

Security Engineering Fall 2015

Lecture 03 – GRC
Fabio Massacci

Fundamental IT Security Questions

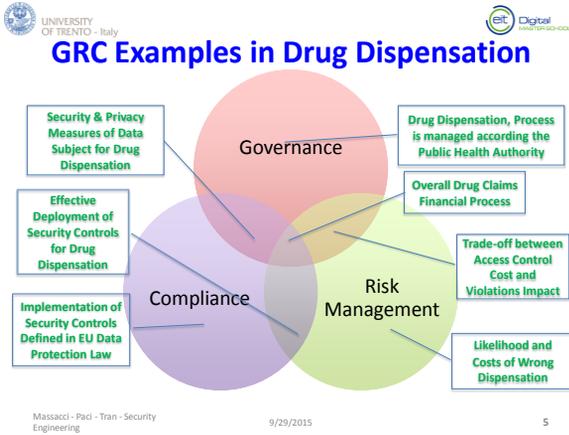
- **Which assets do we need to protect?**
- **How do we decide what to do?**
- **What can we do to counter those threats?**
- **That's a question for Governance, Risk and Compliance.**
 - It applies to all aspects of a company → for our perspective it is IT Security Management

What is GRC?

- **Governance**
 - policies, laws, culture and institutions that define how an organization is managed/run and drives the strategy
- **Risk Management**
 - the coordinated activities that direct and control an organization's risks.
- **Compliance**
 - the act of adhering to regulations as well as corporate policies and procedures

GRC Example

- **Hospital San Raffaele of Milano (Italy)**
 - Largest private medical research hospital in Italy
- **Private Hospitals Manage Drug Dispensation to Patients on behalf of Health Care Authority and Claim Reimbursement Afterward**
 - Some drugs are very expensive: huge financial issues
 - Process is highly regulated
 - Many steps are run by external actors
- **Many privacy and security issues**
 - Protect patient identity
 - Authenticate patients, doctors and nurses
- **Target is to "govern" the process, manage the risks and show compliance with law and show "we are in control"**



Why GRC is Important?

- **Huge Markets**
 - Investors in North America and Western Europe will pay a premium of 14% for companies with good governance [McKinsey report]
 - GRC market in 2008 at approximately \$52.1 billion (and growing). Of this 4% in IT [Corporate Integrity report]
- **Companies Adopt GRC to**
 - Comply with regulations
 - Avoid failing an audit
 - Learn from a bad experience
 - Managing risks
 - Insure, improve and optimize an existing business
- **We focus on the "Security Management" Part**

Massacci - Paci - Security Engineering 9/29/2015 6

What is Security Management?

- **It is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity inside an organization**

Massacci - Paci - Security Engineering 9/29/2015 7

Overview of Sec Management Process

- **IT security management process involves:**
 - determining organizational IT security objectives, strategies and policies
 - identifying and analyzing security threats to IT assets
 - identifying and analyzing risks
 - specifying appropriate safeguards
 - monitoring the implementation and operation of safeguards
 - developing and implement a security awareness program
 - detecting and reacting to incidents
- **How do you do that?**

Massacci - Paci - Security Engineering 9/29/2015 8

Standard Nightmare...

- **Many Regulation to Show Compliance with**
 - Financial Areas (Sarbanes Oxley Act, German Corporate Governance Code, Basel II, Solvency II)
 - Privacy-related (EU Data Protection Directives, HIPAA)
 - Environmental (Title 50 (wildlife) and Title 33 (navigable water))
 - Security related (Toxic Substance Control Act, ITAR, Patriot Act)
- **Many Standards to Show Compliance with**
 - COSO (Enterprise Risk Management – Integrated Framework, 2009 : Guidance on Monitoring Internal Control Systems)
 - ISO (2700X on Information Security, 38500 on IT Corporate Governance, 31000 on Risk Management, 9000 and others on service quality)
 - ISACA (COBIT, ValIT, Risk IT), UK OCG (ITIL v3)
 - PCI-DSS, SAS 70
- **Many different “Philosophies”**

Enterprise Risk Management

- **Developed by PricewaterhouseCoopers and Committee of Sponsoring Organizations of the Treadway Commission (COSO)**
- **Process that:**
 - is effected by every people at every layer of the enterprise
 - is applied in strategy setting and across the enterprise
 - is designed to identify potential events that may affect the enterprise
 - manages the risk to be within the enterprise risk appetite
 - provides reasonable assurance regarding the achievement of the enterprise objectives

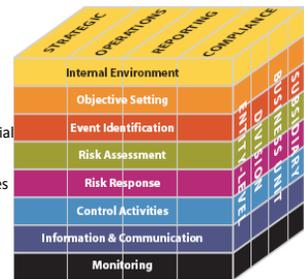
Enterprise Risk Management - II



- **Objective Category**
 - Strategic
 - high-level goals, aligned with and supporting the entity's mission
 - Operations
 - effective and efficient use of the entity's resources
 - Reporting
 - reliability of the entity's reporting
 - Compliance
 - entity's compliance with applicable laws and regulations

Enterprise Risk Management - III

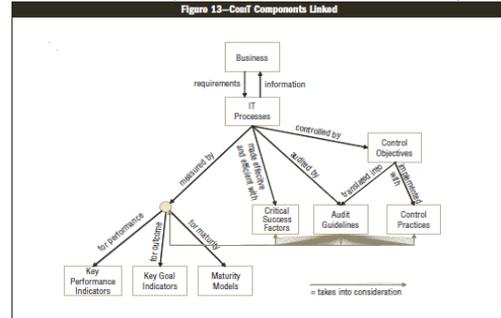
- **ERM Component**
 - Internal Environment
 - Objective Setting
 - Event Identification
 - Risk Assessment
 - Risk Response
 - Cost /benefit of potential risk responses;
 - Possible opportunities lost, once risk responses are applied.
 - Control Activities
 - Information and Communication
 - Monitoring



COBIT

- **COBIT = Control Objectives for Information and related Technology**
 - The ISO27002 proposed by the Auditor’s Association
 - Organized Along Phases of IT Management
- **For each phase identify processes and controls**
 - Plan and organise (11)
 - Acquire and implement (6)
 - Deliver and support (13)
 - Monitor and evaluate (4)
- **Identify also KGIs and KPIs**

COBIT (from Student's Book)



COBIT

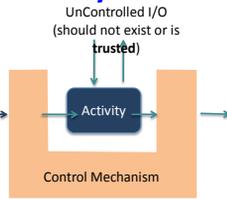
- **Information Criteria Considered x Process**
 - Effectiveness
 - Efficiency
 - Confidentiality
 - Integrity
 - Availability
 - Reliability
- **Level of Importance x Process**
 - Primary or Secondary

COBIT

- **Control Objective**
 - statement to protect the quality-attribute of business (i.e., because of risks or required by regulatory requirements)
 - Hide personal information from the reimbursement report
- **Control Process**
 - a process to achieve the control objective
 - Remove personal data (Name, Tax Code) from the reimbursement report
- **Control Activity**
 - a means/action to achieve a control objective (the one that can really be implemented and measured)
- **Key Goal and Performance Indicators**
 - Measure how good we are in achieving our objectives (KGI) and in implementing our processes (KPI)
 - Number of reports without personal data

How to Control an Activity?

- **Plain (= no control)**
 - part of the trusted organizational base
- **Controlled Activity**
 - Wrap “something” around activity (BP fragment) implementing the business objectives to control major risks
- **Organizational Controls**
 - Personell policies
 - Incentives and procedures
- **Technical Controls**
 - Design time verification + deploy-time certification
 - Run-time Monitoring and Enforcement
- **Measure Controls (KGIs & KPIs)**



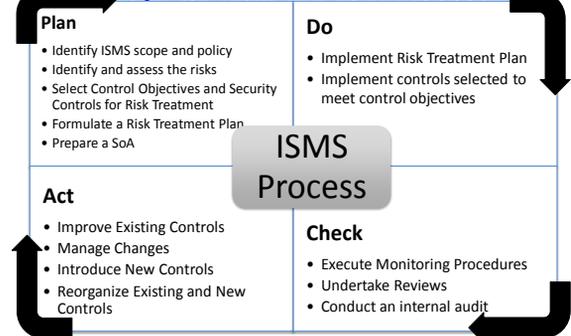
How to Identify Control Objectives?

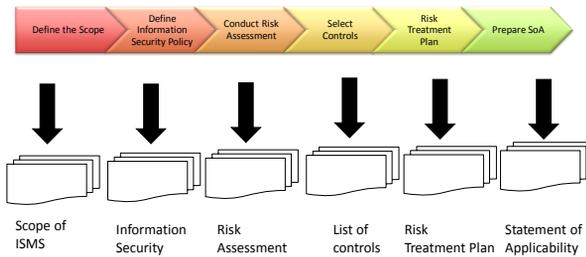
- **Start from Business Objectives and Compliance Requirements**
 - Analyze Risks that might lead to failures
 - Identify Countermeasures (Control Objectives)
 - Refine process on control objectives themselves
- **Refine**
 - Complete → protect from most critical risks
 - Appropriate → their achievement allows the organization to meet its business goal and to mitigate the risks
 - Measurable → enabling unambiguous interpretation of the level of compliance or failure with regards to the control objective

The ISO/IEC 2700x Family of Standards

- **ISO/IEC 27001**
 - Describes the process to establish, implement, operate, monitor and maintain a security management process
- **ISO/IEC 27002**
 - Provides a list of security control objectives and best practice security controls
- **ISO/IEC 27003**
 - Provides guidance to implement the family of standards 2700x
- **ISO/IEC 27004**
 - Provides guidance to help organization measuring effectiveness of security management systems
- **ISO/IEC 27005**
 - Security risk management

ISO/IEC 27001: PDCA Process





- **Define the Scope**
 - Identify lists of areas, locations, assets, and technologies
- **Identify any regulatory or legislative standards that apply to the area under control of ISMS process**
 - Industry Standards
 - State, Local, Federal Governmental, or International regulatory bodies

Scope and Purpose

The company is committed to protecting its information and that of its customers.

To achieve this goal, the company has implemented an Information Security Management System in accordance with ISO/IEC 27001:2005 and the rules and regulations that are part of OSHA Public Law 91-596 84 STAT. 1950.

The company's ISMS is applicable to the following areas of the business:

- Finance department
 - Internal IT systems and networks used for back-end business (such as email, timesheets, contract development and storage, and report writing)
- (Note: IT systems and networks on which company software is developed and stored are part of the Software Development ISMS. Refer to the Software Development Security Manual for more information.)

- **Define the Scope of the Security Policy**
 - Scope of ISMS
 - Importance of Security for the organization
 - Maintaining Information Security and Information Security Systems
 - Information Security Responsibility
 - Security Awareness Training and Education
 - Reporting on Security Incidents
 - Virus Control
 - Organization Information Classification
 - Safeguarding of Organization's Records
 - Data Protection
 - Access Control

- **Risk Assessment**
 - Define the risk assessment approach for the organization
 - Identify assets
 - Identify assets' vulnerabilities
 - Identify potential threats
 - Analyze and evaluate risks
 - Document the risk assessment process

- **Identify appropriate controls to reduce risk**
 - Controls may be controls already deployed in the organization
 - Controls defined in ISO/IEC 27001-27002 standards
 - Controls mandated by legislations or regulations
- **Basic rules for selection**
 - First controls driven by legislation or regulation
 - Controls specific to the organization's business environment
 - Controls from ISO/IEC 27001 and ISO/IEC 27002
- **Run cost-benefit analysis for each selected control**

- **Risk Treatment Plan**
 - Plan on how the organization will address risks to each assets
- **Components**
 - Method selected for treating each risk (accept, transfer, reduce)
 - Which controls are already in place
 - What additional controls are proposed
 - Priority in which to perform the implementation of controls

Asset	Ref. N°	Priority	Treatment	Options	Risk Factor After Treatment	AR	Initial Responsibility	Time table

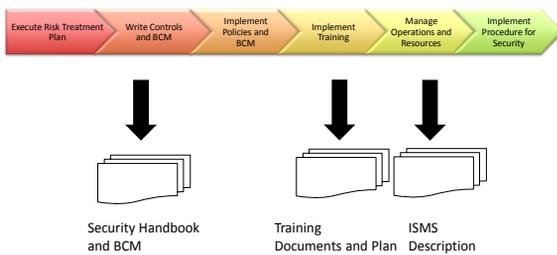
ISO/IEC 27001: Plan Phase

- **Prepare the SoA**
- **For each control listed in the Annex of ISO/IEC 27002 specifies**
 - If the control was adopted
 - Justification for adopting or not adopting the control
 - Reference to the procedure documenting the use of the control

ISO/IEC 27001: Plan Phase – Prepare the SoA

Control	Description	Implement	Justify	Procedure Approach
A.10.7.2	A paper shredder has been added. New process for secure disposal of media has been implemented	Fully		Please refer to the control and policy document

ISO/IEC 27001: The Do Phase



ISO/IEC 27001: The Do Phase

- **Write Policies and Procedures**
- **For each control select a policy and/or procedure that govern the use of the control**
 - E.g use of password for access management
 - Password policy that states what constitutes a strong password
 - Procedure specifies how to initially create and manage strong password

ISO/IEC 27001: The Do Phase

- **Write Policies and Procedures**
 - Why was a control selected?
 - Who is responsible for the control selection, implementation, enforcement?
 - How does one implement the control; enforce the control?
 - What measures and metrics will show the application of the control ?
 - KPI, KGI

ISO/IEC 27001: The Do Phase

- **Metrics and Measurements:**
 - Capture the state of existence and effectiveness of ISMS implementation
 - ISO 27004 provides guidelines to identify metrics and measurements
- **Possible metrics (KPI)**
 - For a firewall, N° of blocked packets with Y identified as potential attacks
 - For anti-virus N° of virus blocked
- **Challenge: transforms these metrics into business value (KGI)**
 - CEO does not care about num of blocked packets

ISO/IEC 27001: The Do Phase

- **Implementing Controls**
- **For each control in SoA investigates the following questions:**
 - Does the organization need this security control at all?
 - What features of this control does the organization need?
 - ISO/IEC 27002 answers these questions
- **Balance security need with available resources (budget)**
 - Best practices vs acceptable practices

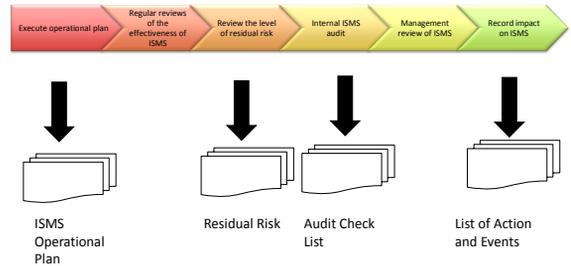
ISO/IEC 27001: The Do Phase

- **Awareness, Training and Education**
 - Provides knowledge about security
 - Security Issues
 - Need for security inside the organization
 - Actions to be taken to contribute to security management
- **Security awareness is**
 - new employees,
 - system administrators,
 - data collection personnel
 - security professionals

ISO/IEC 27001: The Do Phase

- **Managing Operations and Resources**
- **Management of resources to reduce risk**
 - Acquiring Security professionals
 - Managing Security professionals
 - Acquiring Security Tools
 - Managing Security Tools
- **Management of security incidents**
 - Monitoring
 - Detection
 - Notification
 - Response
 - Root Cause Analysis

ISO/IEC 27001: The Check Phase



ISO/IEC 27001: The Act Phase

- **Security is a process, not a destination**



ISO\IEC 27002

- **Code of practice for information security (IS) management**
 - 133 IS control objectives divided over 12 topics
- **Each main security category contains:**
 - control objective stating what is to be achieved;
 - one or more controls that can be applied to achieve the control objective
- **Main Control Objectives**
 - Security Policy
 - Organizing Information Security
 - Asset Management
 - Human Resources Security
 - Physical and Environmental Security
 - Communications and Operations Management
 - Access Control
 - Information Systems Acquisition, Development and Maintenance
 - Information Security Incident Management
 - Business Continuity Management
 - Compliance

Summary

- ***IT Security Management is the process to establish, operate, review, maintain, improve information security inside an organization***
- ***Some standards specify how to do it***
 - ISO/IEC 27001 is the “how”
 - ISO/IEC 27002 is the “what”
- ***Many different variations on how...***
 - COSO, COBIT, SABSA, etc. etc.