INF3510 Information Security
University of Oslo
Spring 2010

Lecture 11

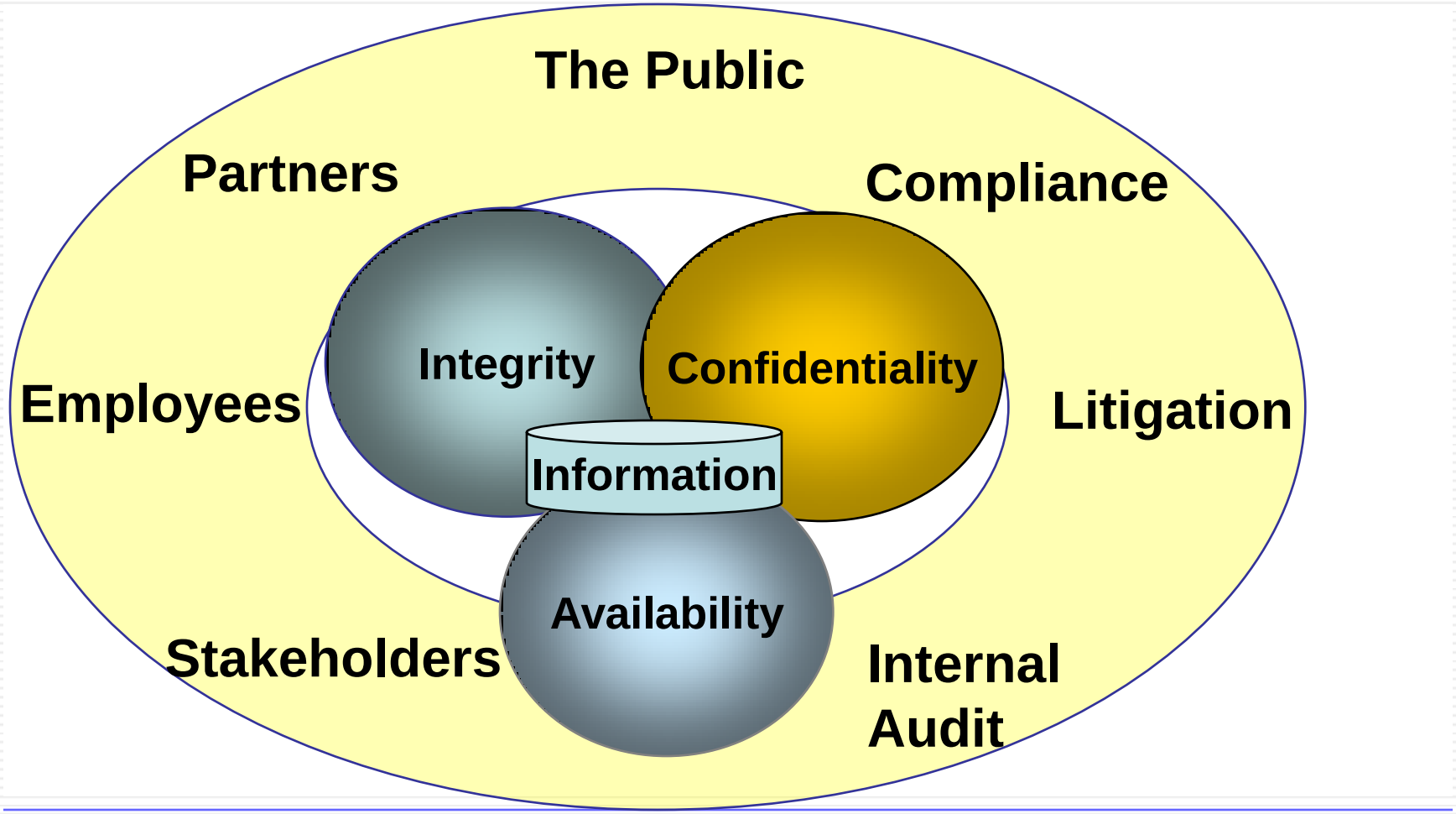
Security Management and Secure Systems Development

Audun Jøsang

Outline

- Information Security Management
  - ISO 27002 Code of practice for information security management
  - ISO/IEC 27001 Information Security Management Systems
- Secure Systems Development
  - Microsoft SDL
  - Other approaches

Context for IS Management



Who is responsible for ISM?

- Consider these groups:
  - Management
    - CEO, CSO, CIO
  - General security staff
  - IT staff
  - Users
  - Third parties
    - Outsourced information security management
    - Customers, suppliers, business partners

Who is responsible for ISM?

- Management
  - Strong and consistent support required for successful ISM
  - Demonstrate commitment to information security through:
    - allocation of resources and personnel;
    - endorsement of information security policy;
    - abiding by information security policy,

Who is responsible for ISM?

- General security staff
  - Information security as a division of general security
    - Physical security impacts on information security
    - General security staff have procedures in place e.g. monitoring access, liason with police
  - May require technical expertise

Who is responsible for ISM?

- IT staff
  - Staff have required technical skills to:
    - manage technology
    - understand security issues and control measures
  - Information security is not just a technology issue
  - Dependence/independence of information security and IT:
    - Monitoring of IT department by IT department?
    - Conflict in relationships with other departments

Who is responsible for ISM?

- Users
  - Create, access and distribute information as part of their regular tasks
  - Security requirements may conflict with essential business activities the users carry out
  - Training required so that users understand the security implications of simple actions – e.g. forwarding email

Who is responsible for ISM?

- Third parties
  - Outsourced information security management
    - Experienced, expert
    - Separation of responsibilities: not aligned with staff
    - What to outsource?
    - How to evaluate the service provided?
  - Customers, suppliers, business partners
    - Investigate security implications
  - Contractors

Who is responsible for ISM?

- Information security is a chain of protection:
  - Only as strong as the weakest link
  - Need co-operation and collaboration at all levels, across an organisation
  - Individuals need to know:
    - what the goals are
    - why they are important
    - their duties and responsibilities
    - how their actions impact on information security

IS Management Standards: Why?

- They provide:
  - evidence of management commitment to, and responsibility for, IS: Management must simultaneously justify the cost and the limitations of security measures.
  - assurance to other departments and organizations: Use of networks increasingly implies that security vulnerabilities will impact upon others - other departments, other organizations, customers, trading partners, etc.
  - assurance to staff: If staff are to be held accountable for their actions regarding information security, they need assurance from the organization of their rights and responsibilities.
  - a checklist of measures: ISM standards provide guidelines on best practice or widely accepted methods for controlling information security through an ISMS and can be used as checklists for important aspects of ISM.

IS Management Standards

- ISO Security Management standards:
  - ISO/IEC 27002 Information Technology – Code of practice for information security management
  - ISO/IEC 27001 Information Security Management Systems
- USA
  - NIST (National Institute for Standards and Technology) Special Publications, including SP800-12, SP800-14, SP800-18, SP800-26 and SP800-30, SP800-64

Information Security Standards

- Are there any other places to find checklists of security measures?
  - CERT/CC - Computer Emergency Response Team Coordination Center
    - http://www.cert.org/nav/
  - NSM – Norsk Sikkerhetsmyndighet
    - https://www.nsm.stat.no/Publikasjoner/
  - SCORE – Security Consensus Operational Readiness Evaluation
    - http://www.sans.org/score/

ISO/IEC 27002– What is it?

Code of practice for information security management

- "… establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization."
- Basically an internationally recognised generic information security standard

Objective:

- "… to provide practical guidelines for developing organizational security, standards and effective security management practices and to help build confidence in inter-organizational activities."

ISO/IEC 27002 - History

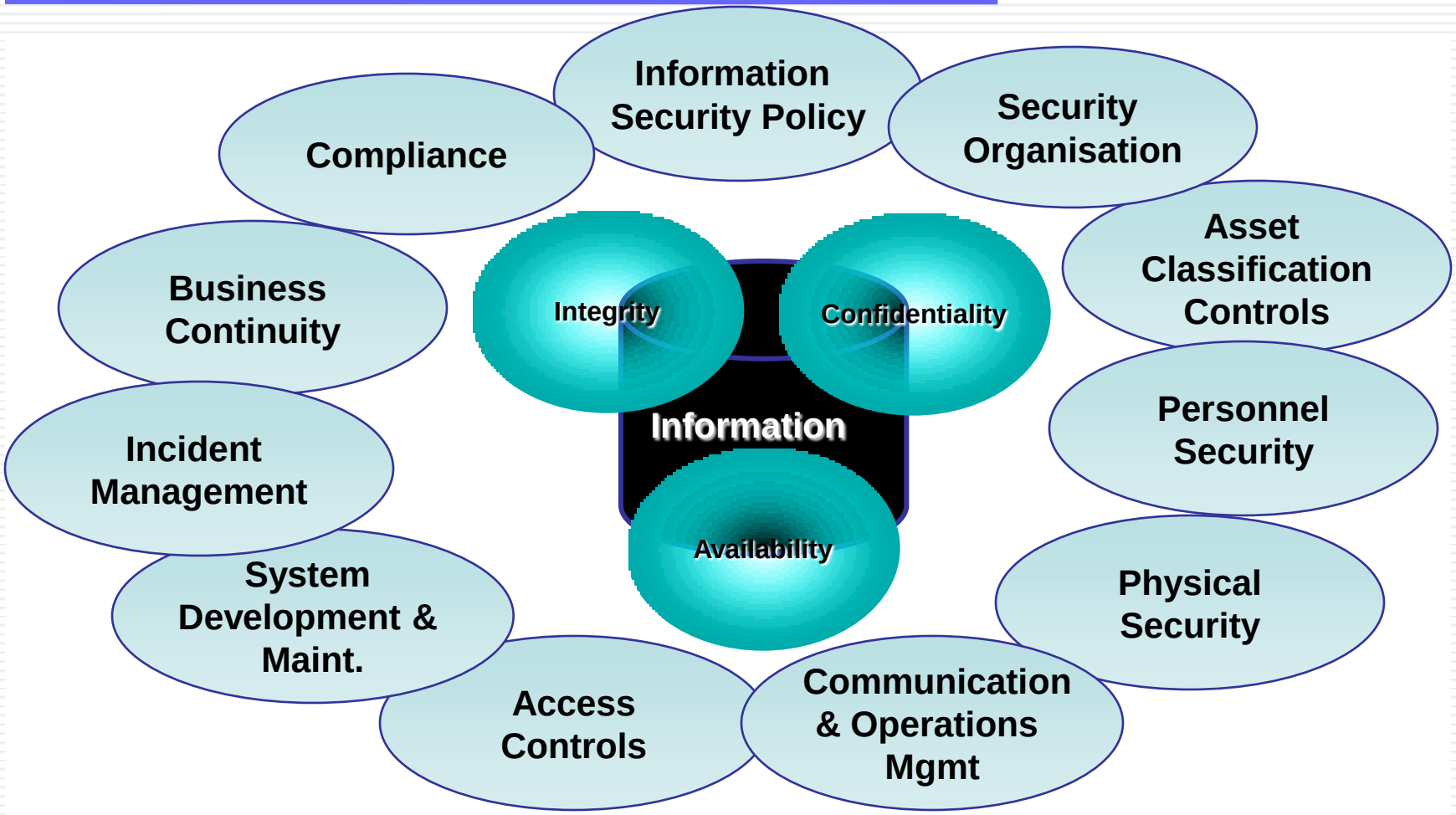
- In early 1990's, recognized need for a practical guide for information security management
  - Group of leading companies in the UK combined to develop the Code of Practice for Information Security Management (now BS 7799 Part 1 Code of Practice)
  - Published as BS7799 version 1 in Feb 1995
  - Adopted as AS/NZS4444:1996
  - New version of BS 7799 adopted as ISO/IEC 17799:2001
  - Updated to AS/NZS ISO/IEC 27002 2005.

Structure of ISO/IEC 27002

- ISO/IEC 27002 identifies:
  - 11 essential security objectives with corresponding controls as a basis for Information Security Management.
  - includes 133 controls

"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 organization."

The 11 Objectives of ISO/IEC 27002



ISO/IEC 27002 - IS Policy

Information security policy

- Objective: To provide management direction and support for information security

- *"Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization"*.

ISO/IEC 27002– IS Policy

Information security policy document

- Should be
  - Approved by management
  - Published and communicated to all employees
- Should state management commitment and set out organisation's approach to managing information security
- At a *minimum*, should include:
  a) definition of information security, its overall objectives and scope …
  b) Statement of management intent …
  c) A framework for setting control objectives and controls including risk assessment and risk management

ISO/IEC 27002 - IS Policy

Information security policy document

- Should include (continued):

d) Brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation, e.g.
   - Compliance with legislative and contractual requirements
   - Security education requirements
   - Prevention and detection of viruses …
   - Business continuity management
   - Consequences of security policy violations

ISO/IEC 27002 - IS Policy

Information security policy document

- Should include (continued):
  - e) definition of general and specific responsibilities for information security management including reporting security incidents
  - f) References to documentation which may support the policy, e.g.
    - More detailed security policies and procedures for specific information systems
    - Security rules for users

ISO/IEC 27002 - IS Policy

Review and evaluation

- Policy should have a defined owner responsible for development, review and evaluation according to a defined review process
- When to review?
  - In response to changes affecting original risk assessment e.g.
    - Significant security incident
    - New vulnerabilities
  - At periodic scheduled times

ISO/IEC 27002 - Security Organisation

- **Objective:**
  - To manage information security within the organisation
  - To maintain the security of organisational information processing facilities and information assets accessed by third parties;
- **Subjects covered:**
  - Management commitment
  - Information security co-ordination
  - Allocation of security responsibilities
  - Authorisation process for information processing facilities
  - Confidentiality agreements
  - Contact with authorities and special interest groups
  - Independent review
  - Identification of risks related to external parties
  - Dealing with customers and third party agreements

ISO/IEC 27002 - Asset Management

- **Objective:**
  - To achieve and maintain appropriate protection of organizational assets.
- **Subjects covered:**
  - Responsibility for assets, including establishing an asset inventory for hardware, software, information, services and people
  - Information classification including advice on labelling and handling assets
    - NB: Classifying and labelling assets is a pre-requisite for a Threat/Risk Assessment

ISO/IEC 27002 – Human Resources Security

- **Objective:**
  - To ensure that employees, contractors and third party users understand their responsibilities and are suitable for their roles
  - To reduce the risk of theft fraud or misuse of facilities and reduce the risk of human error
- **Subjects covered:**
- **Prior to employment**
  - Defining roles and responsibilities;
  - screening;
  - terms and conditions.

ISO/IEC 27002– Human Resources Security

- **Subjects covered (continued):**
- **During employment**
  - Management responsibilities;
  - information security awareness, education and training;
  - disciplinary process.
- **Termination of change of employment**
  - Termination responsibilities;
  - return of assets;
  - removal of access rights.

ISO/IEC 27002– Physical/Environmental Security

- **Objective:**
  - To prevent unauthorised physical access, damage and interference to the organization's premises and information;
  - To prevent loss, damage, theft or compromise of assets and interruption to organizational activities.

- **Subjects covered:**
  - need to establish secure areas with defined perimiters and appropriate barriers and entry controls;
  - need to physically protect hardware equipment to prevent theft;
  - need to protect network cabling from tampering;
  - security of equipment taken off site or sent for disposal.

ISO/IEC 27002– Communications and Operations Management

- **Objective:**
  - To ensure the correct and secure operation of information processing facilities;
  - To implement and maintain the appropriate level of information security and service delivery in line with third party agreements;
  - To minimise the risk of systems failures;
  - To protect the integrity of software and information;
  - To maintain the integrity and availability of information processing and information processing facilities;
  - To ensure the protection of information in networks and the protection of the supporting infrastructure;
  - To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruptions to business activities;
  - To maintain the security of information and software exchanged within and between organizations;
  - To ensure the security of electronic commerce services;
  - To detect unauthorized information processing activities.

ISO/IEC 27002– Comms. & Ops. Mgmt

- Large section that deals with security for computer systems
- Explains main areas of risk, but stops short of explaining technical measures necessary
- Subjects covered:
  - Viruses
  - Malicious software
  - Change control
  - Backup
  - The keeping of accurate access logs
  - Security of system documentation
  - Media handling
  - Protection and authentication of data during transfers and in transit
  - Security of Email and on-line transactions
  - Monitoring and logs

ISO/IEC 27002– Access Control

- **Objective:**
  - To control access to information;
  - To ensure authorized access to information systems;
  - To prevent unauthorized access to information systems, including networked services, operating systems and application systems;
  - To prevent unauthorized computer access;
  - To detect unauthorized activities;
  - To ensure information security when using mobile computing and teleworking facilities**.**
- **Subjects covered:**
  - Access control and how it can be applied to different types of system
  - User registration
  - Issue and usage of passwords
  - Clear desk and clear screen policy
  - Automatic terminal time outs
  - Policy on use of network services
  - Mobile computing policy

ISO/IEC 27002– Systems Acquisition, Development and Maintenance

- **Objective:**
  - To ensure security is an integral part of information systems;
  - To prevent errors, loss, modification or misuse of information in applications;
  - To protect confidentiality, authenticity and integrity of information by cryptographic means;
  - To ensure the security of system files;
  - To maintain security of application system software & data;
  - To reduce risks resulting from exploitation of published technical vulnerabilities.
- **Subjects covered:**
  - acquisition of new systems and modification to existing ones;
  - procedures for software development and maintenance;
  - cryptographic controls.

ISO/IEC 27002 - Security Incident Management

- Objective:
  - To ensure security events and weaknesses are communicated in a manner allowing timely corrective action;
  - To ensure a consistent and effective approach to the management of security incidents.
- Subjects covered:
  - Reporting of events
  - Reporting security weaknesses
  - Collecting evidence

ISO/IEC 27002– Business Continuity

- **Objective:**
  - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

- **Subjects covered:**
  - an overview of the case for a comprehensive business continuity plan which should be designed, implemented, tested and maintained.

ISO/IEC 27002– Compliance

- **Objective:**
  - To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements;
  - To ensure compliance of systems with organizational security policies and standards;
  - To maximize the effectiveness of, and to minimize interference to/from, the information systems audit process.
- **Subjects covered:**
  - Intellectual property rights;
  - Organizational records;
  - Regulation of cryptographic controls;
  - Personal information;
  - Audit controls.

ISO/IEC 27001:2005

Information Security Management Systems – Requirements

- This new international version of the standard clarifies and strengthens some requirements of the original British standard, and includes changes to the following areas:
  - risk assessment,
  - contractual obligations,
  - scope,
  - management decisions,
  - measuring the effectiveness of selected controls.

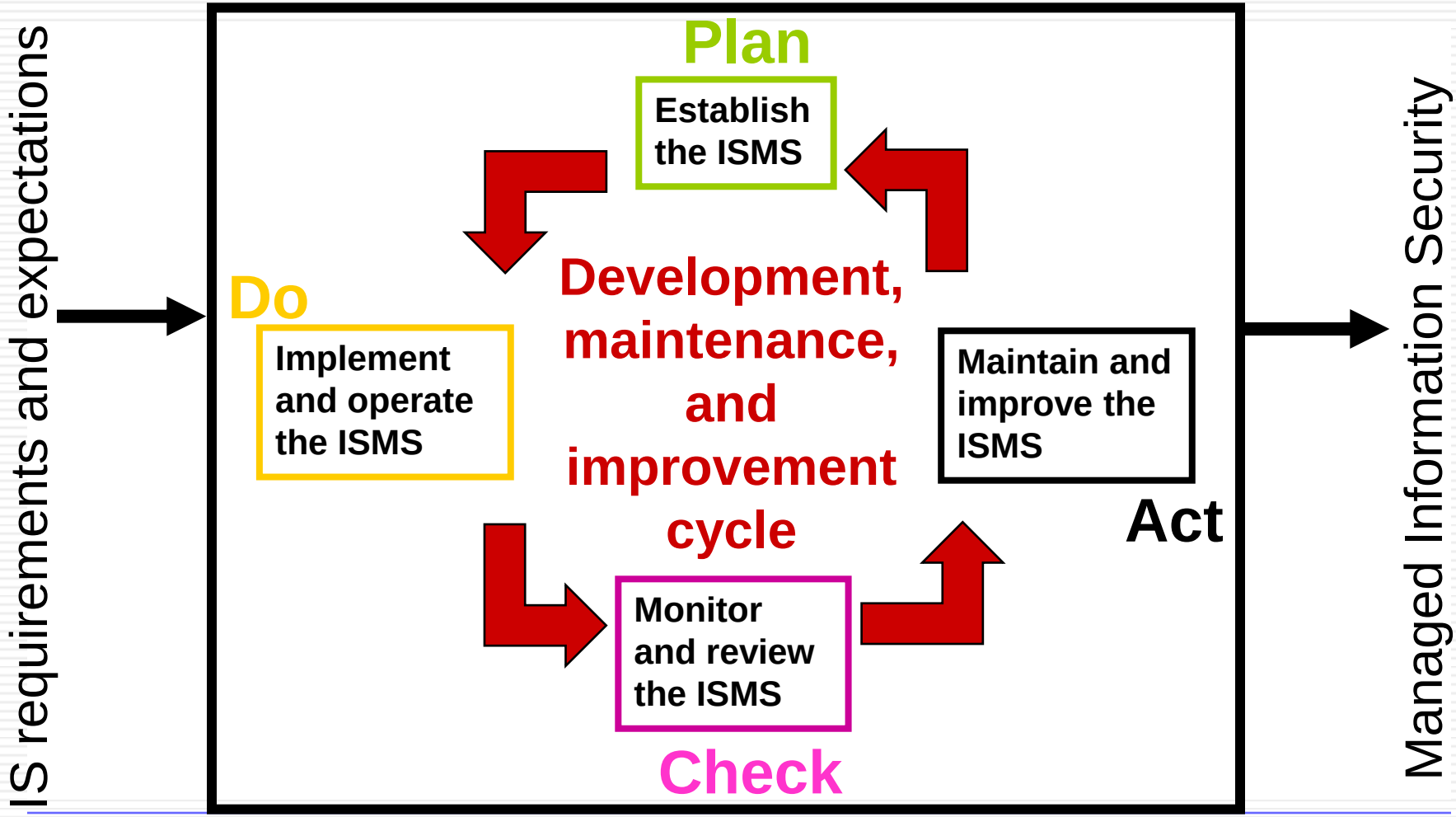
ISO/IEC 27001- What is it?

- Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS (Information Security Management System)
- A comprehensive approach to information security management
- Not just a set of goals and controls as in the code of practice ISO/IEC 27002
- Organisations can be certified against ISO/IEC 27001
- To be used in conjunction with ISO/IEC 27002
- Based on a Plan-Do-Check-Act (PDCA) model

ISO/IEC 27001- History

- The need to establish a certification scheme for information security management emerged late 1990s
- A general approach to security management was needed for certification purposes, not just a code of practice as in BS:7799:1995
- BS 7799.2:1999 created to define a comprehensive ISMS (Information Security Management System) against which certification was possible.
- Led to the dramatic conclusion that **the concept of an ISMS is perhaps of far greater and fundamental importance than the original Code of Practice**.

ISO/IEC 27001- The PDCA Model



ISO/IEC 27001- Plan Phase

- Establish the ISMS
- Purpose: Establish policy, objectives, processes and procedures
- Steps:
  - Define scope and boundaries
  - Define an ISMS policy
  - Define risk assessment approach of the organization
  - Identify the risks
  - Analyse and evaluate the risks
  - Identify and evaluate options for the treatment of risks
  - Select control objectives and controls for the treatment of risks
  - Obtain management approval and authorization
  - Prepare a statement of applicability

ISO/IEC 27001- Do phase

- Implement and operate the ISMS
- Purpose: Implement selected controls, and promote actions to manage identified risks
- Steps:
  - Formulate and implement the risk treatment plan
  - Implement the controls selected in the Plan phase
  - Define how to measure the effectiveness of the selected controls
  - Implement training and awareness programs
  - Manage operations and resources
  - Implement procedures and other controls capable of enabling prompt detection of, and response to security incidents

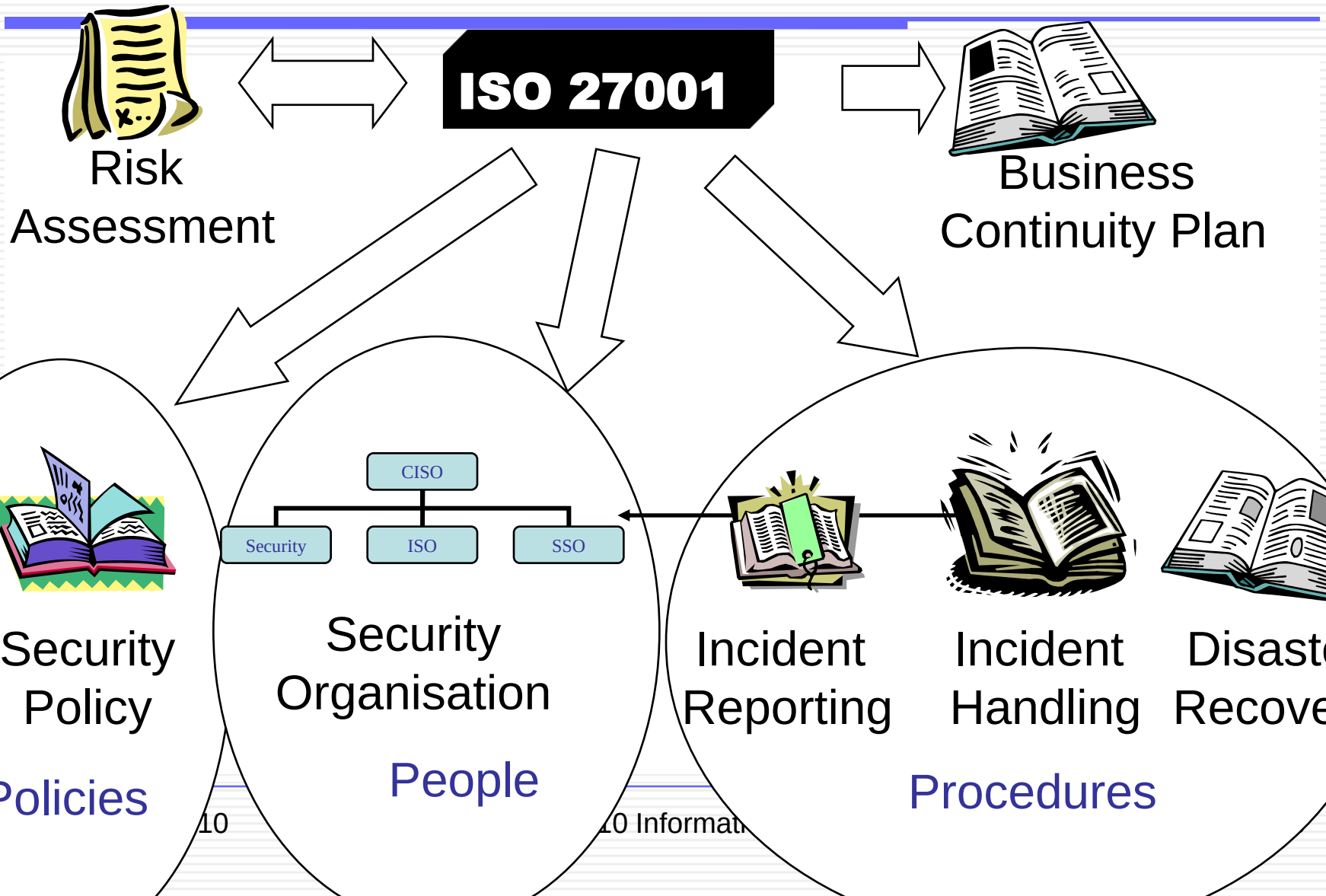
ISO/IEC 27001- Check phase

- Monitor and review the ISMS
- Purpose: to ensure that controls are working effectively
- Steps:
  - Execute monitoring procedures and other controls
  - Regularly review the effectiveness of the ISMS
  - Measure the effectiveness of controls
  - Review the level of residual risk and acceptable risk
  - Conduct internal ISMS audits at planned intervals
  - Undertake a management review of the ISMS on a regular basis (at least once per year)
  - Record actions and events that could have an impact on the effectiveness or performance of the ISMS.

ISO/IEC 27001- Act phase

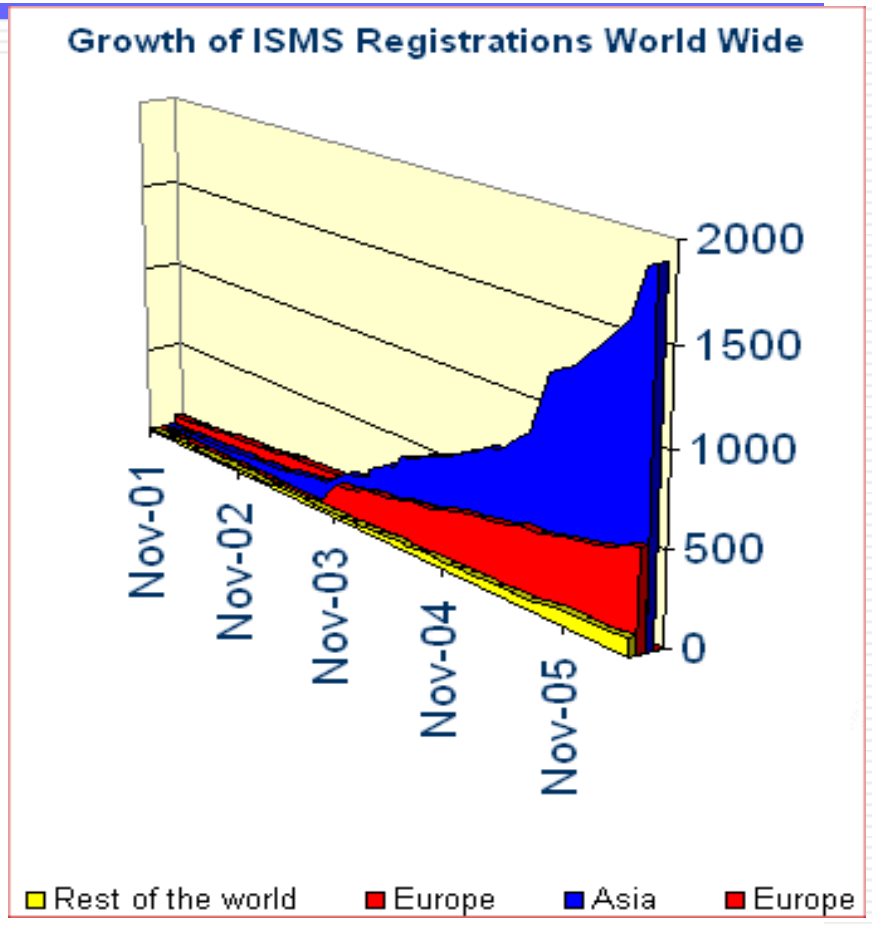
- Maintain and improve the ISMS
- Purpose: Take action as a result of the Check phase
- Steps:
  - Implement identified improvements in the ISMS
  - Take appropriate corrective and preventive actions
  - Communicate the results and actions and agree with all interested parties
  - Ensure that the improvements achieve their intended objective

ISO/IEC 27001Output



ISO/IEC 27001Certification

- Certification according to ISO27001 is conducted by DNV (Veritas) in Norway
- http://www.dnv.no/



Source: Gamma Security Consulting, UK

Secure Systems Development

Secure Systems Development

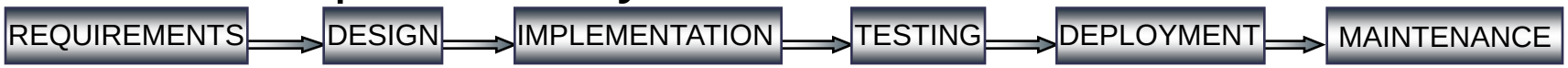
- Software Engineering: Concept of creating and maintaining software applications by applying technologies and practices from computer science and project management fields

  [www.wikipedia.org]

- Secure Software Engineering

“Current”/Traditional Software Engineering

- Over 30 years of software development experience created a well defined application software development lifecycle



- There are many software development methodologies (ex. XP, waterfall, etc) they all have these basic steps
- Capability Maturity Model for Software (SW-CMM), is used to measure quality of methodologies employed

Motivation

- This application development process in its essence fails to address security issues
- Consequently, security flaws are identified only at the later stages of the application lifecycle. And thus
  - Much greater cost to fix
  - High maintenance cost
  - …
- Nearly every company/organization utilizes network security infrastructure (e.g. Firewalls, IDS, etc)
- But very small number of them invest in application security strategy, design, and code review services

So

- For the software industry, the key to meeting demand for improved security, is to implement repeatable processes that reliably deliver measurably improved security
- Thus, there must be a transition to a more stringent software development process that greatly focuses on security
- Goal: minimize the number of security vulnerabilities in design, implementation, and documentation
  - Identify and remove vulnerabilities in the development lifecycle ***as early as possible!!!***

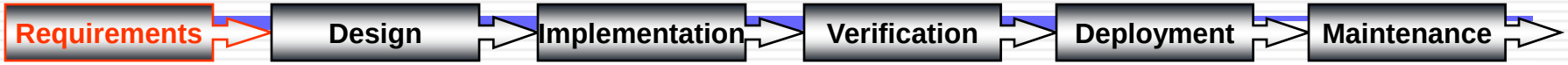
Building Secure Software

Three essential components

- Repeatable process
- Engineer Education
- Metrics and Accountability

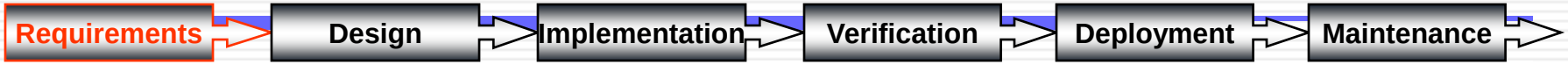
- SDL – Secure Development Lifecycle
  - Used along with traditional/current software development lifecycle/techniques in order to introduce security at every stage of software development

SDL – Requirements Phase



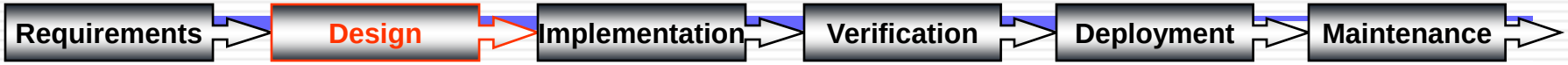
- Development of requirements
  - Gather information about application
- Analysis of requirements
  - Are all the security issues addressed
- Verification of requirements
  - Are there are any inconsistencies / system interface / correctness
  - Documentation!!!
- Feasibility of requirements
- The bottom line: Planning at this stage offers the best opportunity to build secure software in the most efficient manner [cost, time, etc]

SDL – Requirements Phase



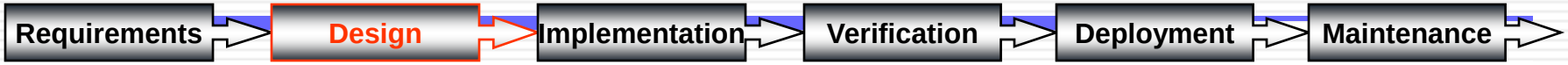
- Develop Security Requirements
  - Security Requirements of a system/application must be developed along with any other requirements requirements (e.g. functional, legal, user, etc)
- Risk analysis
  - Identify all the assets at risk
  - Identify all the threats
- Develop security policies
  - Used as guidelines for requirements
- Develop security metrics

SDL – Design Phase



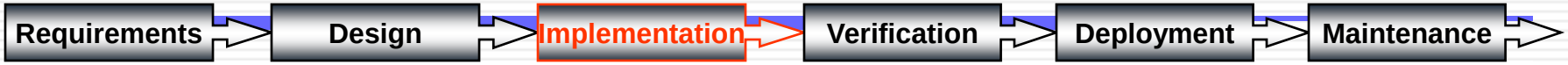
- At this stage all design decisions are made, about
  - Software Architecture
  - Software components
  - Programming languages
  - Interfaces
  - …
- Develop documentation
- Confirm that all requirements are followed and met

SDL – Design Phase



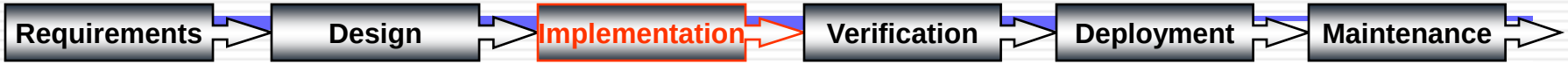
- Treat Models
- Input Data Types
- Security Use Cases
- Security Architecture
- Defense in Layers / Separate Components / Least Privilege
- Tool
  - SecureUML – Secure Unified Modeling Language

SDL – Implementation Phase



- This is the stage where coding is done.
- To produce secure software
  - Coding Standards
  - Centralized Security Modules
  - Secure builds and configurations
    - Known security vulnerabilities - use good programming practices. Be aware of
      - Race conditions
      - Buffer overflow
      - Format string
      - Malicious logic
- Follow Design & Develop Documentation [further]

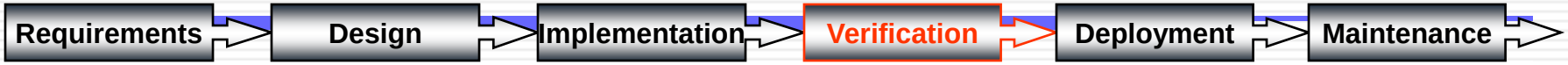
SDL – Implementation Phase



Design and implementation of security features.
From the Requirements

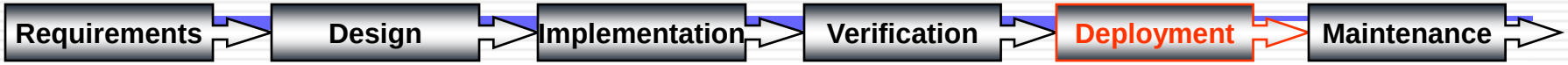
Robust Programming Practices
Good design and coding practices

SDL – Verification Phase



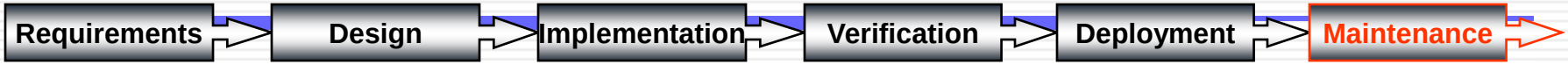
- Testing of the code developed in the previous stage
- Cleared security tests
- Security vulnerability tracking
- Code Reviews
- Documentation

SDL – Release Phase



- Secure Management Procedures
- Monitoring Requirements
- Security Upgrade Procedures

SDL – Response Phase



- Causes:
  - Costumer feedback
  - Security incident details and vulnerability reports
  - …
- Types of maintenance
  - Need to introduce new functionality
  - Need to upgrade to keep up with technology
  - Discovered vulnerability

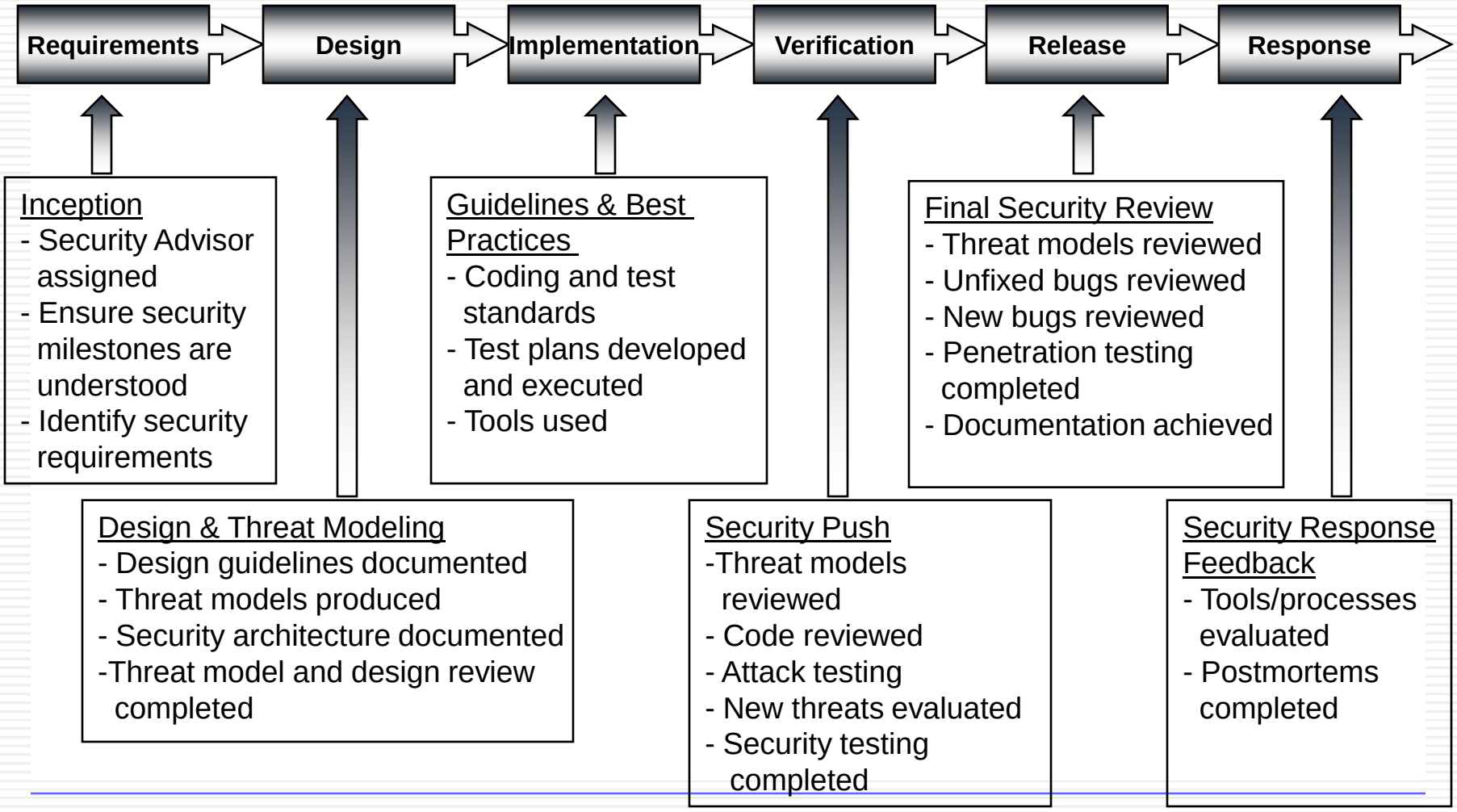
Facts:

- Every security vulnerability / flaw overlooked in an earlier phase will end-up at later phase[s]

- Resulting into greater
  - Cost
  - Time

  of the software development and/or maintenance

SDL @ Microsoft



Mobile Malicious Code

- Malicious code:
  - Code is that which is intentionally included in hardware, software, firmware or data for unauthorized purposes. Computer Viruses, Worms, Trojan Horses, Trapdoors, and Logic/Time Bombs all fall under the definition of malicious code.
- Mobile code:
  - Technology which allows for the creation of executable information which can be delivered to an information system and then directly executed on any hardware/software architecture which has an appropriate host execution environment.

Mobile Malicious Code [cont'd]

- Malicious Mobile Code:
  - Mobile code is the software designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources.

- Types of mobile code are direct and indirect:
  - Direct mobile code can be recognized within the primary transport mechanism, such as a virus within a file.
  - Indirect mobile code may be embedded, such as inside of an attachment to an E-Mail.

Mobile Code Technologies

- Category 1
  - Mobile code that can exhibit broad functionality using unmediated access to services and resources of workstations, hosts and remote systems. [e.g. Active X, VBA, Unix shell script]
- Category 2
  - Mobile code that has full functionality using mediated or controlled access to services and resources of workstations, hosts and remote systems. [e.g. Java Applets, Postscript]
- Category 3
  - Mobile code that has limited functionality, with no capability for unmediated or uncontrolled access to services and resources of workstations, hosts and remote systems. [e.g. JavaScript, VB script]
- Exempt technologies are those which are not considered true mobile code
  - [e.g. XML, Web server scripts]

Mobile Code Techniques

- Trusted Source (Signed Code)
  - A trusted source is a source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication.

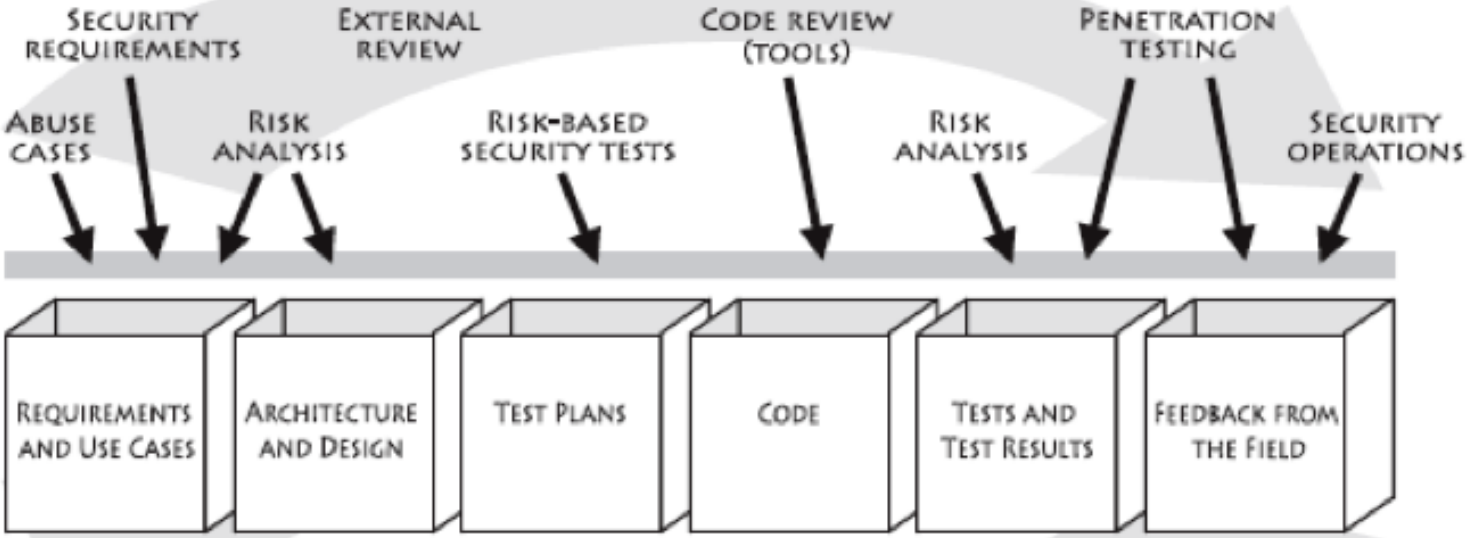
- Screening (Sandbox)
  - Preventive measure to monitor processes and data to intercept malicious code before it is introduced to an IS. Screening also includes monitoring IS for the presence of malicious code which is already present. Malicious code occurs in different forms, which may have different methods for screening.

CLASP

- Comprehensive, Lightweight Application Security Process
  - Centered around 7 AppSec Best Practices
  - Cover the entire software lifecycle (not just development)
- Adaptable to any development process
  - Defines roles across the SDLC
  - 24 role-based process components
  - Start small and dial-in to your needs

Touchpoints

- Gary McGraw's and Cigital's model



The OpenSAMM Project

- Software Assurance Maturity Model
- http://www.opensamm.org
- Dedicated to defining, improving, and testing the SAMM framework
- Always vendor-neutral, but lots of industry participation
  - Open and community driven
- Targeting new releases every 6-12 months
- Change management process
  - SAMM Enhancement Proposals (SEP)

End of lecture

- We have looked at:
  - ISO/IEC 27002
  - ISO/IEC/27001
  - SDL (Secure Development Lifecycle)
  - Other security development framerworks