Appréciation conjointe ISO 27001 et ISO 20000-1

Cesare Gallotti

Paris, 30 Novembre 2010

Agenda

- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

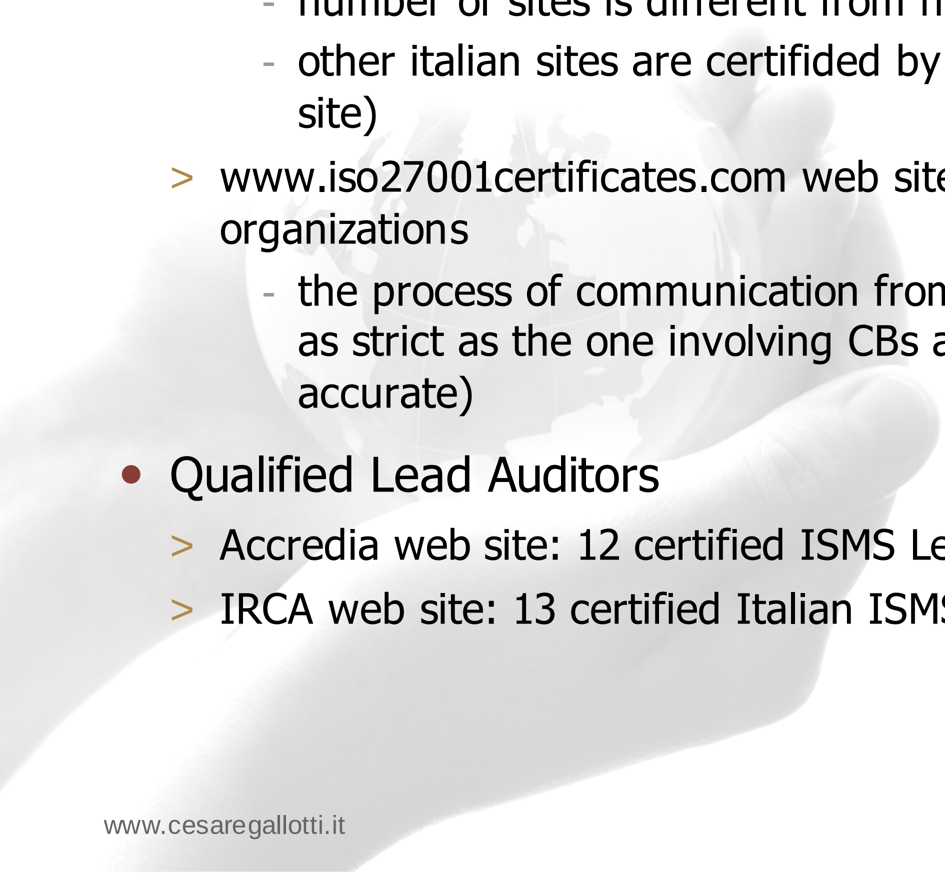
- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

Cesare Gallotti

- University degree in Mathematics
- Lead Auditor ISO/IEC 27001 (CEPAS), ISO 9001:2000 (IRCA), ISO/IEC 20000-1 (itSMF); ITIL Expert (Exin); CISA; Computer Forensics (Post Univ.)
- Past experiences
  - > Consultant, Project Manager and trainer in ISMS and ITSM for Italian consulting firms
  - > Lead Auditor and ICT Technical Responsible for DNV Italy (developing ISO 9001 in ICT, ISO/IEC 27001 and ISO/IEC 20000-1 certification schemes and training)
- Now Free-lance consultant:
  - > Consultancy in ISMS, QMS, Risk Assessment and Data Protection requirements
  - > Third party audits and assessments on Information Security, Quality Management Systems, MMD
  - > Training for LA ISO/IEC 27001, ITIL Foundation and Quality Assurance courses
  - > Activities in Europe, Africa and Asia for different kind of customers
- Web site: www.cesaregallotti.it

- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

Italian market in Information Security



- ISMS certificates:
  - Accredia web site: 294 certified sites for 9 accredited Certification Bodies
    - including Accredia certificates of organizations sited outside Italy
    - number of sites is different from number of organizations
    - other italian sites are certifided by foreigner CBs (not included in Accredia web site)
  - www.iso27001certificates.com web site: 60 ISO/IEC 27001 certified italian organizations
    - the process of communication from Certification Bodies to this web site is not as strict as the one involving CBs and Abs (i.e. data shall not be considered as accurate)
- Qualified Lead Auditors
  - Accredia web site: 12 certified ISMS Lead Auditors for 2 Italian qualification bodies
  - IRCA web site: 13 certified Italian ISMS Lead Auditors

Italian Market in Information Security

- Public sector have issued Requests for Proposal for IT services asking for Information Security Statements based on ISO/IEC 27002:2005 requirements
- Public sector and other big firms have issued RFPs for IT services asking for ISO/IEC 27001:2005 certificates, but it is still rare
- Some RFPs ask for ISMS Lead Auditors for consultancy teams (ISMS Consulting qualification programs are not popular)
- Big firms are usually concerned in ISMS, at least from a formal point of view
- Italian branches of international firms are usually involved in ISMS activities (certification, risk assessment, issuing security statements, etc)
- Personal Data Protection Law is one of the biggest drivers for information security
- Other regulatory drivers for telecommunication and finance companies and IT service providers.

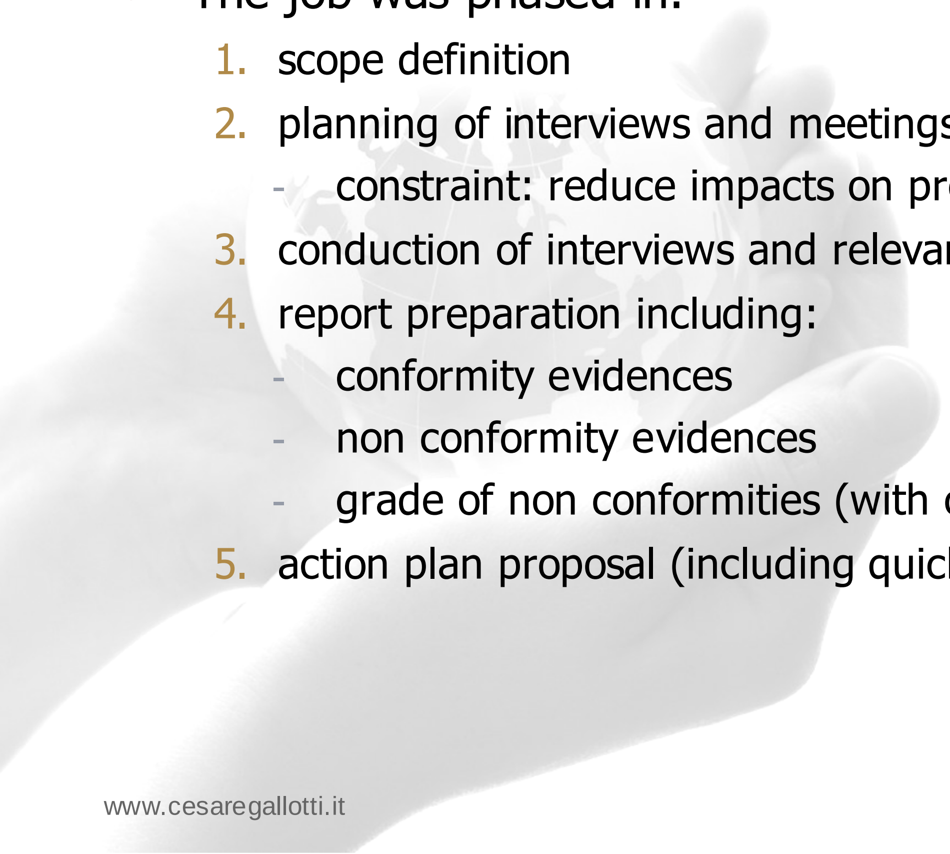
- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

The final customer

- The final customer activities are: the management of IT systems, networks and applications for finance customers.
- It has:
  - one main site,
  - one disaster recovery site (sited in an outsourcer's premises)
  - some "temporary" offices in customers' premises.
- The IT architecture is mainly based on mainframe system
- More than 100 employees are involved in the scope, excluding the numerous sub-contractors

The job

- The customer wanted an assessment against ISO/IEC 27001:2005 and ISO/IEC 20000-1:2005 for subsequent planning of improvement activities in order to obtain accredited certification.
- The job was phased in:
  1. scope definition
  2. planning of interviews and meetings
     - constraint: reduce impacts on productivity
  3. conduction of interviews and relevant documentation gathering
  4. report preparation including:
     - conformity evidences
     - non conformity evidences
     - grade of non conformities (with or without impacts on the certification path)
  5. action plan proposal (including quick wins)

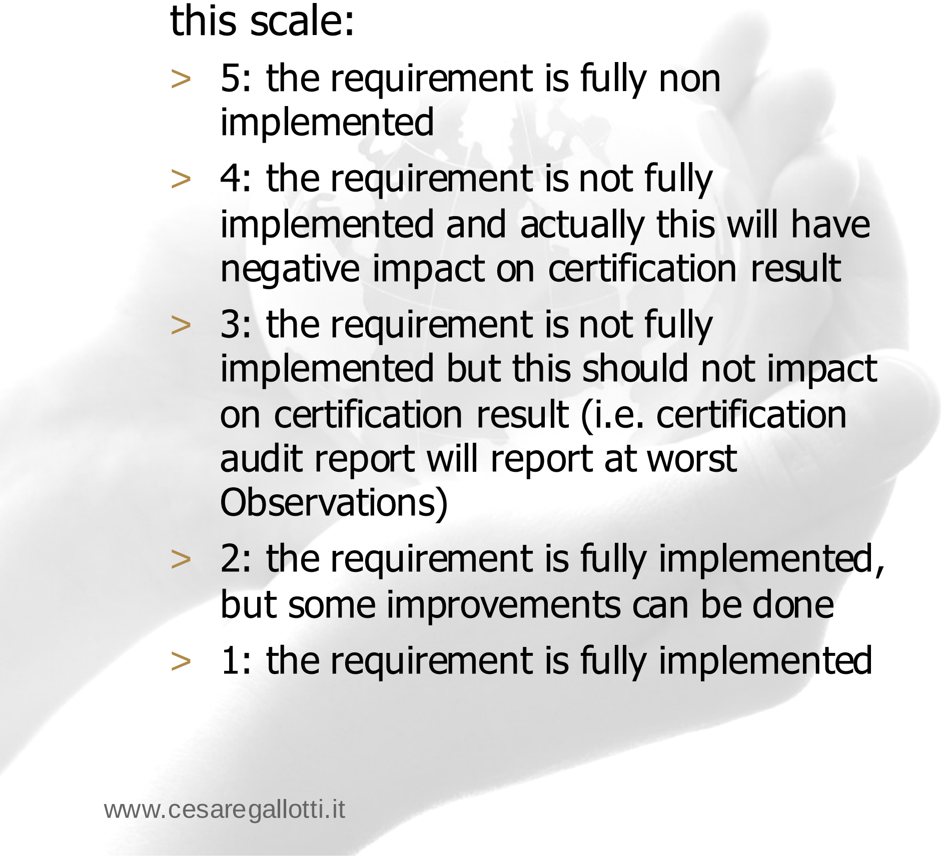


- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

Final deliverables

- The final deliverables were:
  - ISMS and ITSM scope document
  - minutes of meetings
  - assessment results
  - action plan
- The scope was written according to requirement 4.2.1.a of ISO/IEC 27001:2005
  - "characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope"
  - some marginal services were excluded
- The action plan is still under revision with the customer

“Assessment result” document (1/3)

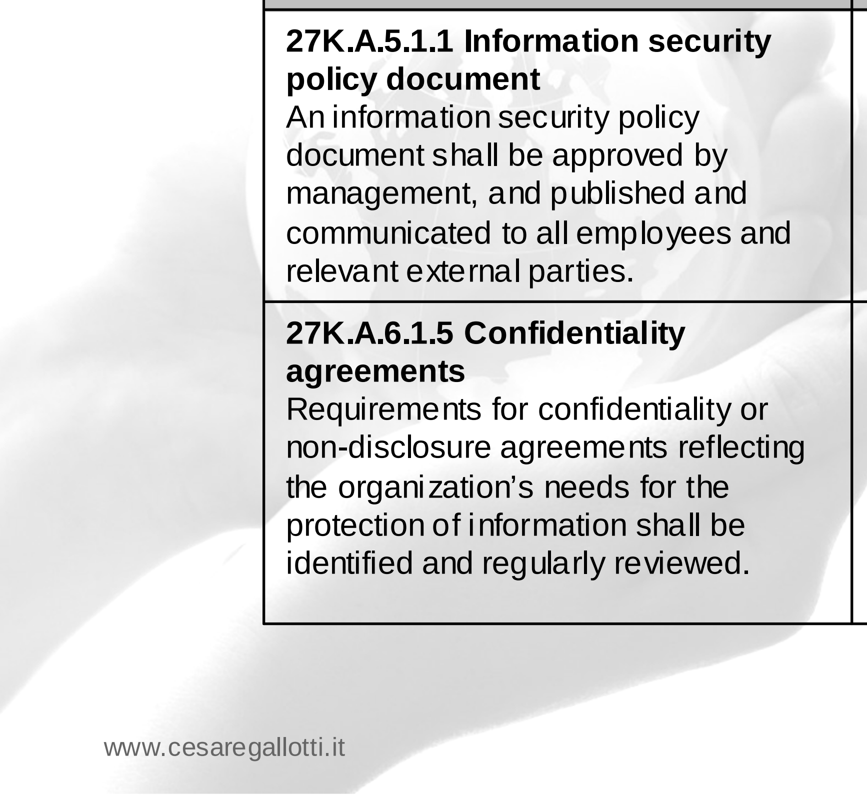


- For any requirement of ISO/IEC 27001:2005 and ISO/IEC 20000-1:2005, an analysis was given
- The evaluation was given according to this scale:
  - 5: the requirement is fully non implemented
  - 4: the requirement is not fully implemented and actually this will have negative impact on certification result
  - 3: the requirement is not fully implemented but this should not impact on certification result (i.e. certification audit report will report at worst Observations)
  - 2: the requirement is fully implemented, but some improvements can be done
  - 1: the requirement is fully implemented

27k Requirement	Analysis	V
27k.4.2.1.a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope (see 1.2).	Document “Scope” is in draft dated 2010-05-09	3

“Assessment result” document (2/3)

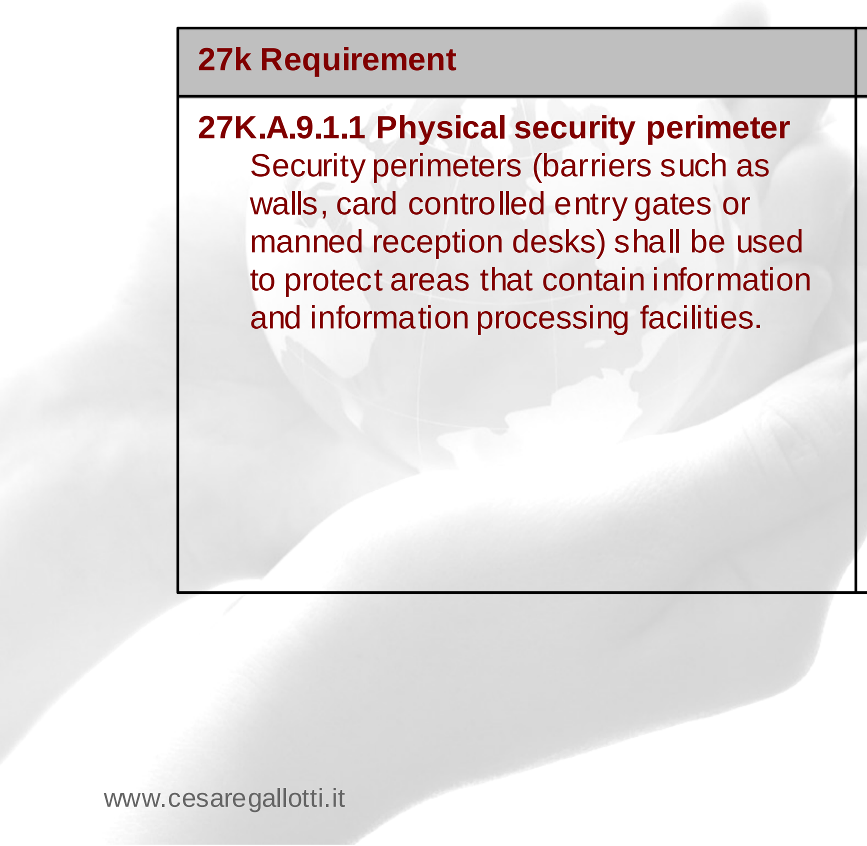
- Care was given to requirements which are repeated or better included in other requirements of one of the two standards.
  - > the term “repeated” should be intended as appropriate



27k Requirement	Analysis	V
27K.A.5.1.1 Information security policy document An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	Cfr 27k.4.2.1.b	3
27K.A.6.1.5 Confidentiality agreements Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified and regularly reviewed.	Cfr A.6.2.3 and 20k.7.3.c for suppliers Cfr 27k.5.1.c, 27k.A.8.1.3, 20k.3.3 for HRs	3

“Assessment result” document (3/3)

- Care was given to “evidences” with the key word “Ref”:
  - when citing documents (DOCxx) or
  - when citing interviews (“INT”) as reported in the minutes of meetings



27k Requirement	Analysis	V
27K.A.9.1.1 Physical security perimeter Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	This requirement is managed through "Physical Security Policy " (Ref DOC00-02-10). In this procedure (Ref DOC00-02-10): - physical risk assessment is not linked with the ISMS risk assessment (§ 3.7) - in chapter 4, there is written that “regular audits will be done” without links with the relevant procedure - only main site is cited (other sites are still under construction, but consideration is needed) During the visit, a barrier was open without control because of working construction (Ref INT11)	3

- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

Tools

- The most important tools we used were:
  - interviews
  - evidences
  - ISO/IEC 27001:2005
  - ISO/IEC 20000-1:2005
- No check lists were used because they
  - could block the interviews
  - would have been too complicated to prepare because the exact tasks of any organizational unit were not clear.

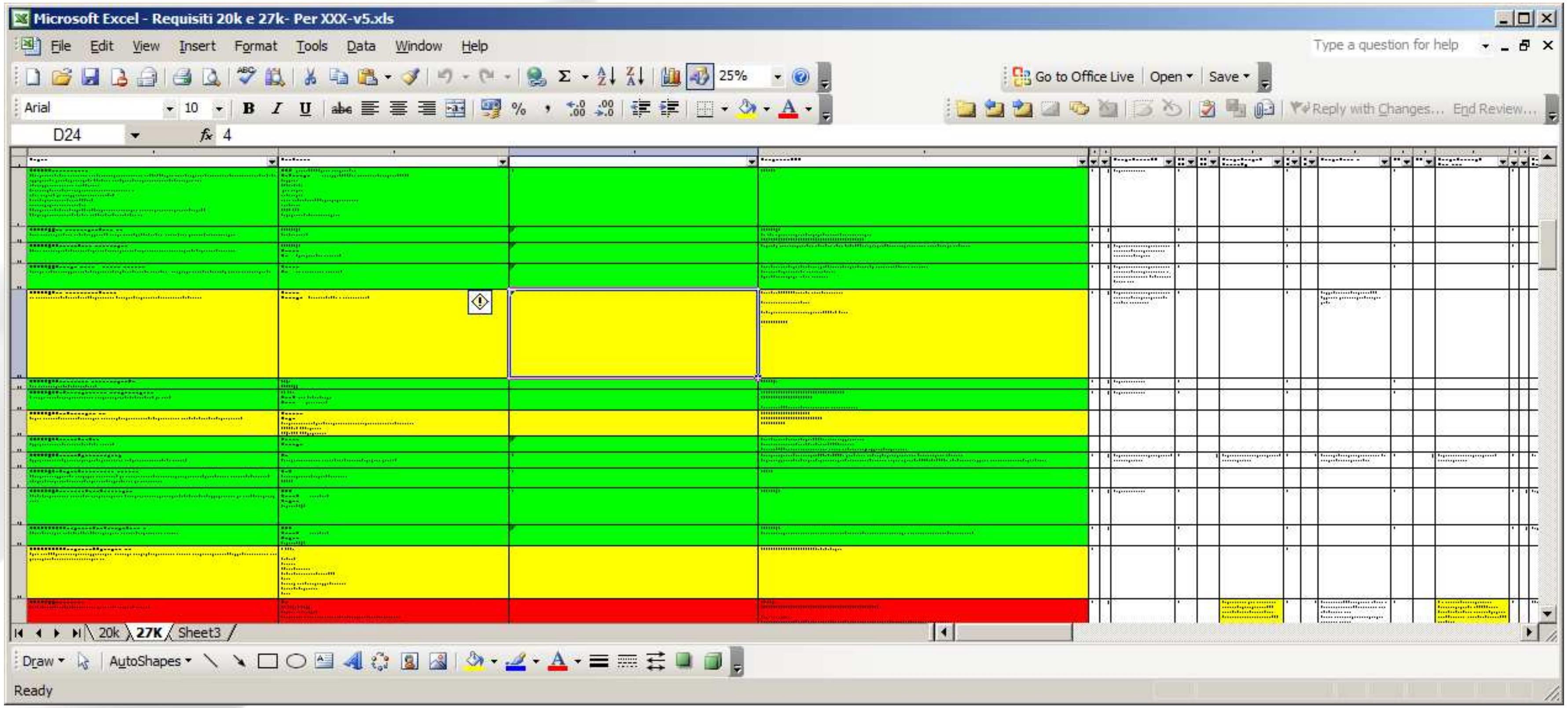
Recording of declarations

- A spreadsheet was used in order to record single declarations against applicable requirements
- For filtering, any couple requirement-OrgUnit was marked:
  - "P" when the unit is primarily accountable for the requirement
  - "S" when the unit is impacted by the requirement
  - null otherwise

Requirement	General notes	MFRM	NW	Fin	Notes for Finance Dept
20k.6.4.a) Budgeting and accounting for IT services There shall be clear policies and processes for: a) budgeting, and accounting for all components including IT assets, shared resources, overheads, externally supplied service, people, insurance and licences; b) apportioning indirect costs and allocating direct costs to services; c) effective financial control and authorization.	**All: if they have impact** **Finance**: primary, considering accounting, budgeting, authorizations for payments, emergencies Overhead: general costs	S	S	P	No procedure They can stratify earnings among services

Colours

- We marked rows:
  - in green when we had enough information for the evaluation
  - in yellow when we were waiting for some procedures or records
  - in red when we failed to correctly analyze the requirement with a relevant OU


Microsoft Excel - Requisiti 20k e 27k- Per XXX-v5.xls
File Edit View Insert Format Tools Data Window Help
Type a question for help
25%
Go to Office Live Open Save
Arial 10
Reply with Changes... End Review...
D24
fx 4
20k 27K Sheet3
Draw AutoShapes
Ready

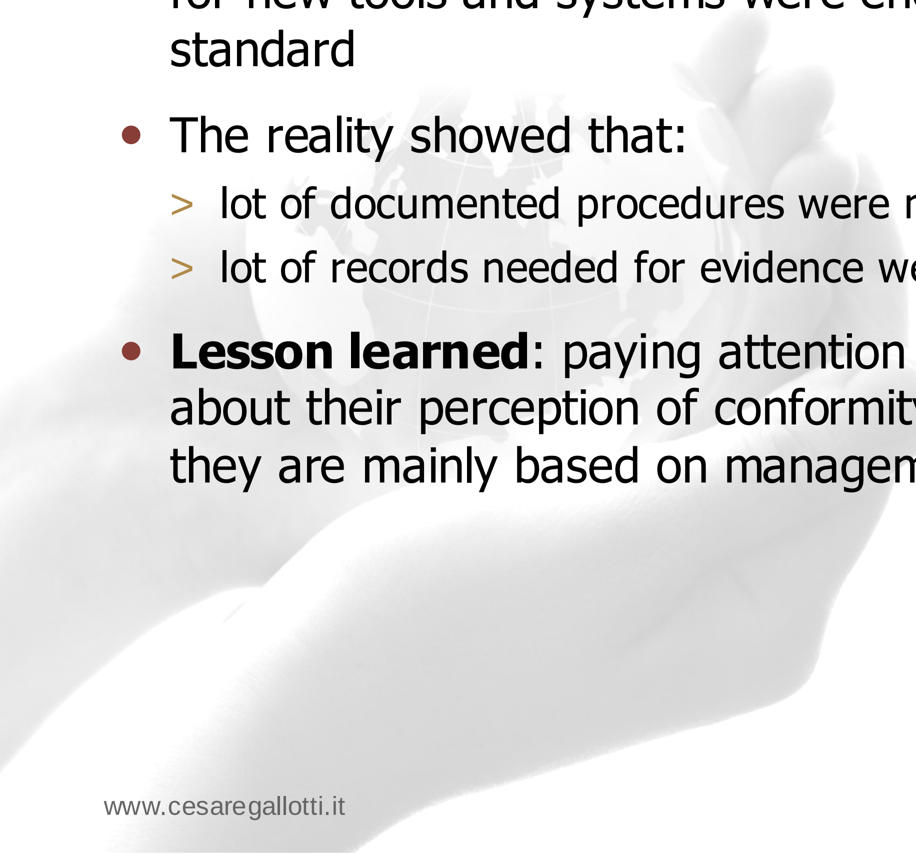
- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

Planning of interviews

- The first 2 meetings were for kick off with top management and for information gathering for scope definition
- Then, driven by the customer, we planned other interviews with top and middle managers
- During these interviews, they presented only general procedures and future projects and no evidences were given
- In the end of interviews with operational staff, we weren't able to plan other interviews with top managers in order to consolidate some information due to "lack of time"
- **Lesson learned**: plan a bottom-up approach for interviews after the first presentation

Technique vs Management vs Auditability

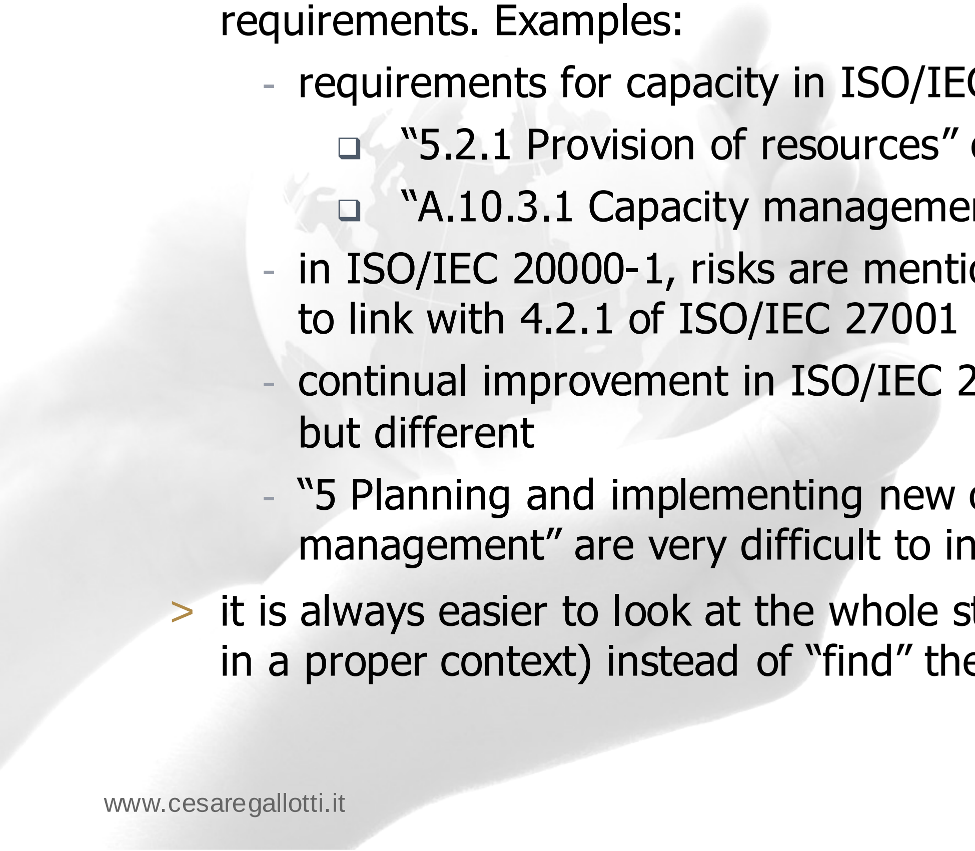
- Top management and quality and security representatives were confident about their high level of conformity to the standards
- Technical staff were confident that investments made in the previous years for new tools and systems were enough for achieving conformity to the standard
- The reality showed that:
  - lot of documented procedures were missing
  - lot of records needed for evidence were missing
- **Lesson learned**: paying attention to top management and technical people about their perception of conformity against Management System standards: they are mainly based on management and records, not on good tools.



Governance audit vs assessment

- Assessments are not audits. So, what is the difference?
- The customer was audited against COBIT by a major consultancy firm
- The report showed that evidences were gathered only through interviews with top management:
  - > no references to records or procedures
  - > lot of mistakes and inconsistencies due to “I’ve heard but I’ve not seen”
- Interviewed personnel were surprised about us asking “can I see an example?”, like it was the first time someone asked them
- **Lesson learned**: other assessments have other objectives than Management System certification, so don’t be confident that people will be prepared to show you procedures and records. Plan accordingly

Check lists? No, thank you

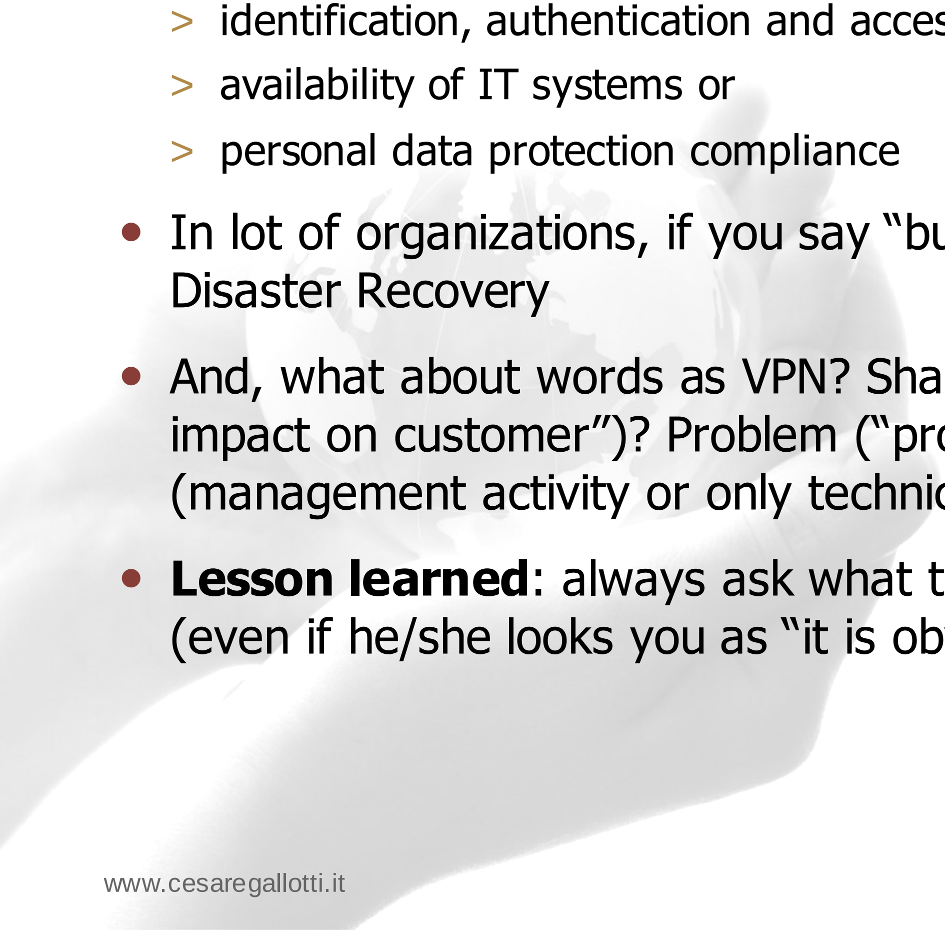


- We decided to not prepare any check list:
  - for preparing them we would have needed lot of time for understanding the activities of any function
  - it is very difficult to merge correctly ISO/IEC 27001 and ISO/IEC 20000-1 requirements. Examples:
    - requirements for capacity in ISO/IEC 20000-1 could be linked to
      - "5.2.1 Provision of resources" of ISO/IEC 27001
      - "A.10.3.1 Capacity management" of ISO/IEC 27001
    - in ISO/IEC 20000-1, risks are mentioned in different requirements, very difficult to link with 4.2.1 of ISO/IEC 27001
    - continual improvement in ISO/IEC 20000-1 and in ISO/IEC 27001 are similar but different
    - "5 Planning and implementing new or changed services" and "9.2 Change management" are very difficult to include in a check list
  - it is always easier to look at the whole standard requirements (with them included in a proper context) instead of "find" them in a check list

Minutes of meetings? Yes, thank you

- After any meeting, we prepared minutes in order to:
  - have feedbacks from interviewed (mistakes, other details not fully treated during the interview or in the report, corrections about names of products or functions)
  - review them when writing the final report
- Minutes didn't showed all items of discussion, but only those relevant for the assessment
- Minutes where used as "evidence" when stating comments in report for each requirement

What is security? And continuity? And...



- In short: security is about confidentiality, integrity and availability.
- In lot of organizations, “security” means only:
  - identification, authentication and access control of users (this case) or
  - availability of IT systems or
  - personal data protection compliance
- In lot of organizations, if you say “business continuity”, they think only about Disaster Recovery
- And, what about words as VPN? Share? Firewall? Incident (“only when it has impact on customer”)? Problem (“problem = major incident”)? Change (management activity or only technical)? etc.
- **Lesson learned**: always ask what the auditee means with these words (even if he/she looks you as “it is obvious!”)

- Presentation
- Italian market in Information Security
- The customer and the requirements of the ISO20k+ISO27k assessment
- Final deliverables
- Tools
- Lesson learned
- Conclusion

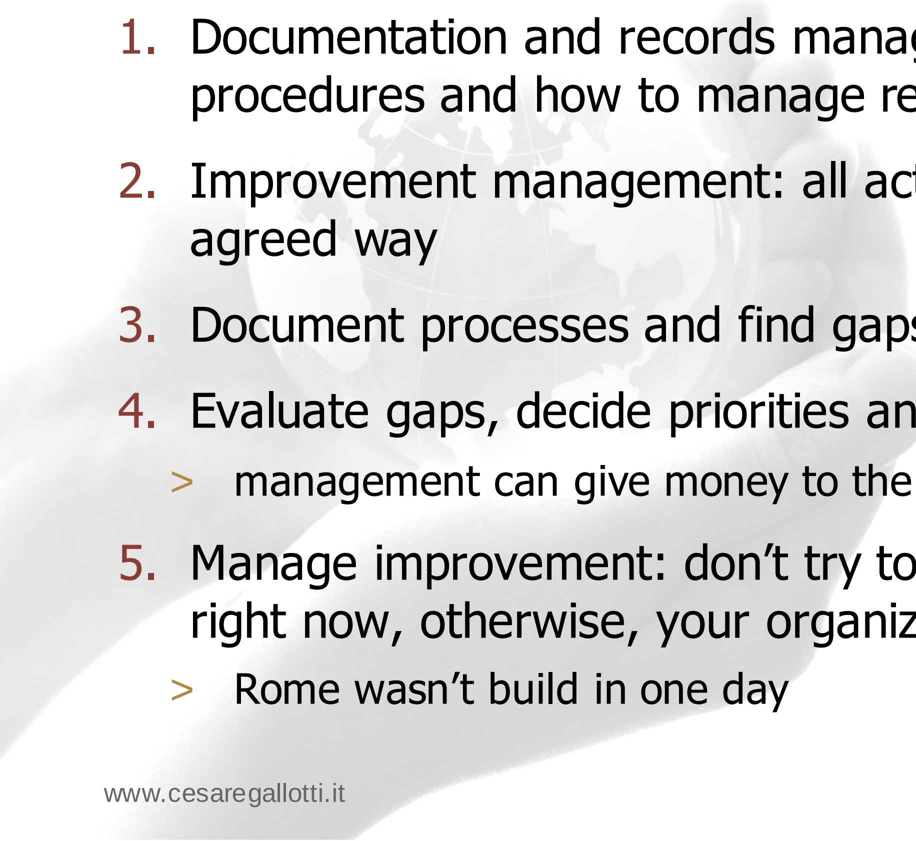
Final results

- Final results were:
  - not all required documented procedures where available
  - procedures where not managed according to a standard template and they weren't linked with each other
  - risk assessment were not conducted according with ISO/IEC 27001 requirements (no links among threats and actions)
  - there were a lack of conformity records or they were archived in not-standard ways
- The most critical issue: lots of internal projects were chartered (measurement of performances, demand management, project management improvement, service catalogue and CMDB), but they weren't linked with the requirements of the standards. This could lead to the need of changing requirements of these projects, with consequent extra costs and risks
- Too many tools were used for the same task (e.g. 4 different tools for incident management) with lack of coordination and consequent lack of "systematic approach": any function decided to implement their own improvements
- Contract with suppliers were not formally linked with SLAs with customers

Shared misfortune...

- In Italian we say "Shared misfortune is half joy".
- Experience tells that lot of organizations share the same lacks (even ISO/IEC 27001 certified organizations).
- Obviously, it is not true that there is any "half joy", but only "shared nonconformities" ;-)

My top 5



0. Management commitment: obviously, if management doesn’t give its support, no one will work on the ISMS/ITSM project;
   - this will also mean that all actual internal project shall be stopped and reviewed in order to align them with ISO/IEC 27001 and 20000-1 requirements
1. Documentation and records management: if you don’t know how to publish procedures and how to manage records, the next steps will be impossible
2. Improvement management: all actions from now on shall be managed in a agreed way
3. Document processes and find gaps: don’t get depressed! Just find gaps
4. Evaluate gaps, decide priorities and have a Management Review:
   - management can give money to the actions and coordinate the different functions
5. Manage improvement: don’t try to be 100% compliant to the standards right now, otherwise, your organization will have troubles
   - Rome wasn’t build in one day

- **Thank you**

- Cesare Gallotti
  cesaregallotti@cesaregallotti.it
  http://www.cesaregallotti.it
  http://blog.cesaregallotti.it