UNIVERSITY ICT SECURITY CERTIFICATION

Ciclosi F.[1], Mauri M. [1], Polzonetti A[2], ...

[1]Computer Center University of Camerino
[2]ELIOS srl. Spin Off University of Camerinos

Keywords
Security, Certification, ISO 27001, ISMS

1. ABSTRACT

Information security management is a key aspect in the good governance of ICT. Due to the evolution and widespread about the Internet, organizations are easier to attack on the information technology systems. Given the above background, the University's IT Services and Systems Centre (CINFO) decided to respond to external requests by trying to manage the change in such a manner that would imply giving up an old approach, based just on technology update, and directly aiming at managing the procedures concerning security issues. In this paper we discute the certificate process at Camerino University and the results obtained.

2. INTRODUCTION

In the last few years, the University of Camerino has been tackling a number of challenges concerning ICT security, both in order to comply with the increasingly stringent regulations for Italian Pas [1], as well as to respond to sudden changes (not just the technological ones) that have been affecting service infrastructures during the current transition from a client-server paradigm to a new functional one. Being based on a cloud system and on software defined networking, the new paradigm is providing the basis for a global interconnection model involving heterogeneous and 'smart' devices that are typical of the so-called 'Internet of Things' [2].

Given the above background, the University's IT Services and Systems Centre (CINFO) decided to respond to external requests by trying to manage the change in such a manner that would imply giving up an old approach, based just on technology update, and directly aiming at managing the procedures concerning security issues.

Within such a scenario, starting from 2012, an in-depth work has been done to gradually redefine all the IT processes, so that they could be provided under stable operating conditions, in compliance with rules and arrangements (not just technical ones), so that confidentiality, integrity and availability requirements could be guaranteed, even though in a general although quantifiable manner .

The final decision to start a virtuous route that, by using the ISO 27001 certification as operating gearing, could lead to a redefinition of internal organizational processes, was made in response to the issues originating from the 'Studio di Fattibilità Tecnica' (Technical Feasibility Study) [3], as per Art. 50-bis ('Continuità Operativa' (Operational Continuity)) of the 'Codice dell'Amministrazione Digitale' (Digital Administration Code) (Legislative Decree No. 82/2005, and as amended through Legislative Decree No. 235/2010) [4].

3. THE CERTIFICATION PROCESS

The certification process included the following macro activities, which were not necessarily performed individually and consequentially:

- Definition of ISMS (Information Security Management System) perimeter
- Establishment of a shared ISMS policy
- Applicability statement (Annex A)
- Redefinition of the organizational structure

- Implementation of a risk analysis method
- Implementation of a risk management strategy developed through improvement actions
- Definition of control effectiveness indicators
- Definition of an audit and review plan

In particular, the process started with a study and investigation phase in order to define the perimeter of the ISMS pertaining to CINFO, including the field of application, as well as limits and exclusions [5]. The outcome of this study phase enabled us to define the certification scope in the following object statement: 'Supply of connectivity, email, web portal, telephone, hosting and management services to the University and to customers that may request them.'

Therefore, an in-depth analysis of the main services supplied by the University on behalf of CINFO was carried out, especially focusing on their organization, infrastructures, data, devices, networks and support technology.

In particular, an asset tree was developed for every service (BS - Business Service), 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)

Likewise, the various parties that are interested in supplying/using such services were also identified and divided into the following groups: students, teaching staff, technical-administration staff, external staff, public parties, private parties and external users. Then a set of guidelines was also developed to specify the structure's features and the requirements set forth by the University's policies concerning IT security. Such guidelines were conceived by keeping in mind that they could also be applied, at a later stage, to methods and tools used for information management. The work devoted to this phase facilitated the rise of a new kind of awareness as regards the meaning of information security, where information started being considered as an essential resource that is needed to carry out the University's business activities. Hence, given its value, it deserves to be properly regulated and protected.

The document infrastructure set up to support the certification process is composed of regulations, roles and rules that specify how resources, including sensitive information, are to be managed, protected and distributed within the University. In particular, each document tackles a single security topic by describing it from any possible points of view and according to any interests it may have for different users [6]. The documents were divided into the following categories:

- DS – System Documents;
- PO – Organizational Procedures;
- PT – Technical Procedures;
- IO – Operating Instructions.

The classification of every single document is made by indicating a chronological number that univocally identifies it within the corresponding category. Moreover, for the benefit of human users, a title explaining the document's contents is also provided. Therefore, the whole documentation was made available to all the interested parties that were authorized beforehand, through publication on a special web portal with limited and controlled access.

The following step saw the development of a matrix that helps to establish a correlation between the control objectives and the controls specified in the Annex A enclosed to the ISO 27001:2005 standard [7], and its applicability to the perimeter of the above-mentioned system (see Figure 1). Within such a context, the current state of implementation by CINFO of the indications set forth for the various controls was also identified and detailed.

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

Figure 1 - Example of how the Control Objectives and Controls matrix (see Annex A) should be completed.

This work tool, that features a peculiar, intrinsic dynamism, was and still is regularly updated so that it may reflect at all times any ISO developments (e.g. the transition from the 27001:2005 version to the new 27001:2013 one [8]), as well as any changes that may occur within the University's ISMS.

The management of the security 'process' also required a redefinition of CINFO's organizational structure. This lead to the development of three functional areas (Systems, Networks, Applications) reporting to the Technical Management and supported by two staff (Secretarial Services and Help Desk). Detailed specifications concerning roles, connections, hierarchical reporting, duties and responsibilities were defined for each functional area.

Then, a customized strategy for risk analysis and an assessment was also defined and implemented. Although it was developed starting from concepts discussed in literature [9], nevertheless the strategy in question was adapted to the peculiar ISMS perimeter being used.

In particular, the method adopted was the Magerit one [10], which was implemented through the PILAR software tool [11]. Such an approach includes five, well defined steps, which are summed up here following and that are repeatable when risk management operations are carried out.

- Step 1 – Assets
- Step 2 – Threats
- Step 3 – Countermeasures
- Step 4 – Impact
- Step 5 - Risk

When tackling Step 1, the assets that are important for the University are defined through an analysis of the main ones [12] – i.e. those that are made of data and processes that transform them into information. That's why the concept of 'assets interdependence' (i.e. the measure in which an asset from a higher level is affected by a security accident involving a lower level asset) is quite important. So, assets were divided into five levels in order to formalize their dependence and make the calculation of cumulative or consequent risk easier. As regards asset value, a qualitative ranking system was opted for (with a 0-10 range), to allow for a quicker positioning of each asset's value in relation to the others, even when the final risk outcome is not expressed in financial terms, but according to a conventional order of magnitude.

When dealing with Step 2, first of all, all the threats that were considered relevant to every asset type were identified. Then the asset groups and the relevant threats were matched together. That

was done because not all the threats affect all the assets. Moreover, even when an asset is affected by a threat, it may not be concerned by all the threat's dimensions and in the same way. Finally, once it was defined which threat may damage a given asset, the latter's vulnerability level was established by considering the frequency value (how many times a year the threat occurs) and damage value (average value, as a percentage, of the damage suffered when the threat occurs).

During Step 3, the impact and risk that may theoretically concern the assets were calculated, as a cautionary measure, in the worst possible case, i.e. as if there was no protection in place. Therefore, such an approach would show what may happen if none of the countermeasures were activated. Generally, the countermeasures may be included in the risk calculation either by reducing the threat frequency (preventative countermeasures), or by limiting the damage caused (containing countermeasures).

When working on Step 4, the impact that threats may have on the systems was calculated by considering both the asset value and the damage level that, in theory, such threats may cause. During the process, special attention was devoted to the dependence relation between the various assets, keeping in mind that whereas the IT system value is based on the services offered and on the data processed, however, threats do tend to affect the means used. Two types of calculations were chosen: the cumulative impact and the reflected impact ones.

During Step 5, the last one, the actual calculation of the risk value was carried out [13] [14], by considering the impact of threats and their occurrence frequency. Using a given asset as reference, the single risks were combined or grouped in different ways, as it had already been done for the impacts, until a global value was obtained and expressed by using a ranking system.

The single risks, related to a given asset, may realistically combine or group in different ways, just as it may happen with impacts, as described in Step 4.

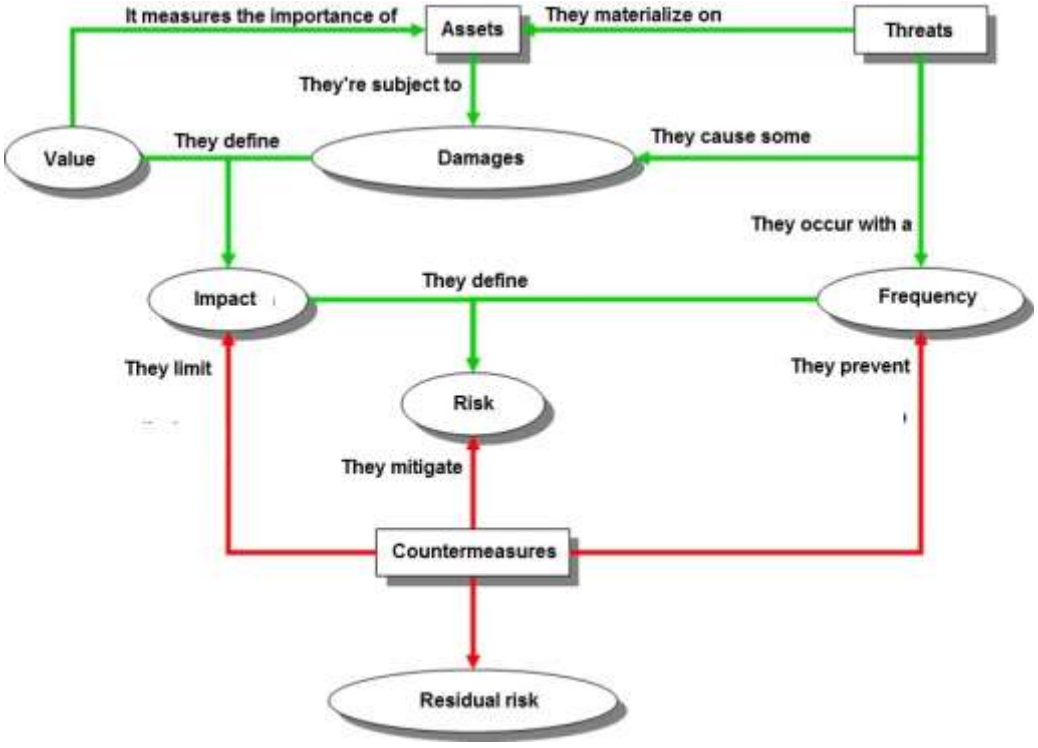

Figure 2 - The steps of the risk analysis and management method adopted.

At the end of the risk analysis, the global risk value related to a single asset is, therefore, expressed according to its level of criticality by using an eight-point ranking system:

- {0} := Negligible
- {1} := Low
- {2} := Medium-low
- {3} := Medium
- {4} := Medium-high
- {5} := High
- {6} := Critical
- {7} := Very critical

where two threshold values were defined beforehand, that are:

- 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.

Within such a perspective, it was decided to accept the consequent residual risk value if the latter is lower than the action threshold value.

Once the identification phase concerning existing risks was concluded, such risks were tackled through a method based on the improvement actions to be taken, in order to reduce their associated value. (see Figure 3). By considering a continuous improvement process based on the Deming Cycle, the implementation status of the proposed actions recorded in the Improvement Action Registry is constantly monitored and works as an input for every new risk analysis and management process that is constantly carried out, at least on an annual basis. Within such a perspective, the evidence detected also provides an opportunity to indirectly monitor the effectiveness of actions that were undertaken.

#	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

Figure 3 - Example of how a record should be set up in the Improvement Action Registry

Within the ISMS adopted by CINFO some special indicators were defined in order to continuously monitor the effectiveness of activated controls, and were also properly associated to the related regulations [15]. A special card was created for every indicator, along the lines of ISO/IEC 27004:2009 [16], where the most important features of the indicator in question are summed up.

Such indicators and the ISMS get continuously into contact through the implementation of decision criteria. In particular, the acceptability thresholds define whether a given value may or may not be considered risky, and potential improvement actions may be triggered. On the other hand, the desirability thresholds define whether a given value may or may not be considered acceptable and, in the latter case, an alert message to the system administrators may be activated.

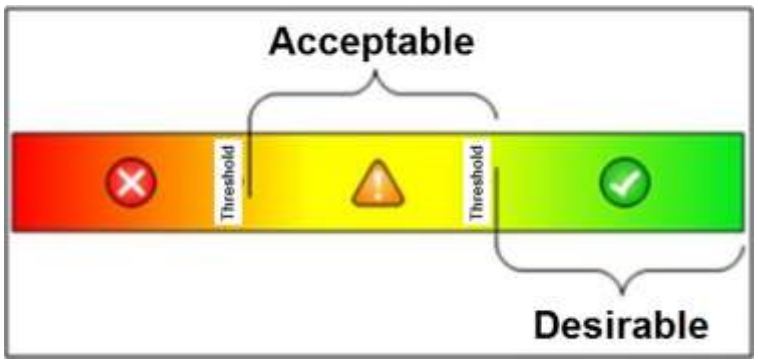

Figure 4 - Diagram of a decision criterion

The values resulting from the effectiveness measurements, or the values associated to all the indicators that were defined based on the frequency identified for their detection, are gathered through a special table-like form that helps to check the trend of what has been detected, compared to previous years and to the minimum (acceptable) or recommended threshold values (desirable).

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**

Figure 5 - Example of how a record should be completed in the Table for Effectiveness Indicators of Activated Controls

The system continuous improvement is guaranteed by setting up a 3-year program for internal auditing [17]. During the auditing, all the requirements set forth by ISO regulations are carefully analyzed. If anything unacceptable is detected, the implemented procedure specifies that a corrective action is to be 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

Figure 6 - Example of how a record should be entered in the Internal Audit Report

In addition to the internal auditing, an annual review of the whole ISMS should also be carried out. During the review, all the incoming and outgoing elements that may be useful to perform a proper assessment of the system are gathered, in order to ensure that the system is effective, adequate and suitable on an ongoing basis. At the same time, any improvement opportunities and amendment needs are also evaluated, including what needs to be done for the information security policy and its objectives.

4. TRANSITION TOWARD THE NEW ISO 27001:2013

The transition and adjustment process concerning the new ISO 27001:2013 [18], which has already been carried out last year, required that some changes (not particularly expensive ones) had to be made within the ISMS, in order to adjust both the regulatory references and the structure of some documents to the new requirements set forth by the ISO standard.

For example we have revisioned our system documents 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.

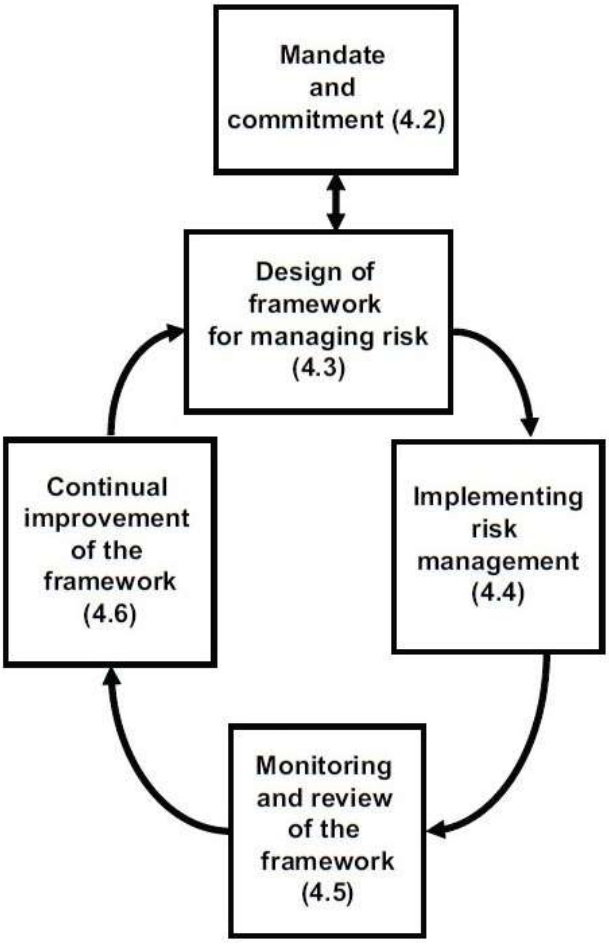

Figure 7 – The Framework for managing risk by the ISO/IEC 31000:2009 Clause 4

From an organizational point of view, no special arrangements were required, since over the years the system has been organized in such a manner that would facilitate a linear transition toward a new version of such a standard.

5. RESULTS OBTAINED

In order to comply with the requirements specified in the ISO 27001 standard, in the year 2013, CINFO has got a new tool dedicated to the management of security incidents called CIM (CINFO incident management). It is a web application used by all employees for the registration and management of events or security incidents.

The implementation of the CIM 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, for the corrective actions definition, as well as for the internal audits and the annual review.

As an example of the results of this virtuous cycle we'll illustrate how from the analysis of data collected in the CIM it has been possible to identify the cause of some anomalies and then to proceed to their resolution. We will present two examples: the first relating to the reduction of the data center services downtime and the second relating to the backup jobs management.

5.1. Reducing the services downtime in the data center

About the first aspect, 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 and to the inadequate air-conditioning system (this situation became especially critical during the summer, when outdoor temperatures were higher). In the first quarter of 2014, we renewed the data center's air conditioning infrastructure and then we proceeded to the obsolete SAN replacement.

The outcome of these actions has guaranteed an immediate decrease in the downtime of services in the data center from 2.1% in 2013 to 0.08% in 2014. After that it has constantly maintained its level below the threshold level (set at 1%) in the following years too. In fact, the 2015 total value was 0.58% and the one detected in the first quarter of 2016 was 0.02%.

Table 1 - Comparison of different downtime data center services rate in the period 2013-2016 (first quarter)

Year	ID	Description	Detection rate	Annex A point	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total	Desirable	Acceptable
2012	I31	Uptime datacenter services (%)	1m	A.14	0,0%	0,3%	0,2%	0,0%	0,5%	0,0%	1,0%	0,3%	0,5%	0,2%	0,7%	0,2%	0,3%	1%	3%
2013	I31	Uptime datacenter services (%)	1m	A.14	0,0%	0,0%	0,5%	0,6%	0,8%	0,0%	10,3%	0,7%	0,7%	10,8%	0,7%	0,0%	2,1%	1%	3%
2014	I31	Uptime datacenter services (%)	1m	A.14	0,1%	0,1%	0,0%	0,0%	0,0%	0,00%	0,52%	0,00%	0,00%	0,00%	0,00%	0,26%	0,08%	1%	3%
2015	I31	Uptime datacenter services (%)	1m	A.14	0,00%	0,30%	0,07%	0,14%	2,89%	0,07%	0,13%	0,40%	0,14%	0,00%	2,78%	0,00%	0,58%	1%	3%
2016	I31	Uptime datacenter services (%)	1m	A.14	0,00%	0,00%	0,07%										0,02%	1%	3%

5.2. Backup management improvement

About the second point 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. In order to solve this critical situation the following corrective actions have been implemented:

- logical and operational organization of the first and second level backup systems, including the consolidation and/or replacement of hardware equipment;
- the update of the technical procedure called 'backup', by better specifying the information to be saved, the media handling and the backup job instances recording management.

The outcome of these actions has guaranteed an immediate increase in the percentage of the backup successfully managed from 88,13% in the fourth quarter of 2014 to 98.47% in the first quarter of 2015. In general by comparing the data on an annual basis, there was a significant increase, rising from 90.26% in 2014 to 98.38% in 2015. These data are also confirmed by the first detection in 2016 which, in March 31, showed a successful rate in the first quarter, amounting to 96.09%.

Table 2 - Comparison of different backup success rates in the period 2013-2016 (first quarter)

Year	ID	Description	Detection rate	Annex A point	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total	Desirable	Acceptable
2016	I10	% Backup successfully	3m	A.10			96,09%										96,09%	85%	75%
2015	I10	% Backup successfully	3m	A.10			98,47%			97,45%			98,91%			98,70%	98,38%	85%	75%
2014	I10	% Backup successfully	3m	A.10			90,96%			88,42%			93,53%			88,13%	90,26%	85%	75%
2013	I10	% Backup successfully	3m	A.10			98,30%			99,40%			99,46%			99,5%	99,17%	85%	75%

5.3. Final conclusion

To sum up, the choice made to follow the ISO27001 certification route revealed to be far-sighted, since it drove the ISMS toward a method change based on the management of the security 'process'. Therefore, an actual change of route has taken place, one that has led to designing (or redesigning, in many instances) the systems for distributed services provided by the University. Special attention was devoted to security issues considered in a holistic manner and not just from a technology point of view anymore. Therefore, we can definitely state, without a shadow of a doubt, that, apart from the unquestionable prestige and proven quality level of our University, the main benefits obtained through the certification process are to be found in the cultural change that has been introduced, one that represented a real quantum jump and marked a clear cut with the past.

6. REFERENCES

[1] Agenzia per l'Italia Digitale website (2014). *Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale*. Retrieved April 27, 2016, from http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf

[2] Ciclosi, F. (2015). *Implementare il paradigma SDN con OpenFlow Switch Protocol. Guida teorico-pratica di riferimento*. Roma, Italia: published by the author.

[3] Iacono, G., Marzano, F., Medaglia, C. M., (2012). La continuità operativa negli Enti locali. Guida pratica alla gestione del Piano. Dogana, Repubblica di San Marino: Maggioli Editore.

[4] Art. 50-bis D.Lgs. 7 marzo 2005 n. 82.

[5] ISO (2013). *ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls*.

[6] ISO (2016). *ISO/IEC 27000:2016, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*.

[7] ISO/IEC (2005). *ISO/IEC FDIS 27001:2005(E), Information technology - Security techniques - Information security management systems - Requirements*.

[8] Wings2i IT Solutions Pvt. Ltd. Website (2014). *Comparison of Controls between ISO/IEC 27001:2013 & ISO/IEC 27001:2005*. Retrieved April 22, 2016, from http://www.wings2i.com/pdfs/Differences%20between%2027001%202013%20Vs%202005.pdf

[9] Chavas, J. P., (2004). *Risk Analysis in Theory and Practice*. San Diego, USA: Elsevier Academic Press.

[10] PAe portal administracion electronica website (2012). *MAGERIT - version 3.0 (English version) Methodology for Information Systems Risk Analysis and Management. Book I: method*. Retrieved April, 21, 2016 from http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/MAGERIT_v_3_-book_1_method_PDF_NIPO_630-14-162-0/MAGERIT_v_3_%20book_1_method_PDF_NIPO_630-14-162-0.pdf

[11] EAR / PILAR website (2014). *Report Templates*. Retrieved April, 21, 2016 from http://www.pilar-tools.com/doc/v54/ReportTemplates_en_e_2014-01-30.pdf

[12] Freund, J., Jones, J. (2015). *Measuring And Managing Information Risk - A FAIR Approach*. Waltham, USA: Elsevier Inc.

[13] ISO (2009). *ISO/FDIS 31000:2009(E), Risk management - Principles and guidelines.*

[14] International Electrotechnical Commision (2009). *IEC/FDIS 31010:2009(E), Risk management - Risk assessment techniques.*

[15] ISO (2011). *ISO/IEC 27035:2011, Information technology -- Security techniques - Information security incident management.*

[16] ISO (2009). *ISO/IEC 27004:2009, Information technology -- Security techniques -- Information security management - Measurement.*

[17] ISO (2011). *ISO/IEC 27007:2011, Information technology -- Security techniques -- Guidelines for information security management systems auditing.*

[18] ISO (2013). *ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems - Requirements.*

7. AUTHORS' BIOGRAPHIES

Francesco Ciclosi is a twenty years experience analyst and trainer, responsible for designing distributed systems services. He is graduated in computer science and has achieved several professional certifications such as: Cisco CCNA, Microsoft MCSE, MCT, MCSA, MCTS and VMware VCA-DCV. He's the author of many articles about computer security and of the books "Implement the paradigm with SDN protocol OpenFlow switch" and "S.A.T.A. traveling to the System of Access to Administrative Transparency ". He has worked with many government agencies, private companies and universities, in the framework of national projects, such as the Italian electronic identity card project. Currently he's working at Camerino University as Information Security Management System manager and cloud computing, server virtualization and storage platform administrator. He's also working as "Computer Science" contract professor at Macerata University. He has previously worked at "Asur" CEO office, at Nestor, the experimental safety laboratory of Tor Vergata University in Rome and at Siemens Informatica "Security Data Networks". Further information is available at https://www.linkedin.com/in/francesco-ciclosi-a0668062