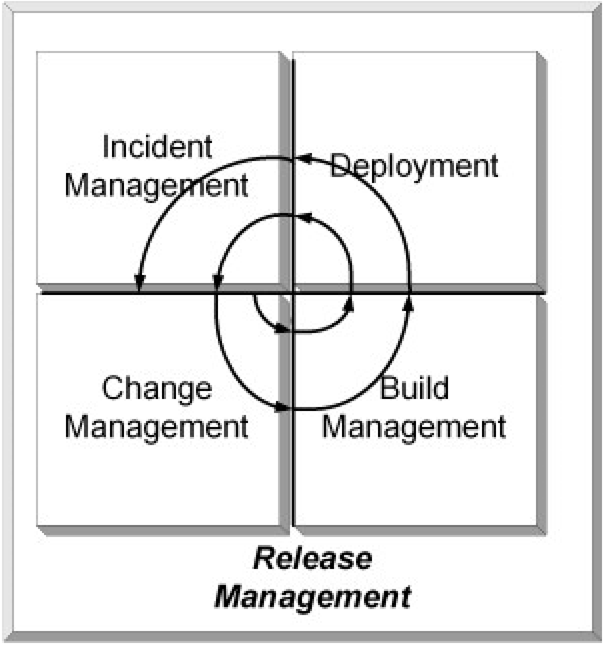
  (All kinds of preventive actions in ISO9001)

Control processes

- Configuration management
- Change management

Release process

- Release management process



Summary of
ISO20000 – ITSM

- ISO20000 is not ITIL
- Service Management Framework
- Service Delivery
- Service Management and Support
- **Informally as a best practice:**
  - It can be used by all parties and in all sectors:
    - Service Provider
    - Service Acceptor

Summary of **The Presentation**

- Management Systems are best practices
- Common Sense
- Think simple
- **Your way is the best way...**

...until the best practices !!!

You need to improve continually.

BSI – British Standards Institution

A Global Market Leader

- Leading global certification body with over 68,000 certified locations and clients in over 120 countries
- A leader in the assessment and certification of:
  - Information Security – ISO/IEC 27001
  - IT Service Management – ISO/IEC 20000
  - Quality – ISO 9001
  - Quality – ISO 9001 - TickIT
  - Business Continuity – BS 25999

BSI – British Standards Institution

Services

- Information and guidance
- Customer events
- Training
- Second and third-party auditing and verification
- Registration and certification
- Continual assessment and strategic reviews
- Business improvement tools, performance benchmarking and software solutions

BSI – British Standards Institution

- BSI Contact details
  - **Ridvan Yaldizkaya – Sales & Marketing Manager** [Ridvan.Yaldizkaya@bsigroup.com]
  - **Ozlem Unsal – Country Manager** [Ozlem.Unsal@bsigroup.com]
  - Telephone: +90 (216) 445 90 38

Questions ?

Thank you very much for your attendance...

Understanding Management Systems Concepts

Boğaç ÖZGEN
Lead Auditor

References

- BSI ITSM webinar presentation
- PERA - TickIT Auditor Training Course
- WikiPedia
- http://www.swan.ac.uk/university/StaffInformation/RiskManagement/WhatisRiskManagement/
- http://www.itilpeople.com/Glossary/Glossary_i.htm
- http:// wordnet.princeton.edu/perl/webwn
- http://www.TickITPlus.org
- http://www.BSI-Global.com

Thank you...

- BSI Contact details
  - **Ridvan Yaldizkaya – Sales & Marketing Manager** [Ridvan.Yaldizkaya@bsigroup.com]
  - **Ozlem Unsal – Country Manager** [Ozlem.Unsal@bsigroup.com]

Telephone: **+90 (216) 445 90 38**

- Contact details
  - **Boğaç ÖZGEN** [Bogac.Ozgen@GyroFalco.com]

Telephone: **+44 (79) 6843 6880**