USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

CYBERSECURITY STANDARDS AND BEST PRACTICES: PART 2 - UTILITIES AND ISO/IEC 27001 ISMS 2005/2013

STEFANO BRACCO, ACER

ACER
Agency for the Cooperation of Energy Regulators

First approach with ISO/IEC 27001 standard

Summary

- Starting with the basics of ISO 27001 to understand best practices
- The systematic approach toward certification and information Security certification systems
- The certification path: from preparation of an audit to certification of utilities and energy market participants
- Answers to uncomfortable questions (by the end of this session)

Pills of implementing ISO 27001: the steps

- **Step 1 - Ensure management support**
- **Step 2 - Define the scope of an audit**
- **Step 3 - Define and perform Risk Assessment**
- **Step 4 - Process the Risk Treatment**
- **Step 5 – Define the Statement of Applicability**
- **Step 6 - Develop a Risk Treatment Plan**
- **Step 7 - Implement controls**
- **Step 8 - Monitoring the implementation of the ISMS**

Pills of ISO 27001: how the standard looks like

4 Context of the organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the information security management system

4.4 Information security management system

5 Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

6 Planning

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

7 Support

7.1 Resources

7.2 Competence

7.3 Awareness

Pills of ISO 27001: how the standard looks like

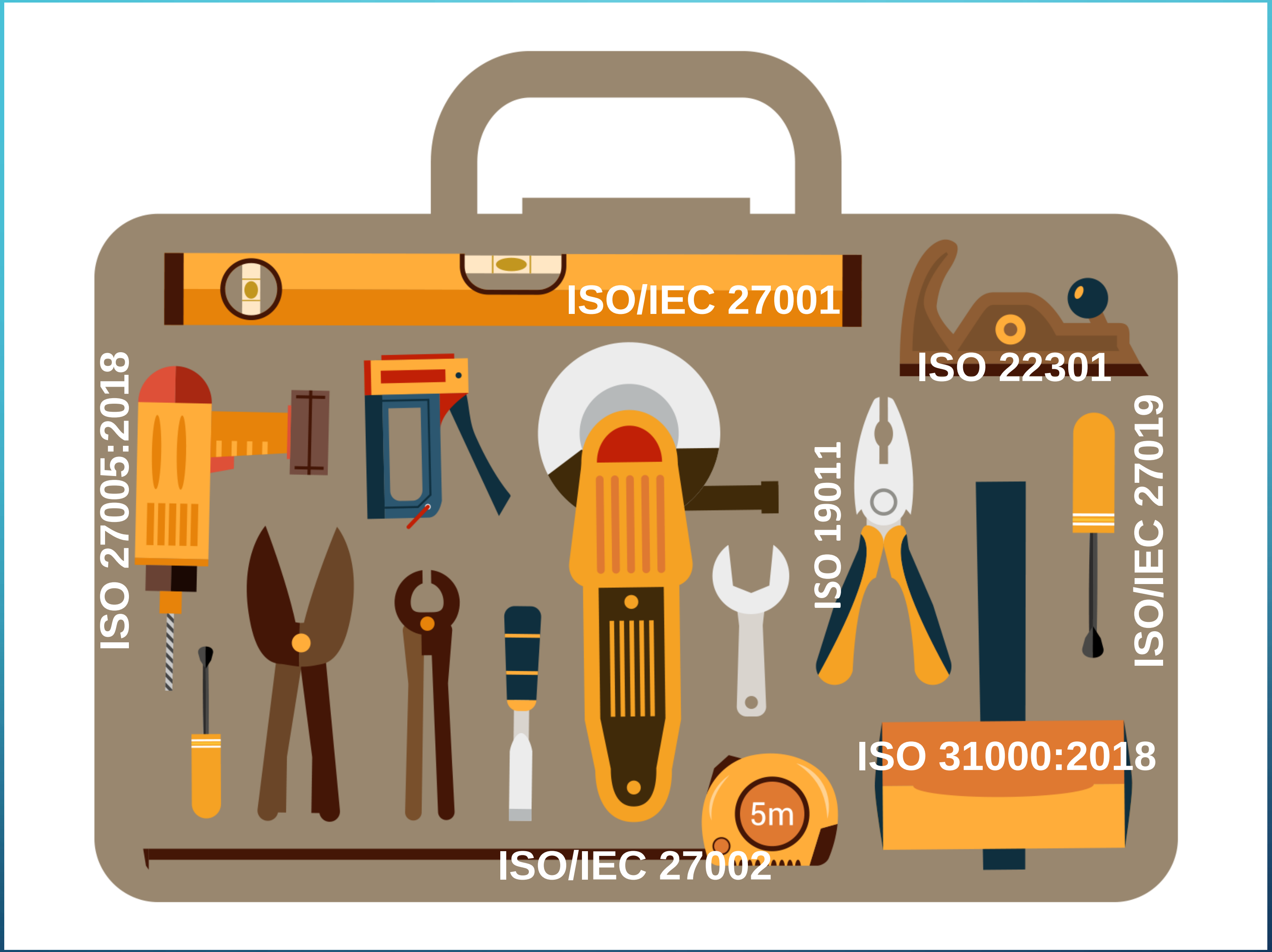
7.4 Communication
7.5 Documented information
8 Operation
8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment
9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review
10 Improvement
10.1 Nonconformity and corrective action
10.2 Continual improvement
Annex A (normative) Reference control

Which version?

2005 vs 2013 vs ??

Systematic approach

My toolbox.....


ISO/IEC 27001
ISO 22301
ISO 27005:2018
ISO 19011
ISO/IEC 27019
5m
ISO 31000:2018
ISO/IEC 27002

A toolbox cannot help you if you would select the wrong tools

- First step in implementing cybersecurity through ISO: decide what you want to achieve (areas that you want to cover, processes will be in scope, level of deepness you intend to go into);
- Select the right tool(s) that would better fit with the purpose and your needs;
- Controls are equally important, but some are crucial for utilities, for this reason we have specific guidelines for them (ISO 27019);
- Auditors act based on standards as well: know the way they act reading proper standards!
- In any case, first familiarise with standards yourself….

A toolbox cannot help you
if you would select the wrong tools

- ❖ *ISO/IEC 27001:2013 can be complex only if you approach from a distance with no knowledge: seek for help, if possible, or study with a bit of guidance*
- ❖ *ISO/IEC 27001:2013 is a way to think and to approach security problems, it is not a low level standard to blindly apply or a “tick the box approach”*
- ❖ *Before using it, try understand the general philosophy of ISO and ISO 27001 standard*

Digging into the standard: the audit as a compulsory step for achieving CERTIFICATION

An audit is….

“A systematic, independent and documented process for obtaining audit evidence (3.3) and evaluating it objectively to determine the extent to which the audit criteria (3.2) are fulfilled”

ISO 19011

The auditor

- S/he is not an inspector and not a referee, just an auditor (ISO 19011)
- **S/he is a certified professional**
- **S/he is a domain specific professional**
- **Auditors are there to help, and not there to take a position against or in favor**

Relationship between the utility and the auditor

- S/he is focused on the scope and not on all other facts
- S/he is not there to provide any judgement, but just to check that you comply with a reference norm
- Focused on what you did, what you documented, how solid is your job and if s/he can have enough evidences that you comply
- Can offer two additional pair of eyes or innovative ideas

Tip: Before becoming confrontational with an auditor, try to understand which is the interpretation of the norm by the auditor, then try to agree on the common view and on the strategy to achieve that part of the norm.

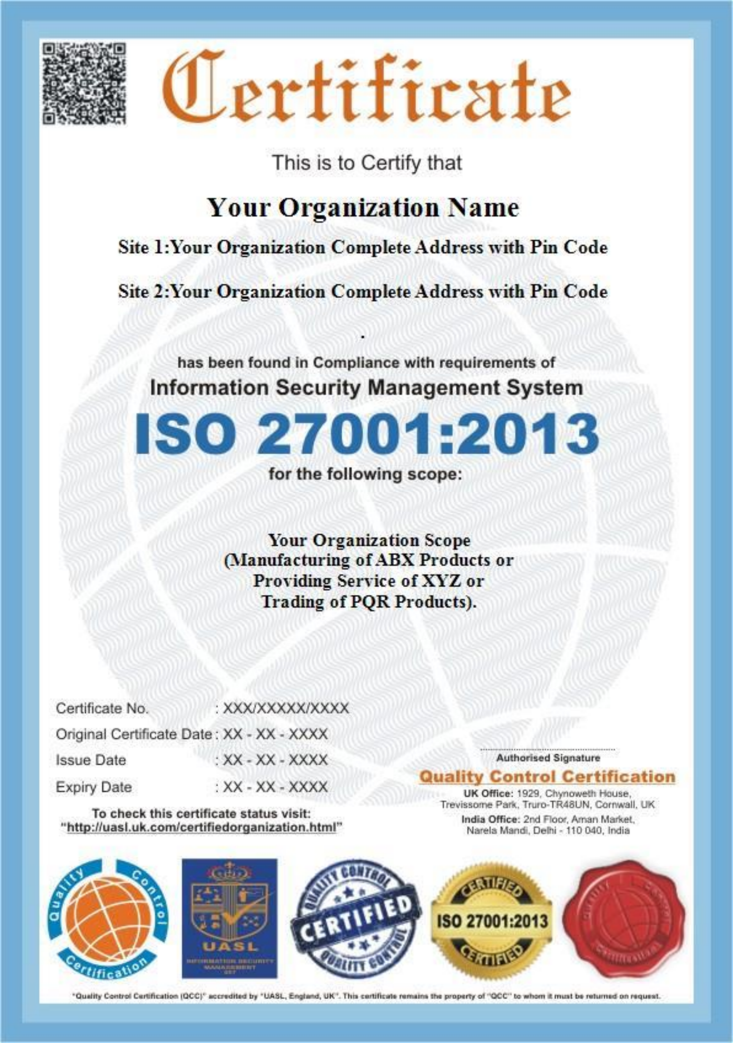
The audit process

- ❖ Preliminary visit
- ❖ Audit certification visit
- ❖ Recertification visit
- ❖ Surveillance audits
- ❖ Average cost
- ❖ Is it really needed?

The aftermath of an audit

And the winner is.....

- The one who started well
- The one who knows that can do better
- We know our business



Certificate

This is to Certify that

Your Organization Name

Site 1:Your Organization Complete Address with Pin Code

Site 2:Your Organization Complete Address with Pin Code

has been found in Compliance with requirements of

Information Security Management System

ISO 27001:2013

for the following scope:

Your Organization Scope
(Manufacturing of ABX Products or
Providing Service of XYZ or
Trading of PQR Products).

Certificate No. : XXX/XXXXX/XXXX
Original Certificate Date : XX - XX - XXXX
Issue Date : XX - XX - XXXX
Expiry Date : XX - XX - XXXX

To check this certificate status visit:
"http://uasl.uk.com/certifiedorganization.html"

Authorised Signature

Quality Control Certification

UK Office: 1929, Chynoweth House,
Trevissome Park, Truro-TR48UN, Cornwall, UK

India Office: 2nd Floor, Aman Market,
Narela Mandi, Delhi - 110 040, India

"Quality Control Certification (QCC)" accredited by "UASL, England, UK". This certificate remains the property of "QCC" to whom it must be returned on request.

The aftermath of an audit

POOR
FAIR
GOOD
EXCELLENT

What not to do if you loose

- Do not argue with an auditor
- Do not fire your CISO
- Do not punish anyone involved in a negative result: just analyze what happened and set corrective measures.

What to do if you loose

- Ask explanations to the auditor
- Plan to re-do the work and ask your CISO what was missing/what went wrong
- Try to build an information security culture before approaching the next attempt: anyway you are on the path, it will just take some more time.

ISO 27001 doesn't mean absolute security by standard and definition

- ISO 27001 means I understand my business and my information security risks
- ISO 27001 means I have a method to manage risks and to work on them and my company is conscious
- ISO on 27001 on low level means I can set a plan to achieve a complex plan
- ISO on 27001 on low level means I can have an incident and I have a process to manage it
- ISO on 27001 on low level means I do mistakes, but I learn from that
- ISO on 27001 on low level means I may have a lot of technology that would help me and I decide how to use it

ISO 27001 certification would be useless if….

If I will do just because of a legal requirement with no value added:

- Hire a consultant to set up the system;
- Hire a consultant to prepare certification papers;
- High a certification body to obtain the ISO 27001 certification.

If utilities would just copy/paste from others avoiding to assess and mitigate their real information security risks;

If utilities would just copy/paste from others avoiding to assess and mitigate their real information security risks;

Common mistakes approaching ISO 27001 certification

- *Standards come with glitches, vulnerabilities and possible improvements: standards are done by people and for people and developed over time*

- *Auditors are people as well: they assess based on what you tell them. If you lie to an auditor you will get a (fake) “certification“ at your own risk.*

- *In case you do a good job, you will received a deserved well-recognized paper re-assuring others that their and your information are safe, at the extent possible*

- *Standards cover specific areas with different levels of detail, but more you know and use them more shining will be the .*

- *If you do not like ISO, we respect this, until you do something: you keep safe,secure and healthy, delivering energy to end customers.*

We are ISO!

- Each Nation can contribute to ISO Standards
- Each expert can help in making it better
- Each country can have its own specific reading with specific shades
- We do not tick boxes, we check that tasks are executed in the right way
- We share a system but not the implementation
- We can trust others because we all manage to have a system, still in different contexes
- We certify methods and processes
- We do not certify the people or products

Thank you for your attention

We are here to help!

www.acer.europa.eu