University ICT Security Certification

Francesco Ciclosi, University of Camerino

- Is secure an organization complies with the standard ISO/IEC 27001?
  - ❍ TRUE
  - ❍ FALSE
- Is the standard ISO/IEC 27001 a metric of the organization's information security level?
  - ❍ TRUE
  - ❍ FALSE

First answer: FALSE

- Is secure an organization complies with the standard ISO/IEC 27001?

- It's not true that the compliance with the standard ISO/IEC 27001 guarantees the safety of the organization
- Generally the **compliance with the standard doesn't say nothing about** the real **level of information's security**

Second answer: FALSE

- Is the standard ISO/IEC 27001 a metric of the organization's information security level?

- The standard ISO/IEC 27001
  - Is not a metric of the level or quality of security
  - Gives us some guidance about the correct manner to manage the information security process

About the ISO 27001 scope

- The scope:
  - **is to certify** the quality of the information security management process
  - **is not to certify** the quality of the solutions, of the technologies or of the configurations

- This standard follows the same approach used by the ISO 9000 family (industrial processes' quality certification)
  - Where the focus is not on the tool's quality but on the tool's management process quality

The risk treatment

- Is necessary to implement a process of security risk treatment (compliance with the standard ISO 27005:2011):
  - Define all controls needed to implement the right risk treatment
  - Compare the same controls with those defined in the Annex A, in order to verify the presence of the mandatory controls
  - Arrange the Statement of Applicability (SOA)
  - Prepare a risk treatment global plan
  - **Obtain the risk owner's endorsement** about the risk treatment plan and about the residual risk

Reference control objectives and controls

- The ANNEX A is the section of the standard where are defined:
  - the controls
  - the controls objectives
- that represent the requirements to ensure the standard compliance of the ISMS

Annex A	ISO 27001:2005	ISO 27001:2013
Control areas	11	14
Controls objectives	39	35
Controls	133	114

The controls

- Are divided in **thematic sections**
  - (such as: technological aspects, logical or physical security, human resource, business processes, and so on)
- Every sections is also divided in one or more **subsections**
- Every sections is organized as follows:
  - A **general objective** with a short description
  - One or more **pair "control/control objective"**

Definition of the perimeter

- A first study and investigation phase in order to define:
  - the perimeter of the ISMS
  - the field of application (SOA), as well as limits and exclusions
- The outcome enabled us to define the following certification scope: «Supply of connectivity, email, web portal, telephone, hosting and management services to the University and to customers that may request them»

Analysis of the main services provided

- We have developed an asset tree for every Business Service(BS), in order to map out its layout
- The asset tree includes the following information units:

IF (Information)	**SW (Software)**
HW (Hardware)	**COM (Communication devices)**
L (Locations)	**P (People- Human resources)**

Stakeholder identification

- Identification of the various parties that are interested in supplying/using such services
  - students
  - teaching staff
  - technical-administration staff
  - external staff
  - public parties
  - private parties
  - external users

The document infrastructure definition

- Is set up to support the certification process
- Is composed of regulations, roles and rules
- These documents **specify how resources**, including sensitive information, **are to be managed**, **protected** and **distributed** within the University
- The documents were divided into the categories:
  - System Documents;
  - Organizational Procedures;
  - Technical Procedures;
  - Operating Instructions.
- The classification of each documents is made by indicating an identifier chronological number

The correlation matrix

Annex A – Control Objectives and Controls			Current state	Applicable	Notes
A.5 Information security policies					
A.5.1 Management direction for information security *Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*					
A.5.1.1	Policies for information security	Control A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	DS 02 – ISMS Policy	SI	NOT NEW
A.5.1.2	Review of the policies for information security	Control The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Annual Review	SI	NOT NEW

The risk assessment/management strategy

- We have defined a customized strategy for risk analysis and risk assessment
- This strategy was Suitable to the perimeter of our ISMS
- The method adopted was the **Magerit** one, which was implemented through the **PILAR** software tool
- The methodology is compliance with the standard ISO/IEC 27005:2011 «Information security risk management»
- The approach consists of 5 steps

The five steps (1/3)

- **1 - Assets**
  - Definition of the assets that are important for the University, through an analysis of the main one, paying attention to the "dependency between the assets"
  - Division of assets into five levels
  - Enhancement of assets with a qualitative ranking system for a better positioning of each asset's value in relation to the others
- **2 - Threats**
  - **Identification** of all the **threats** that were considered relevant to every asset type
  - **Matching** between **asset groups** and **threat**
  - **Definition** of the **vulnerability level** considering the **frequency** value and the **damage** value

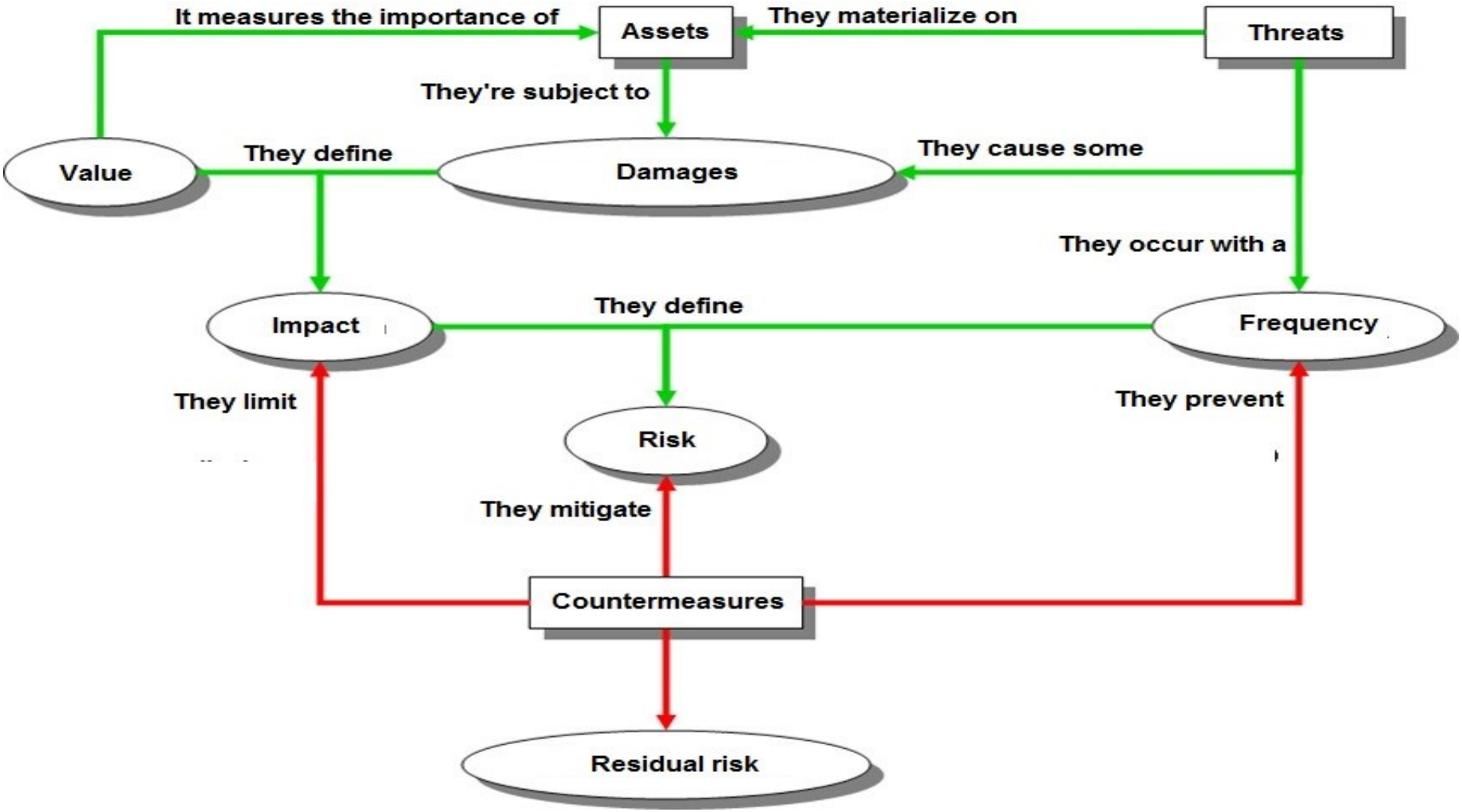
The five steps (2/3)

- **3 - Countermeasures**
  - Calculation of impact and risk that may theoretically concern the assets in the worst possible case (as if none of the countermeasures are activated)
  - The countermeasures may be included in the risk calculation either by:
    - reducing the threat frequency (preventative countermeasures)
    - limiting the damage caused (containing countermeasures)
- **4 - Impact**
  - Calculation of the impact that threats may have on the systems
    - considering the asset value
    - considering the damage level that such threats may cause
  - Two types of calculations were chosen:
    - the cumulative impact
    - the reflected impact

The five steps (3/3)

- **5 - Risk**
  - **Calculation** of the **risk value**
    - considering the impact of threats
    - considering the threats occurrence frequency
  - **Combination** or **grouping** the **single risks** in **different ways** (a given asset is the reference), until a **global value is obtained** and expressed by using a **ranking system**
  - As output of the risk analysis process , the global risk value (related to a single asset) is expressed by using an eight-point ranking system
  - There is **two threshold values** that are defined beforehand:
    - **alert threshold** – no further countermeasures need to be taken below such a value
    - **action threshold** - if such a value is reached, then suitable countermeasures need to be immediately identified to bring the risk value back to acceptable levels
  - **We have decided to accept the consequent residual risk value if it's lower than the action threshold value**

The risk treatment methodology



The improvement actions

- Are recorded in a special register
- Are constantly monitored
- Act as an input for every new risk analysis and management process, that is constantly carried out, at least on an annual basis
- Is possible to indirectly monitor the effectiveness of this actions
- This cyclical improvement process complies with standard ISO/IEC 27005:2011 «Information security risk management»

#	Source	Ref. Doc.	Point ISO27001	Weakness	Action
1	AR	DS-05, § 6.3.1, countermeasures [AUX6]	9.2.3	cabling is not completely protected and identifiable	Configuration errors, interferences and data interception may easily occur if cabling is not checked

Consequences	Priority	Responsibilities	Resources	By	Evidence status on 25 June, 2015	%
Labelling all the cables related to the systems. Separating power cables from data cables. Checking that unauthorized interception of data traffic is impossible by accessing the cabling.	Medium	Mr. Rossi	Internal	31 Dec, 2015	PT-20 – Security and cabling schema.docx - V.0 del 18/11/2013	100

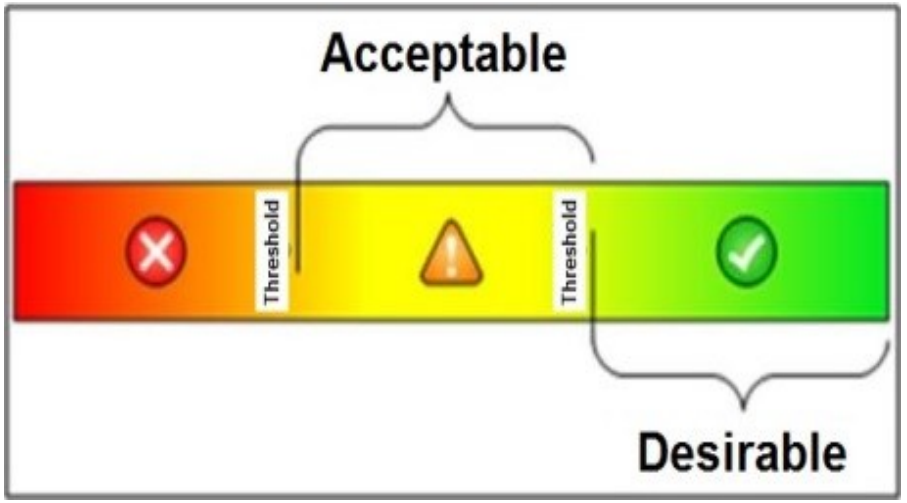
The indicator table

- In the ISMS are defined same indicators
  - finalized at the continuous monitoring of the effectiveness of the activated controls
  - punctually associated with the reference standard
  - gathered through a special table-like form that helps to check the trend of what has been detected

ID	Description	Detection rate	Annex A point	2013	1	2	3	4	5	6	7	8	9	10	11	12	2014	Desirable	Acceptable
I27	Password quality	6m	A.11.3.1	3			4			4			5			5	5	2	4

The indicator thresholds

- **Acceptability**
  - defines whether a given value may or may not be considered risky
  - may trigger improvement actions
- **Desirability**
  - defines whether a given value may or may not be considered acceptable
  - may activates alert messages to the system administrators



The system continuous improvement

- The system continuous improvement is guaranteed by the accomplishment of periodical:
  - **internal audits** (scheduled over three years)
  - **annual review** of the whole ISMS (carried out by the Direction of CINFO)
  - **external audits** (carried out by the thirty party certification authority RINA S.p.A.)

The internal audit

- During the auditing, all the requirements set forth by ISO regulations are carefully analyzed
- If a non conformity is detected then a corrective action is immediately entered in the Improvement Actions Registry

Point	Requirement	Objective Evidence	Detection
4.2	Understanding the needs and expectations of interested parties	DS13 (Context and scope) DS01 (SGSI Perimeter) DS04 (ISMS Organization)	NO

The annual review

- During the review are gathered all the **incoming** and **outgoing elements** that may be useful to perform a proper **assessment** of the **ISMS**, in order to ensure on an ongoing basis
  - effectiveness
  - adequateness
  - suitability
- At the same time are also evaluated any improvement opportunities and any amendment needs

Transition toward the new ISO 27001:2013

- The last year we have completed the transition process concerning the new ISO 27001:2013
- This task have required some changes (not particularly expensive ones) within the ISMS, in order to adjust
  - the regulatory references
  - the structure of some documents
- to the new requirements set forth by the ISO standard.

- As Example: we have done a system documents review in order to substitute the Deming Cycle (Plan-Do-Check-Act) with the new but equivalent “Framework for managing risk” (Design-Implementing-Monitoring/review-Continual improvement) introduced by the standard ISO/IEC 31000:2009

Results obtained

- In order to comply with the requirements specified, CINFO has got a new tool dedicated to the management of security incidents
- The implementation of this system has been fundamental and throughout the years has allowed the CINFO to collect a large amount of data, used as an input for
  - the indicators table
  - the corrective actions definition
  - the internal audits
  - the annual review
- From the analysis of data collected it has been possible to identify the cause of some anomalies and then to proceed to their resolution

The reduction of the data center services downtime

- The data recorded in CIM during the year 2013 saw a significant downtime
- time in some services housed at the university data center
- The analysis of these data allowed us to identify the cause of the problem, due to
  - the presence of two particularly obsolete SAN
  - the inadequate air-conditioning system
- The corrective actions implemented allowed us to solve this anomalies

The backup jobs management

- From the analysis of the types of incidents recorded in CIM, it has been possible to identify the inadequacy of backup procedures using obsolete hardware and heterogeneous software platforms
- The following corrective actions have been implemented:
  - logical and operational organization of the first and second level backup systems
  - consolidation and/or replacement of hardware equipment
  - update of the technical procedure called “backup”, by better specifying
    - the information to be saved
    - the media handling
    - the backup job instances recording management
- The corrective actions implemented allowed us to solve this anomalies

My contacts

linkedin
http://it.linkedin.com/pub/francesco-ciclosi/62/680/a06/

facebook
https://www.facebook.com/francesco.ciclosi

twitter
@francyciclosi

www
http://www.francescociclosi.it