ISO-27001 ISMS

Lessons learned and useful tips for CISOs to turn their day to day work into a management system

Julien Levrard
<Julien.levrard@hsc.fr>

Hervé Schauer Consultants

- IT security company founded in 1989
- Fully independent intellectual expertise services
  - Free of any distribution, integration, outsourcing, staff delegation or outside investors pressure
- Services: Consulting, coaching, audits, pentests, training
- Fields of expertise
  - Technical security
    - OS, Network, Application, industrial systems, infrastructure
  - Organizational security
    - IS management, Risk management, ISO-27001, PCI DSS, ARJEL, HDS
  - Business Continuity
  - Legal
- Certifications
  - CISSP, ISO 27001 Lead Auditor, ISO 27001 Lead Implementor, CISA, PCI-DSS QSA, ISO 27005 Risk Manager, ITIL, GIAC GCFA, GIAC GPEN, OPQCM, OPQF, etc.

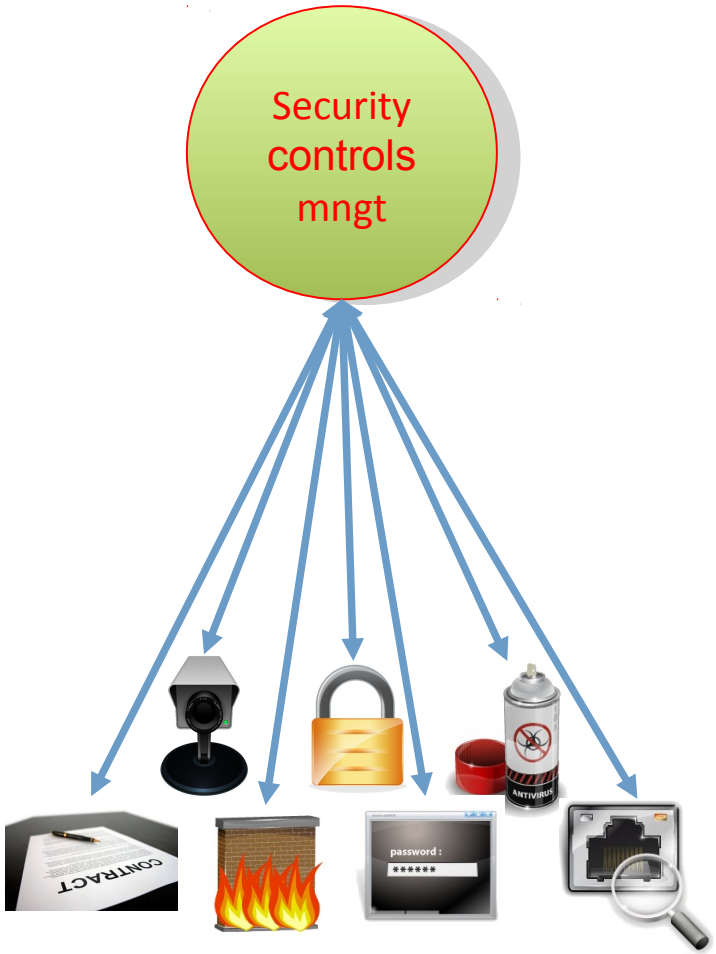
The need for an HSC ISMS framework

- Objective:
  - Unify our way of implementing ISMS
  - Capitalize the lessons learnt within our engagements
  - Generic framework that should be simple enough to be understood by a business manager in 5 min
  - Logical segregation of ISO-27001 requirements
- How to do it:
  - Think as “the management”

Security controls

- Premise n° 1:
- **No organization has been waiting any ISO standard to implement security controls**

Security controls management

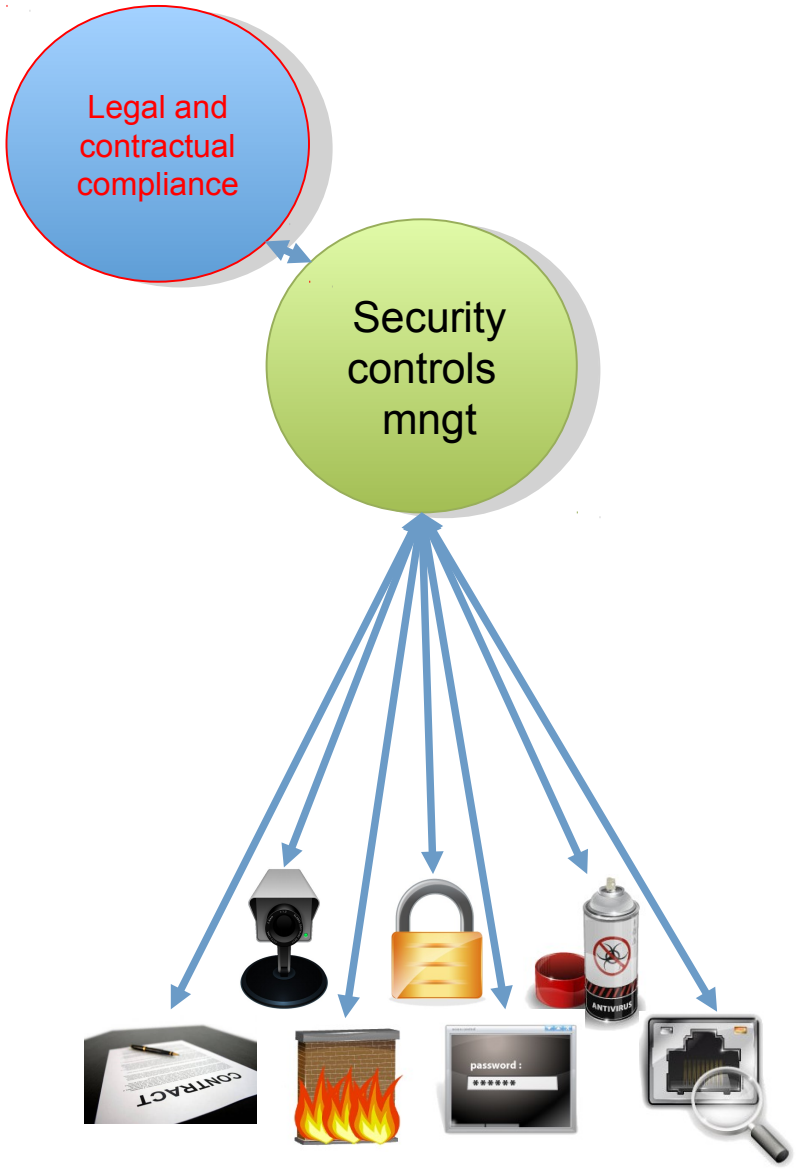


- Do we know
  - What security controls are in place or planned
  - What activities are associated to these controls and who is in charge of them?

- Premise n°2:

  We expect the CISO to be able to answer those questions

Mandatory compliance management

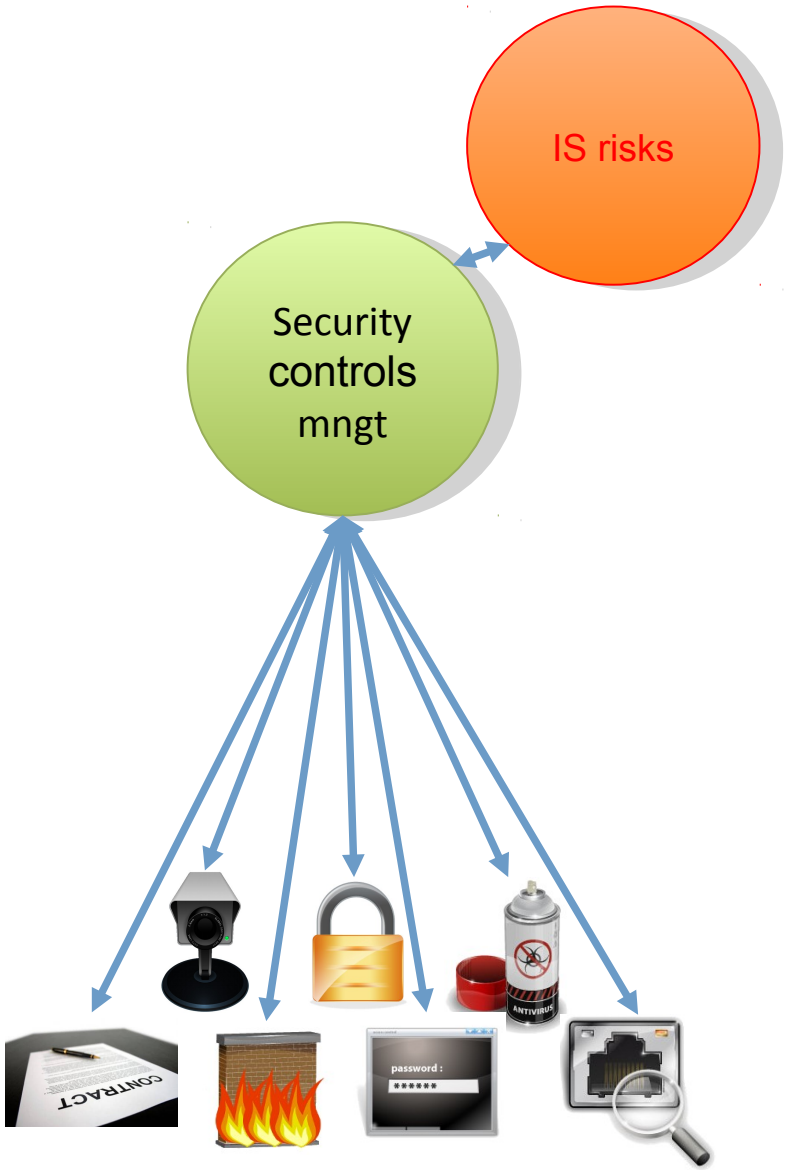


- Did the CISO identify
  - Legal and contractual requirements regarding Information Security?
  - What security controls should be implemented in order to cover them?

- Premise n°3:

  The CISO knows what are the mandatory security requirements the organization is subject to and what to do to keep people out of jail

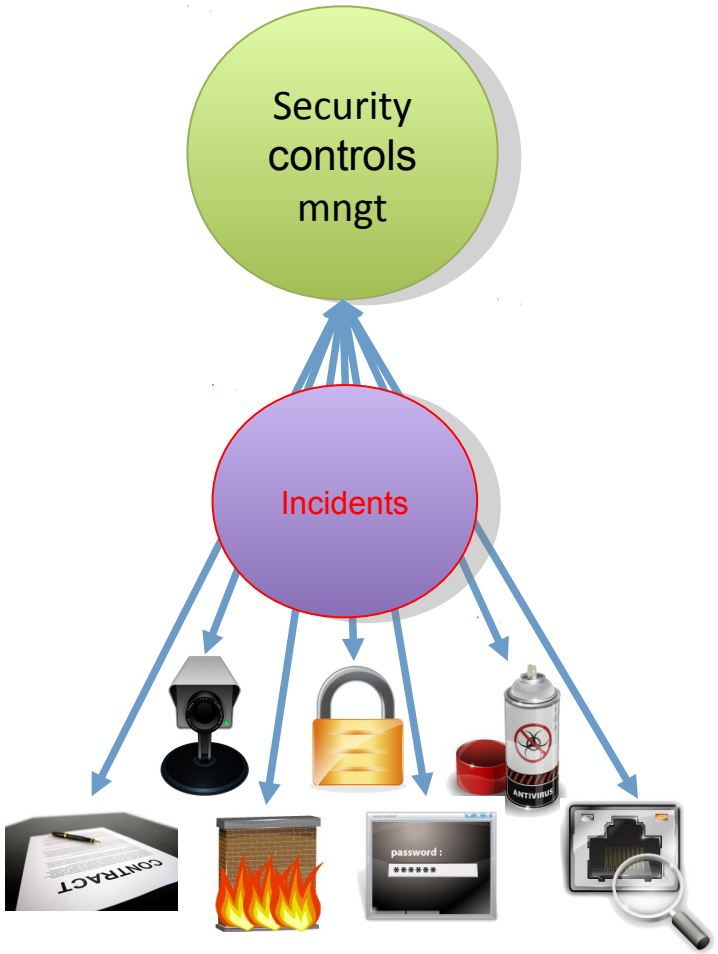
IS risks management



- Did the CISO identify/understand
  - What the interested parties expectations are?
  - The important processes and information that should be protected?
- Are information security expenses efficient?
- Does the CISO have a good understanding of the information system?
- Premise n°4:

  The CISO understand the business risks and is capable of interpreting them as information system risks and pilot the security expenses according to those risks

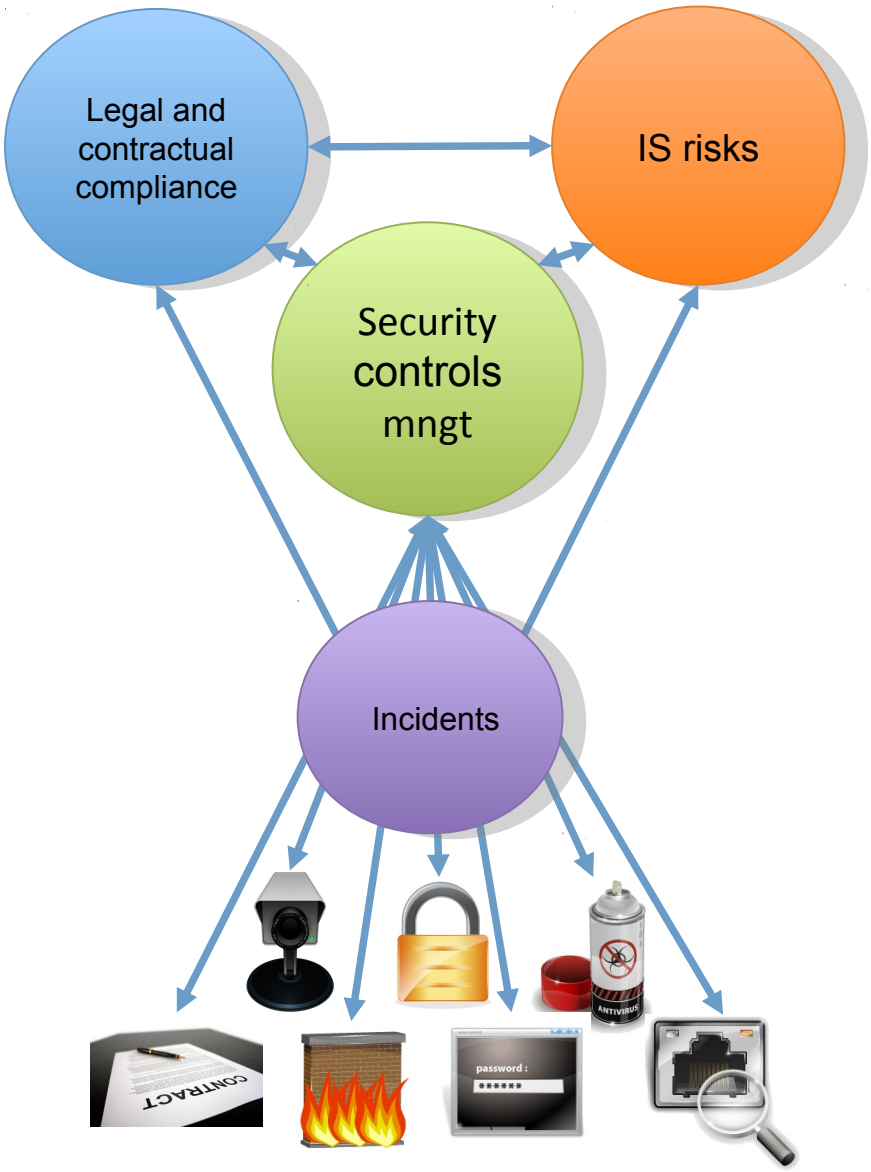
IS incident management



- Premise n°5:

  If a severe incident is badly managed, the CISO loses his job

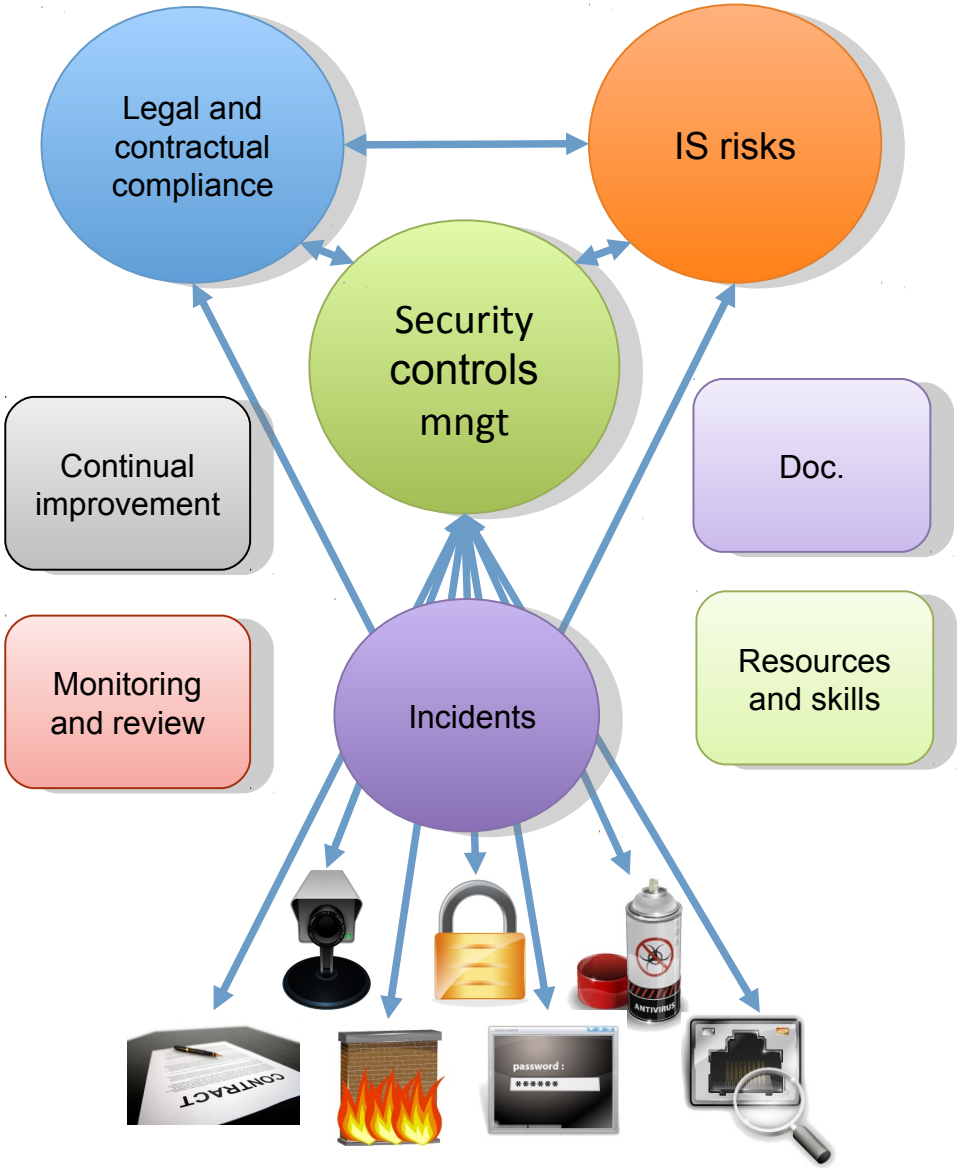
Summary of the 5 premises



- No organization has been waiting any ISO standard to implement **security controls**
- We expect the CISO to know what **security controls** are in place and who is in charge of them
- The CISO knows what are the **mandatory security requirements** the organization is subject to and what to do to stay out of jail
- The CISO understands the **business risks** and is capable of interpreting them as information system risks and pilot the security expenses according to them
- If a severe **incident** is badly managed, the CISO loses his job

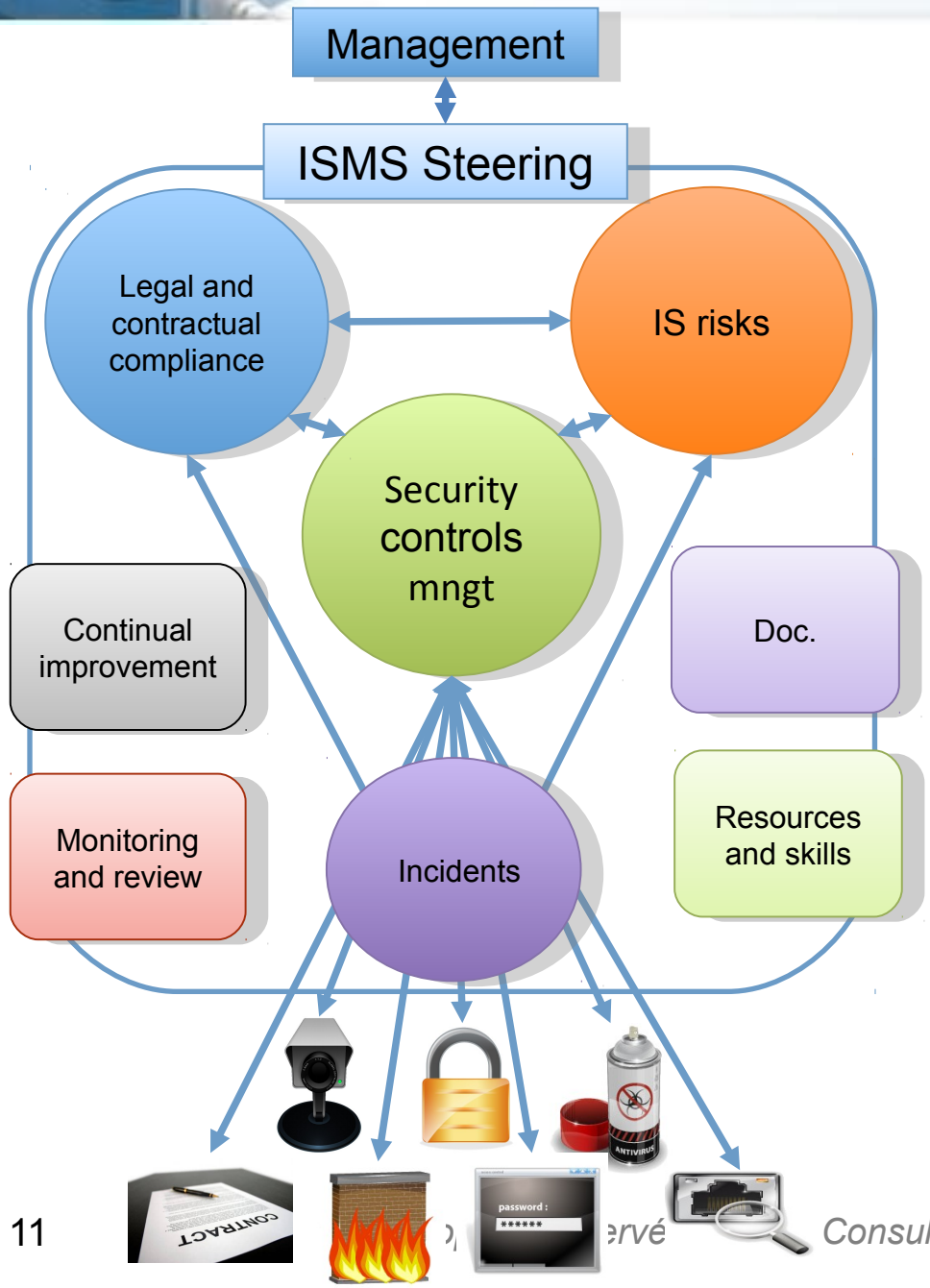
These 5 premises are applicable to any organization that pretends managing information security

Information Security management system (ISMS)



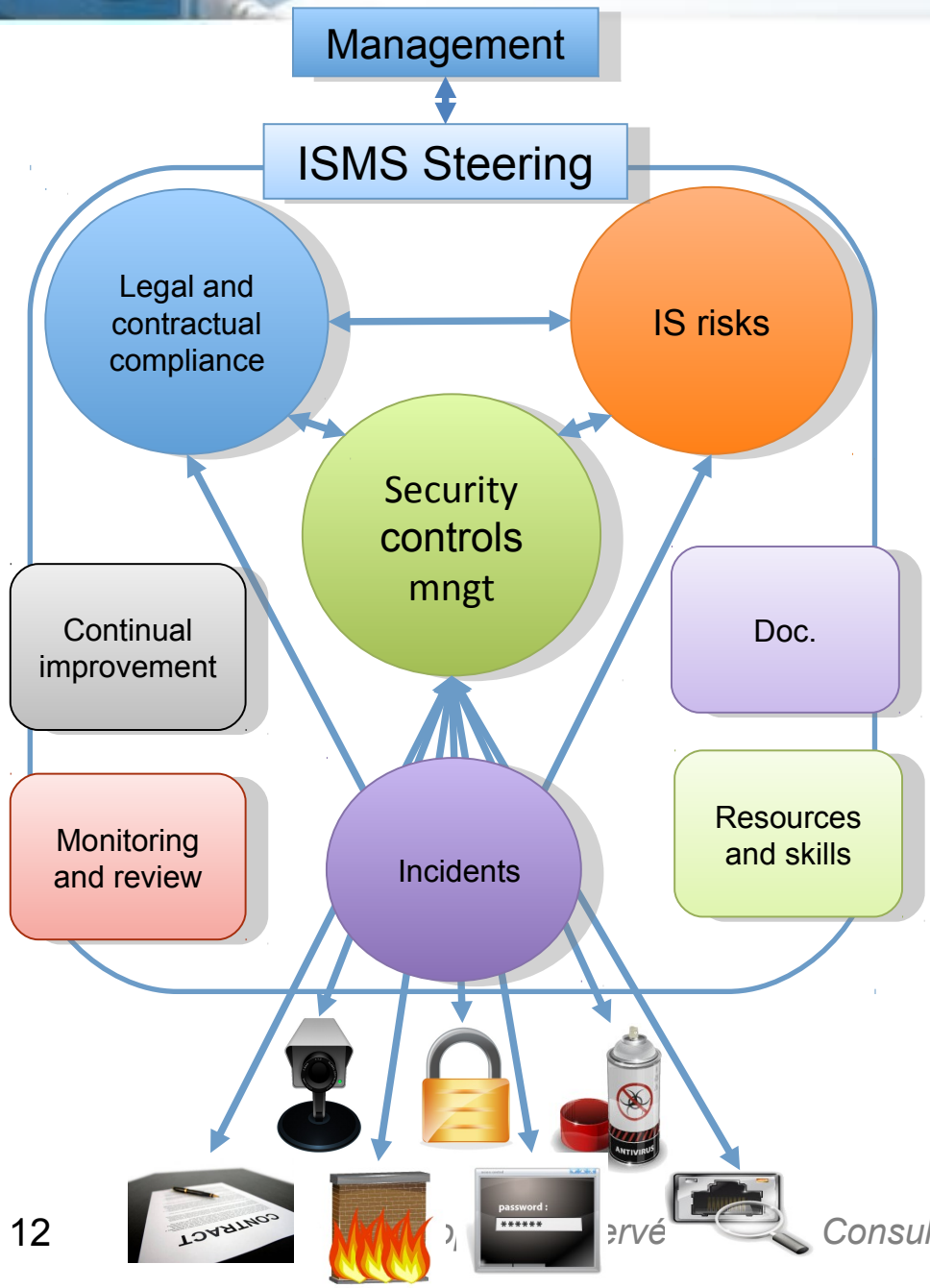
- Implementation of P-D-C-A way of working for all security management activities
  - Documentation management
  - Records management
  - Resources management
  - Training and awareness management
  - Monitoring and review
  - Continual improvement

How to comply with ISO-27001



- Formally involve the management
- Formalize information security management processes
- Formalize mandatory documents and records:
  - Statement of Applicability
  - ISMS policy and perimeter
  - Risk assessment methodology
  - Etc.

HSC ISMS model



- Represents best practices in information security management
- Relevant for any type of organization (just like the standard)
- Easy to understand and accessible to management and business owners
- Segregates the ISMS in logical activities
  - Eases maturity assessment
  - Structures the ISMS project plans
- Directly usable as a framework
  - For initial assessment
  - For implementation project
  - For internal audit

Implementation feedback and advice for the clueless CISO

An ISMS is not a compliance project

- Do not

  Drive your implementation project following the standard sequentially

  - With the ISMS seen as a compliance project
  - Using a GRC tool to drive your implementation

- But do:

  Use a solid information security management framework

  - Customized to fit your actual information security organization

Think “Run” as soon as possible

- Do not:
  - Implement an ISMS without anticipating the ISMS after its certification
    - The standard is strongly mixing:
      - The target: A state of the art IS management
      - The project steps to reach the target
  - Appoint only a project manager
    - And forget to appoint a CISO
- But do:
  - Anticipate the “run” phase during the “build” one
  - Project activities → Continual improvement
  - Risk assessment interviews → Internal audit interviews
  - Project manager → CISO

Segregate management controls from risk reduction controls

- Do not:
  - Consider all 133 annex A security controls to mitigate technical risks
    - Some controls reduce all risks:
      - A.5.1.1, A.6.1.1, A.8.2.2, A.15.1.1 …
    - So we have to select them anyway
    - It's difficult to measure how risks are reduced by these controls
- But do:
  - Consider these security controls as management process activities
  - Focus risk assessment on technical risks and associated security controls (A.9, A.10, A.11 and A.12)
  - Turn your “compliance oriented” risk assessment into an operational document that you can share with technical staff

Be a guide, not a pen-pusher

- Do not:
  - Try to implement an ISMS without the operational staff's involvement regarding security controls
    - Documentation, monitoring
    - Weak link between CISO and staff
    - It's often easier to document and manage documentation of security controls on your own or with consultants but:
      - The ISMS will not be working and it will lead to a double security controls documentation with inconsistency issues
- But do:
  - Help, explain, guide, support, check, monitor, train (but do not do their job)
  - Find support within middle management to enforce your requests

Create your own security controls management tools

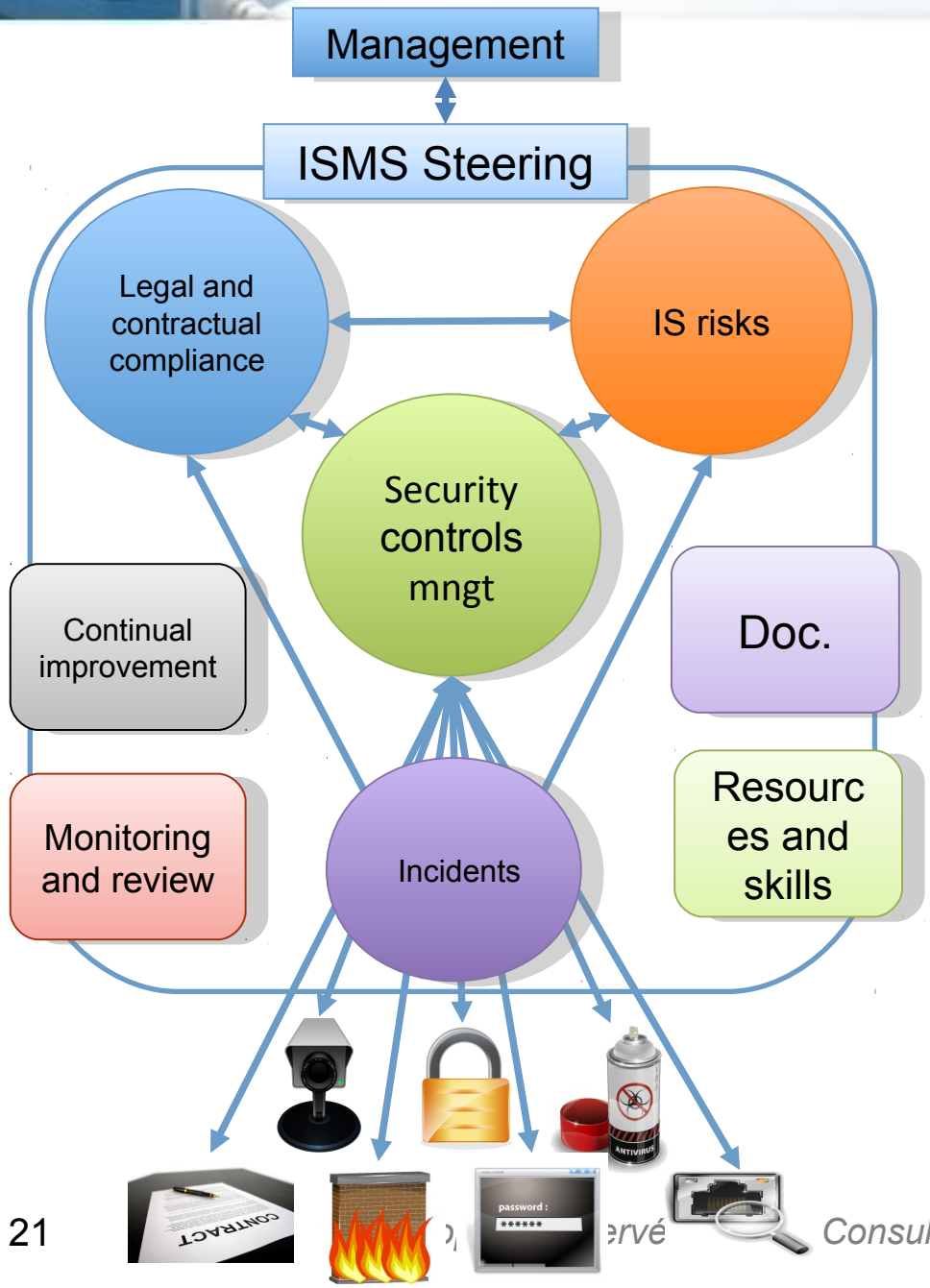
- Do not :
  - Use SOA as a tool for managing security controls, or worst, as a risk treatment plan
    - Except if you like the way it's organized ;-)
    - It will lead to a painful and laborious way to manage your security controls
- But do:
  - Arrange you security controls list the way they are *actually* operated and managed
  - Use the SOA to check completeness and to communicate with the auditor
  - Consider formalizing a high level global RTP and specific operational RTPs (HR, IS, Business, etc.)

Check, check, check and check again

- Do not:
  - Neglect monitoring and review activities
    - It's the CISO's strongest tool to validate the work
    - With no M&R, the CISO stays on a theoretical level and do not identify operational issues
    - The ISMS is one-way (IS policy style)
  - Underestimate the internal audit costs
  - Underestimate the cost of adequate records and indicators
- But do:
  - Formally monitor the project progress and RTP implementation
  - Invest strongly from the beginning of the project in monitoring of security controls efficiency
  - Link all audit activities to the ISMS (Pentest, SOX, ISAE 3402, etc.)

What are we working on?

Work in progress



- Continual improvement with consultants field feedback
- Improvement of best-practices for each process
- Optimization of our engagement and improvement of quality
- Integration of other security frameworks within the ISMS:
  - Health Care data
  - PCI DSS
  - Online gaming
  - SOX/ISAE-3402
- Automation of indicators management to monitor the ISMS

Questions ?

?