EPIC Cloud
Panoramica e aspetti di utilità generale per l’INFN

Barbara Martelli

Meeting RTD 20 dicembre 2021

EPIC Cloud – Enhanced PrIvacy and Compliance Cloud

- Nata dall'esigenza di alcuni progetti in ambito salute di gestire dati personali e particolari nel rispetto delle normative nazionali e internazionali (GDPR, autorizzazioni del Garante Privacy, Misure Minime AgID – direttiva NIS, D.Lgs n. 196 30 giugno 2003, ecc…)
  - Harmony Alliance
  - Alleanza Contro il Cancro
  - Altri progetti che trattano dati medici
  - Oggi anche Health Big Data
- Richiesta da parte dei titolari dei dati di certificare ISO/IEC 27001 la piattaforma che li avrebbe gestiti
- Inizialmente piattaforma bare-metal (no cloud)

Perchè Harmony ha richiesto proprio ISO 27001

- In 2016 GDPR entered into force, it applies since 25 May 2018. GDPR is about protecting natural persons with regard to the processing of personal data.
- Genomic data like ones managed in Harmony are personal data (fit in the Art.9 special categories of personal data) and are mostly impossible to be anonymized -> GDPR shall be applied
- Harmony is the Data Controller, INFN-CNAF is the Data Processor
  - *"Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller" (GDPR Art. 24 – Responsibility of the controller)*
  - *"…the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation…"* (GDPR Art. 28 - Processor)
  - *Adherence to […] an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements* set out in paragraph 1 of this Article" *(GDPR Art.32 – Security of processing)*
- ISO/IEC 27001 is the main certification mechanism compliant with GDPR requirements (Art. 43, 58, 63)

From the Controller side (Harmony), the fact that CNAF is ISO certified is a way to demonstrate that processing is performed in accordance with GDPR

ISO 27017, 27018 e 27701

- Tra il 2017 e 2020 abbiamo ammodernato la piattaforma, migrando verso un'architettura cloud openstack (stesse tecnologie usate in INFN Cloud)
- Rischi specifici per l'Information Security in Cloud -> necessario ampliare la lista dei controlli:
  - ISO 27017 Code of practice for information security controls for cloud services
  - ISO 27018 Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
- *Se offri servizi cloud e vuoi essere ISO 27001 compliant devi aggiungere i controlli secondo le linee guida 27017 (cloud) e 27018 (gestione di PII in cloud)*
- *Altro standard interessante nella famiglia 27k è ISO 27701 (PIMS Personal Information Management System) – non ancora adottato al CNAF.*

EPIC Cloud

- The new ISO certified cloud platform has been named EPIC Cloud (Enhanced PrIvacy and Compliance).
  - Link to the certificate
- EPIC Cloud offers an IaaS Community Cloud* for the community of
  - biomedical and genomic researchers
  - Industrial researchers
- EPIC Cloud is based on the same technologies of INFN Cloud with various enhancements introduced to meet higher security and privacy standards. For example:
  - The IAM provides 2FA, integration with web services, SSH and VPN (OpenVPN)
  - OneData has more auditing functionalities
  - Network segregation between OpenStack tenants is guarantee by ACLs
  - Standard shared responsibility model:
    - User manages data, applications, runtime, middleware and OS
    - CNAF manages networking, storage, servers, virtualization
  - Advanced logging and auditing services (centralized syslog managed applying the ***segregation of duties*** principle)

** **Community Cloud: Cloud deployment model** where **cloud services** exclusively support and are shared by a specific collection of **cloud service customers** who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.*
Ref. ISO 17788

Qualche dettaglio sullo standard ISO/IEC 27001

Requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS)

…ma cos'è un ISMS?

(o in italiano SGSI Sistema di Gestione della Sicurezza delle Informazioni)

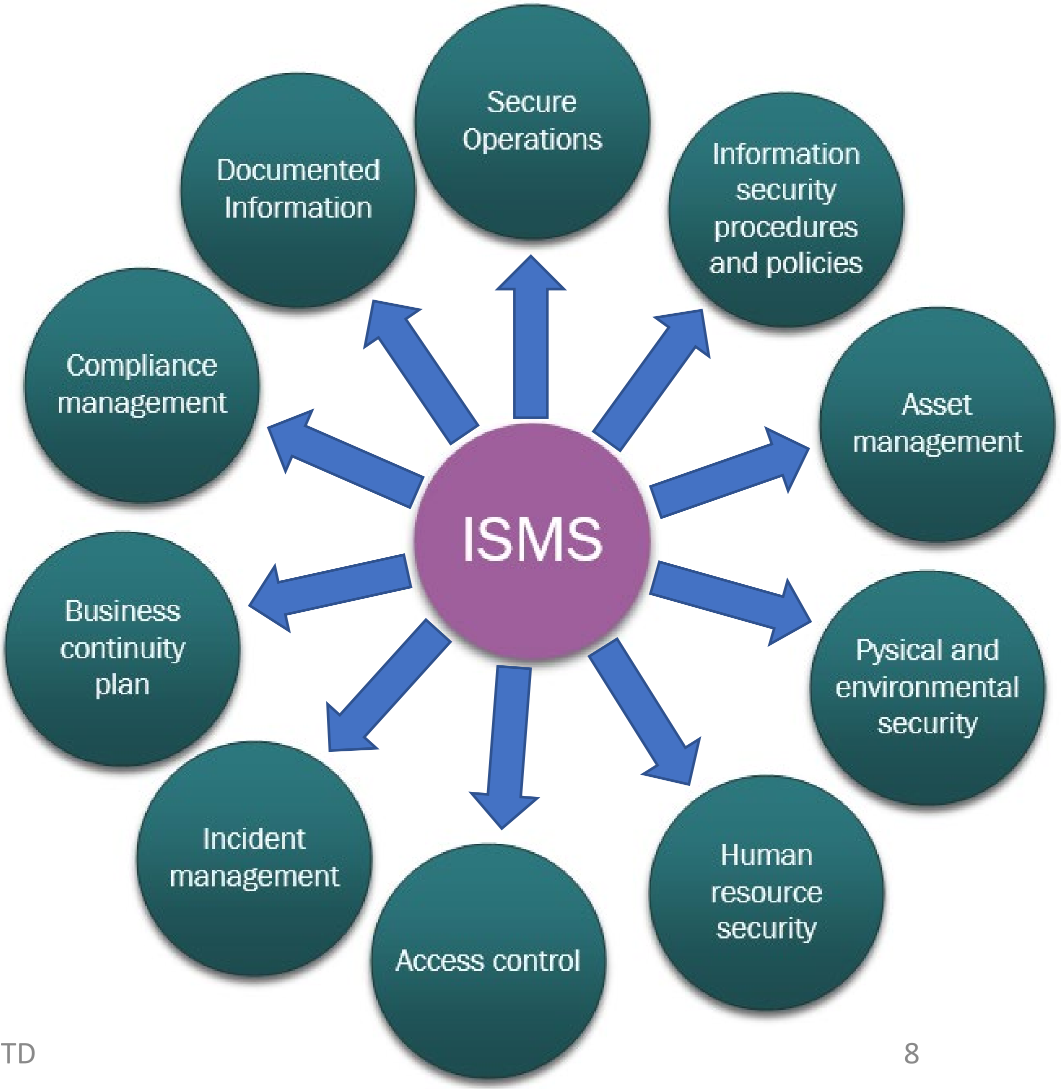
Information Security Management (ISM)

- Information Security Management is about preserving the Confidentiality, Integrity and Availability (CIA) of information and associated information facilities (systems, services, infrastructure or physical locations)
- It ensures business continuity by minimizing business damage by preventing and reducing the impact of security incidents
- Other properties can also be involved, such as authenticity, accountability, non-repudiation and reliability
- The objectives of the ISM are NOT fixed, they depend on the context and are defined by the organization

Componenti di un ISMS

Established standard Project Management techniques applied to Information Security Management:

- It is an organizational framework linking all the elements relevant to the information security, in order to assure that policies, processes and security objectives are implemented, communicated and assessed.
- It needs to continually improve -> **Deming Cycle**
- It is centered to the risk assessment process -> all decisions are based on the output of this process
- Goal: achieving the optimal CIA **balance**, i.e., ensuring Confidentiality of information, while still ensuring the information remains accessible to authorized persons and is not altered



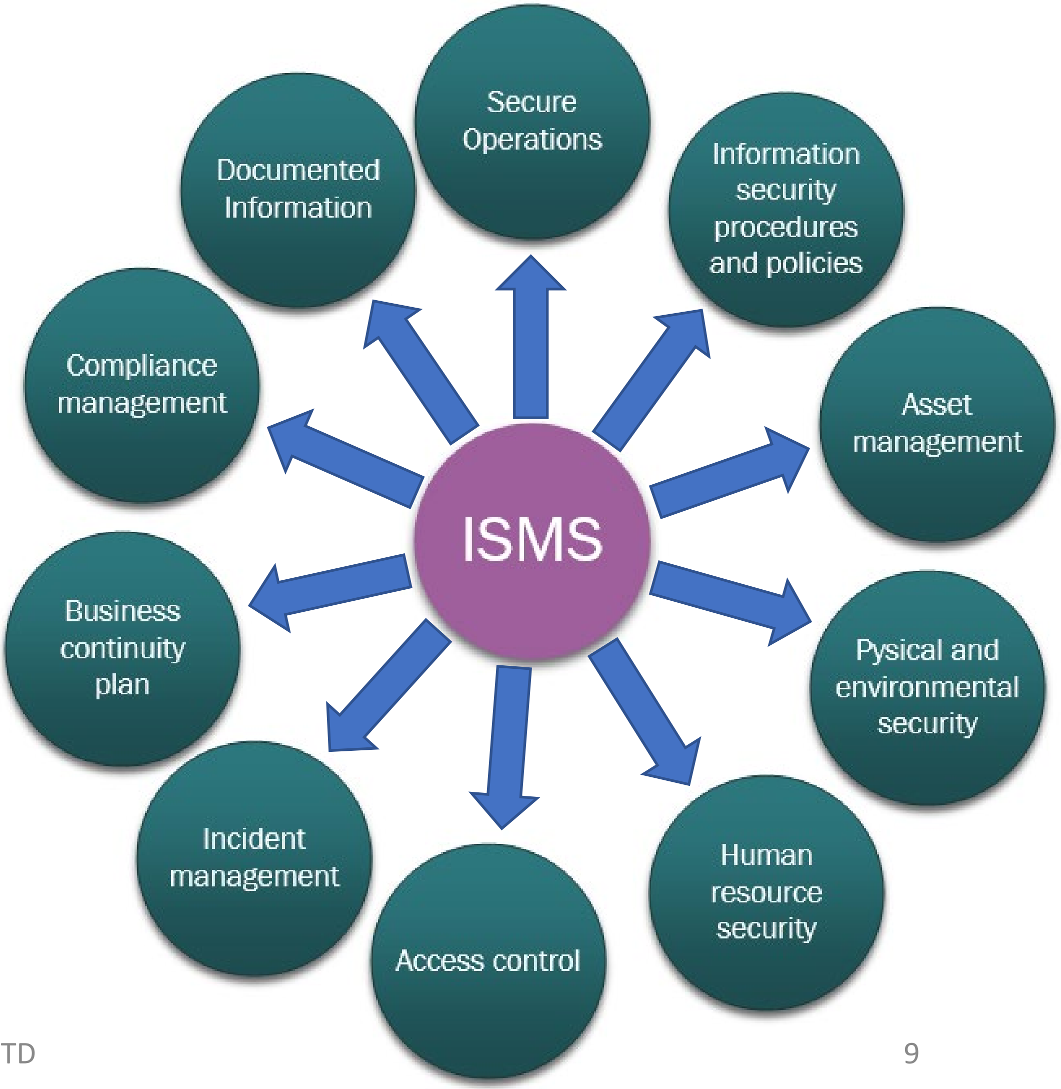
Cosa NON dovrebbe essere un ISMS

(dal materiale del corso ISO 27001 del British Standard Institute)

What it should not be:

The management system should be appropriate to the organization and should NOT be:

- All about the paper work
- Box ticking activities
- Simply about compliance with the standard
- A straight jacket that stops change



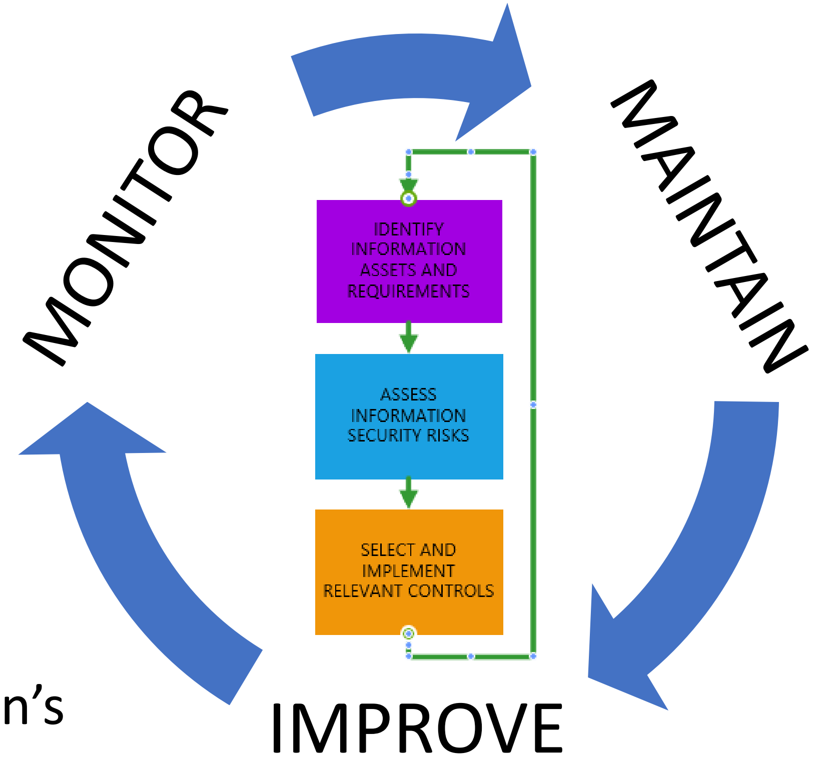
Passi da fare per implementare un ISMS

ISO 27001 adopts a process-based approach.

- identify information assets and their associated information security requirements
- assess information security risks and treat information security risks
- select and implement relevant Controls to manage unacceptable risks
- monitor, maintain and improve the effectiveness of controls associated with the organization’s information assets

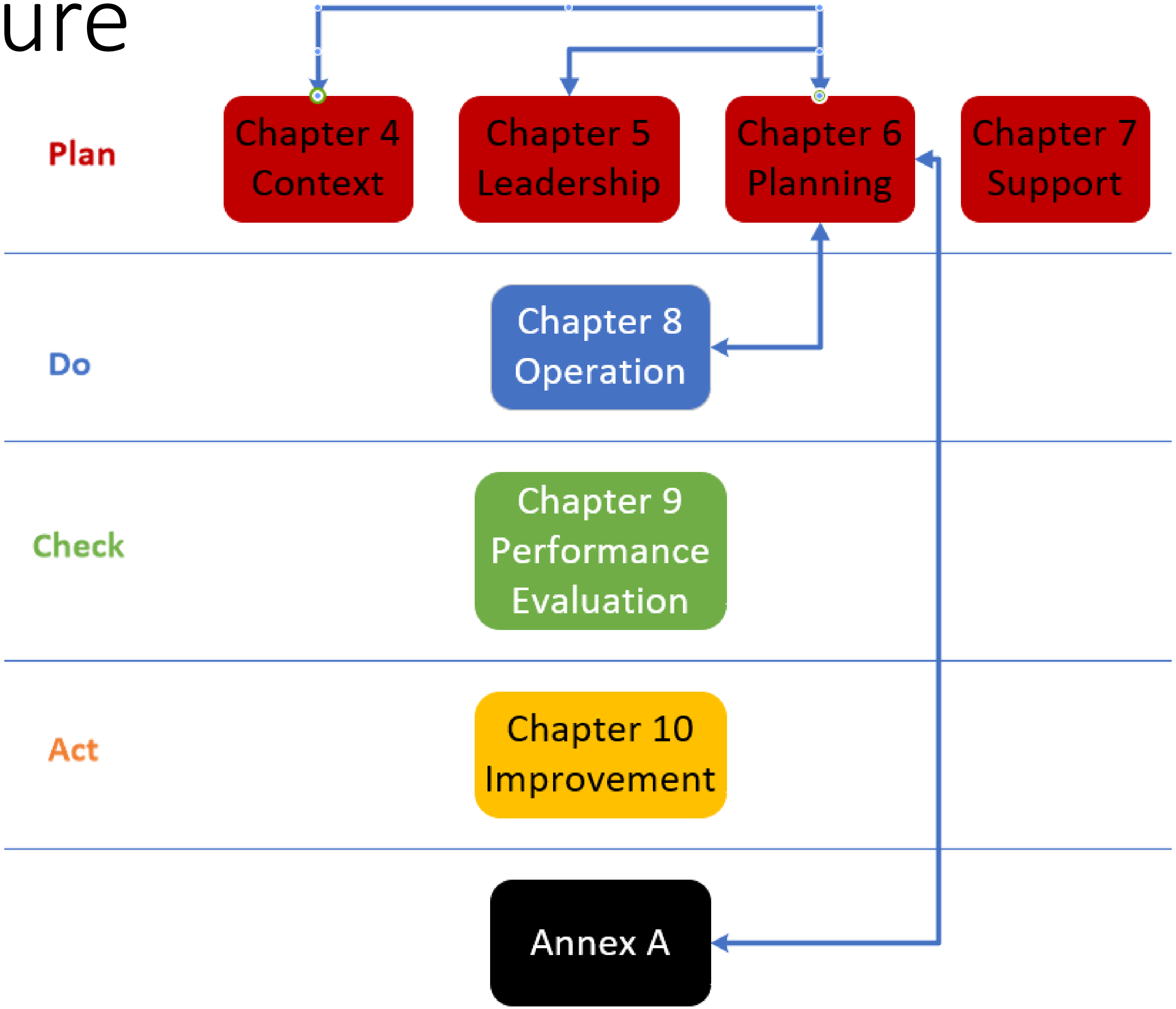
To ensure the ISMS is effectively protecting the organization’s information assets on an ongoing basis, it is necessary that steps be continually repeated to identify changes in risks or in the organization’s strategies or business objectives.

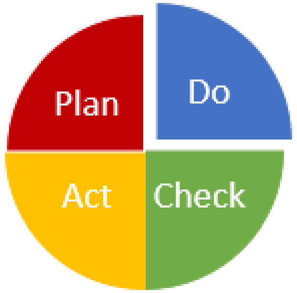
Ref. ISO 27000


MONITOR
MAINTAIN
IDENTIFY INFORMATION ASSETS AND REQUIREMENTS
ASSESS INFORMATION SECURITY RISKS
SELECT AND IMPLEMENT RELEVANT CONTROLS
IMPROVE

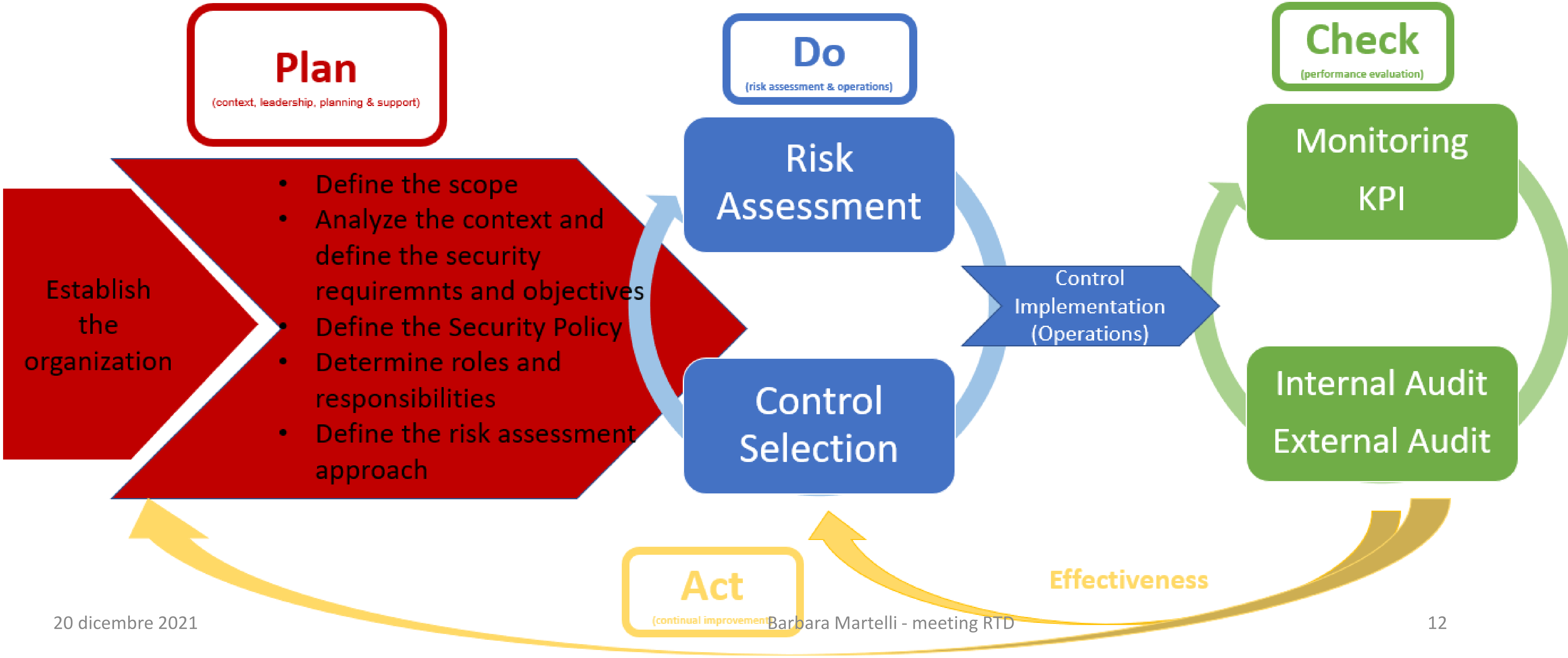
The ISO 27001 structure

- ISO 27001 composed by
  - 10 Clauses
  - Annex A (normative)
    - Control Objective: statement describing what is to be achieved as a result of implementing controls
    - Control: measure that is modifying risk
  - Applies the PDCA cycle
- Nonconformity: non-fulfilment of a requirement
- Corrective Action: action to eliminate the cause of a nonconformity and to prevent recurrence





Deming Cycle and Risk Assessment



Plan
(context, leadership, planning & support)

Establish the organization

- Define the scope
- Analyze the context and define the security requiremnts and objectives
- Define the Security Policy
- Determine roles and responsibilities
- Define the risk assessment approach

Do
(risk assessment & operations)

Risk Assessment

Control Selection

Control Implementation (Operations)

Check
(performance evaluation)

Monitoring

KPI

Internal Audit

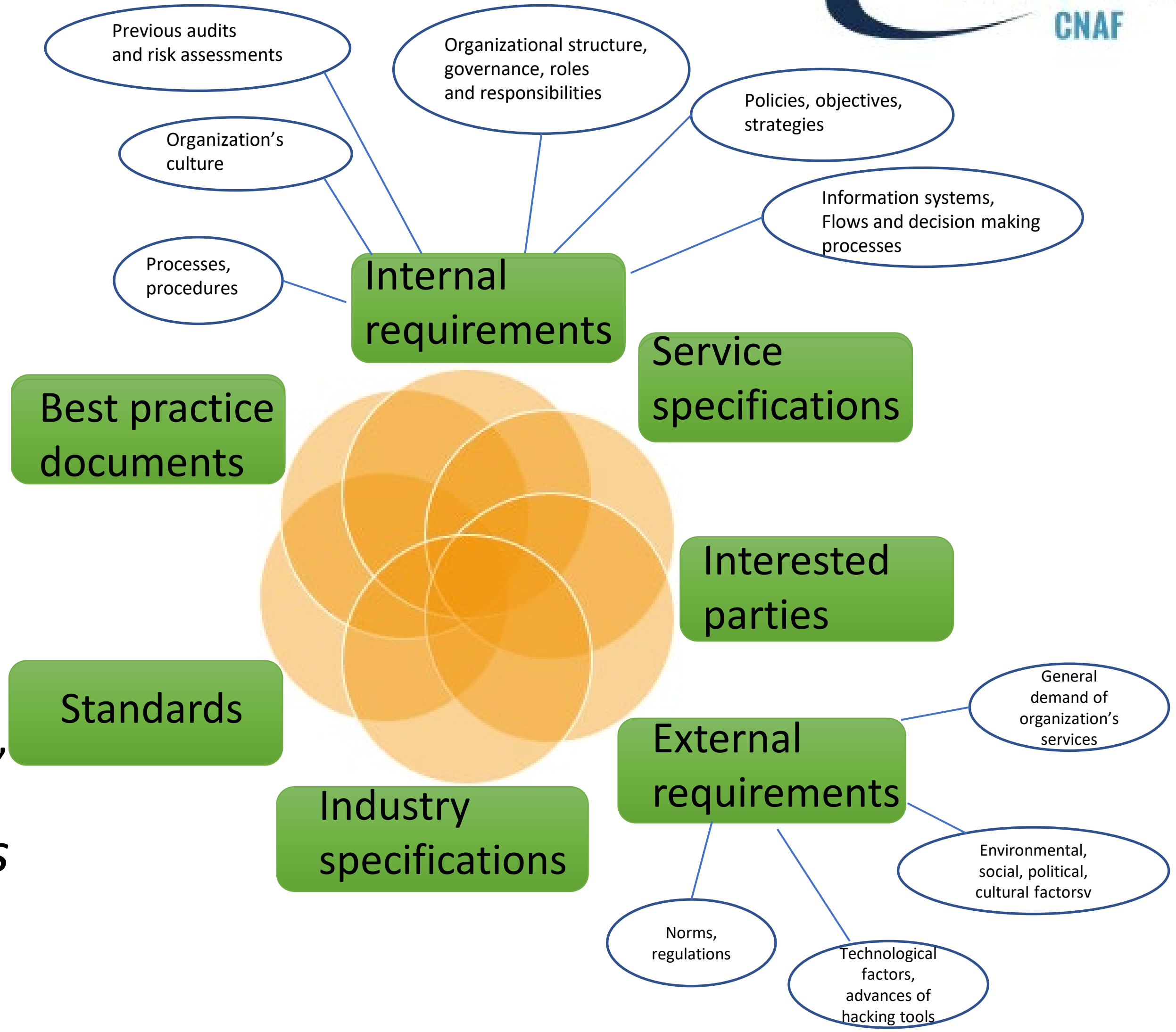
External Audit

Effectiveness

Act
(continual improvement

Analyze the context and define the security requirements

- Identify stakeholders and their expectations
- Identify information security requirements
- Define and communicate the information security policy
- Define information security objectives (they should be SMART: Specific, Measurable, Achiveable, Relevant, Time-bound)
  - E.g: *implement 2FA on all accounts by the end of the year*



Internal requirements

Previous audits and risk assessments

Organizational structure, governance, roles and responsibilities

Policies, objectives, strategies

Organization's culture

Information systems, Flows and decision making processes

Processes, procedures

Service specifications

Best practice documents

Interested parties

Standards

External requirements

General demand of organization's services

Environmental, social, political, cultural factorsv

Norms, regulations

Technological factors, advances of hacking tools

Industry specifications

Plan

Define roles and responsibilities

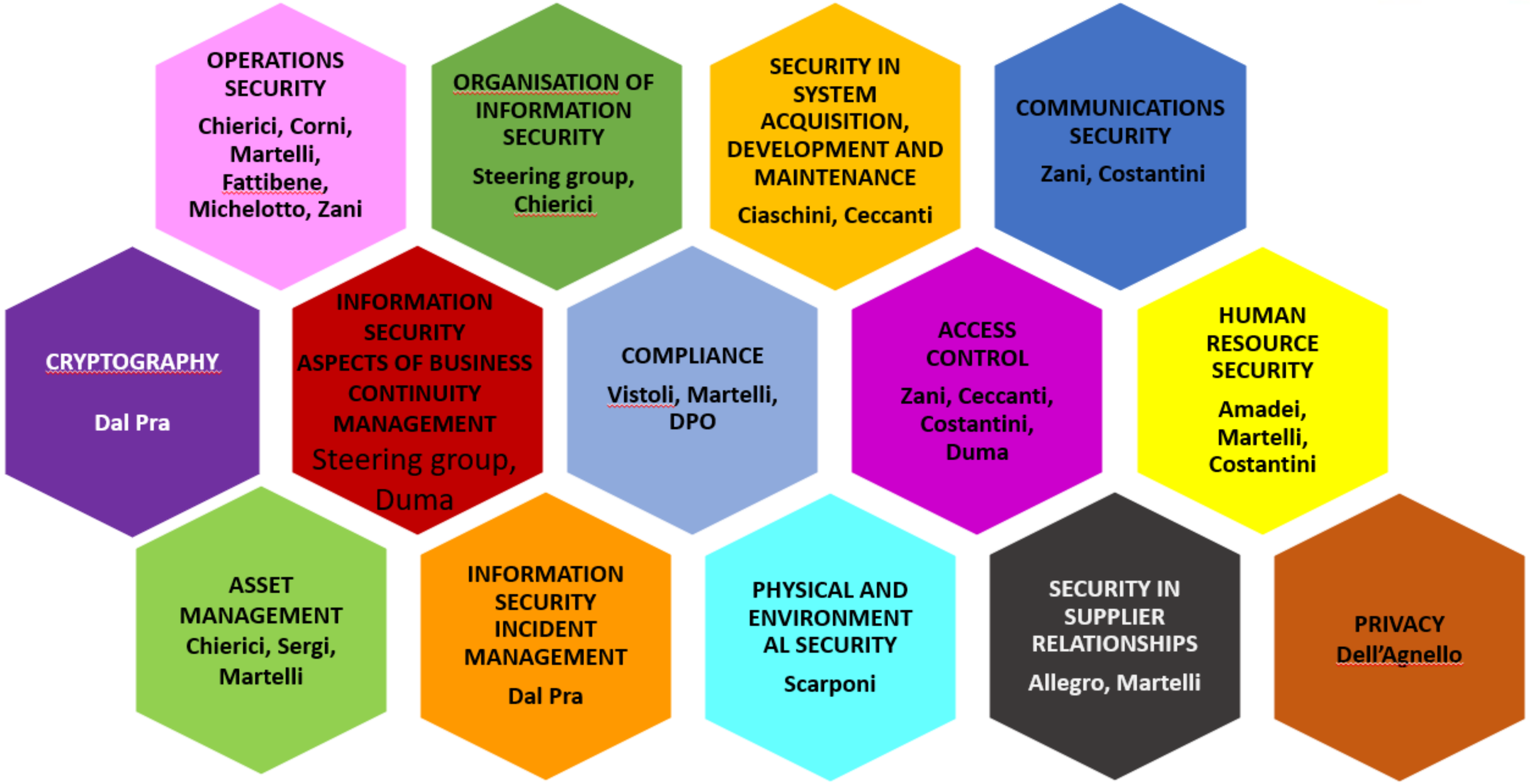
- It is mandatory to define and assign roles authorities, responsibilities and accountabilities for relevant roles with respect to risk management and information security
- Responsibilities and authorities need to be assigned to:
  - Ensure conformance to ISO 27001
  - Reporting on ISMS performance

Plan

Defined roles and responsibilities at CNAF

- **Steering Group (dell’Agnello, Vistoli, Salomoni, Cesini, Martelli)**
    - Has the authority to allocate material and human resources in order to reach the security objectives
    - Is responsible of the maintainance of information security, also in adverse situations (incidents, disasters, crises)
- **ISMS Manager (Martelli)**
    - Is responsible for estabilishing, implement, maintain and improve the ISMS and reach the security objectives
    - Coordinates the processes of risk assessment, internal audit, security incident management
- **Security Group (Ciaschini, Chierici, Zani, Duma, Fattibene, Martelli, Longo, Scarponi)**Is responsible for the conformance of the ISMS to the ISO 27001 standard, norms and regulations
    - Approves all documents defining or modifying Security Requirements
- **Security Coordinator (Ciaschini)**
    - Coordinates the Security Group and the Risk Analysis process
- **Control Objectives Responsibles**: are responsible of the definition and implementation of the Security Controls (Annex A of the ISO 27001 standard)

Annex A Control Objectives



OPERATIONS SECURITY
Chierici, Corni, Martelli, Fattibene, Michelotto, Zani

ORGANISATION OF INFORMATION SECURITY
Steering group, Chierici

SECURITY IN SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE
Ciaschini, Ceccanti

COMMUNICATIONS SECURITY
Zani, Costantini

CRYPTOGRAPHY
Dal Pra

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
Steering group, Duma

COMPLIANCE
Vistoli, Martelli, DPO

ACCESS CONTROL
Zani, Ceccanti, Costantini, Duma

HUMAN RESOURCE SECURITY
Amadei, Martelli, Costantini

ASSET MANAGEMENT
Chierici, Sergi, Martelli

INFORMATION SECURITY INCIDENT MANAGEMENT
Dal Pra

PHYSICAL AND ENVIRONMENT AL SECURITY
Scarponi

SECURITY IN SUPPLIER RELATIONSHIPS
Allegro, Martelli

PRIVACY
Dell’Agnello

ISO 31000 the standard for risk management

- ISO 31000 guidelines provides a common approach to managing any type of risk and is not industry or sector specific.
- The guideline can be used throughout the life of the organization and can be applied to any activity, including decision making at all levels.

BS ISO 31000:2018

BSI Standards Publication

PD ISO Guide 73:2009

delines

BSI Standards Publication

BS EN IEC 31010:2019

Risk management —
Vocabulary

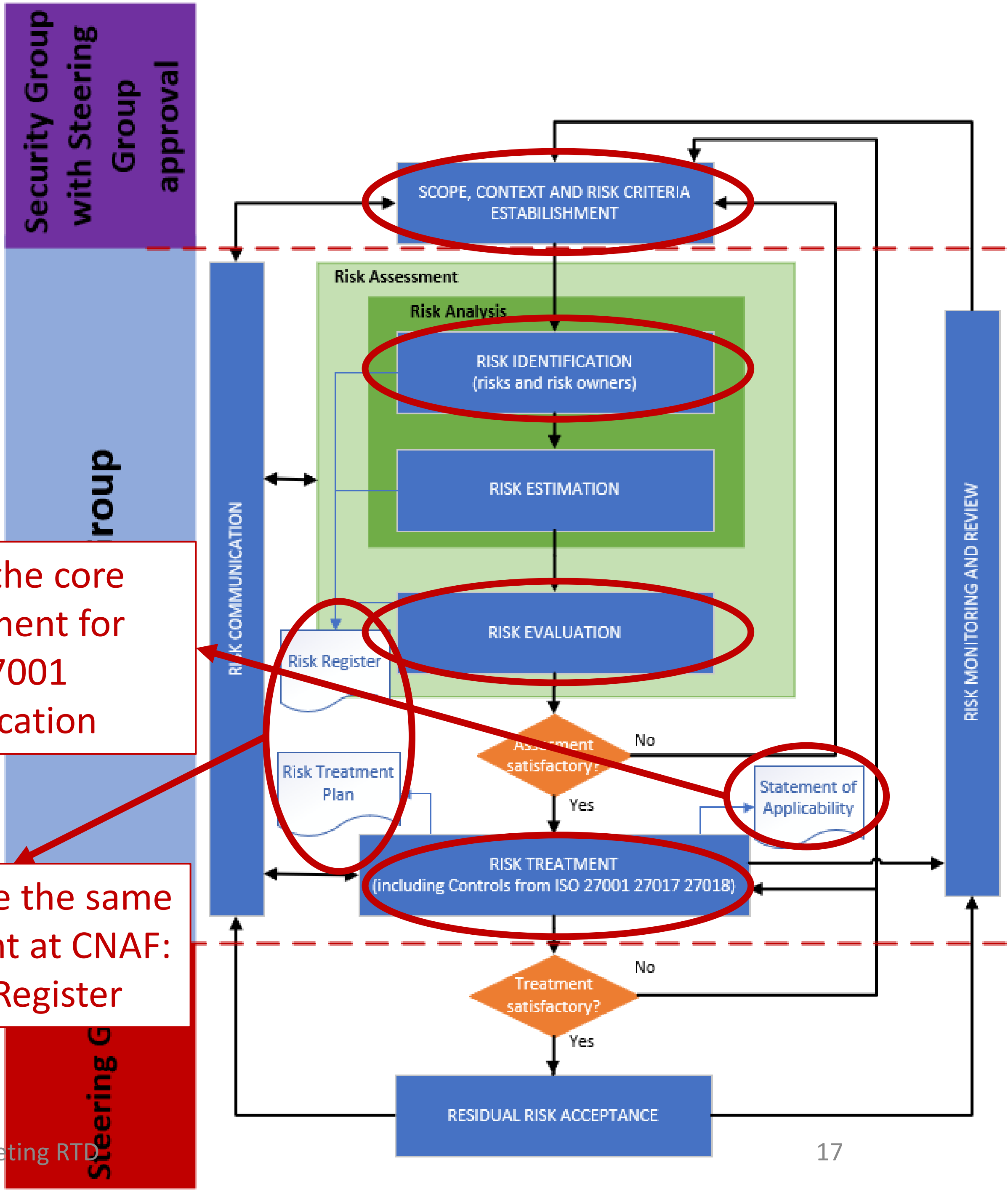
BSI Standards Publication

Risk management – Risk assessment
techniques (IEC 31010:2019)

ISO 31000 available read-only for free here:
https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Risk Management Process in EPIC

- Inspired by:
  - ISO 27005 guideline with modifications
    - we don't start with asset identification, but we use a scenario-based risk assessment
  - and ISO 31000
- Iterative process aimed at supporting the decision-making process
- In EPIC is performed once a month and whenever a relevant change in the system occurs
  - ISO 27001 clause 8.2 requires to perform it *"at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). "*
- Established criteria to define Risk Owners (person or entity with the accountability ar authority to manage a risk), one per Annex section)



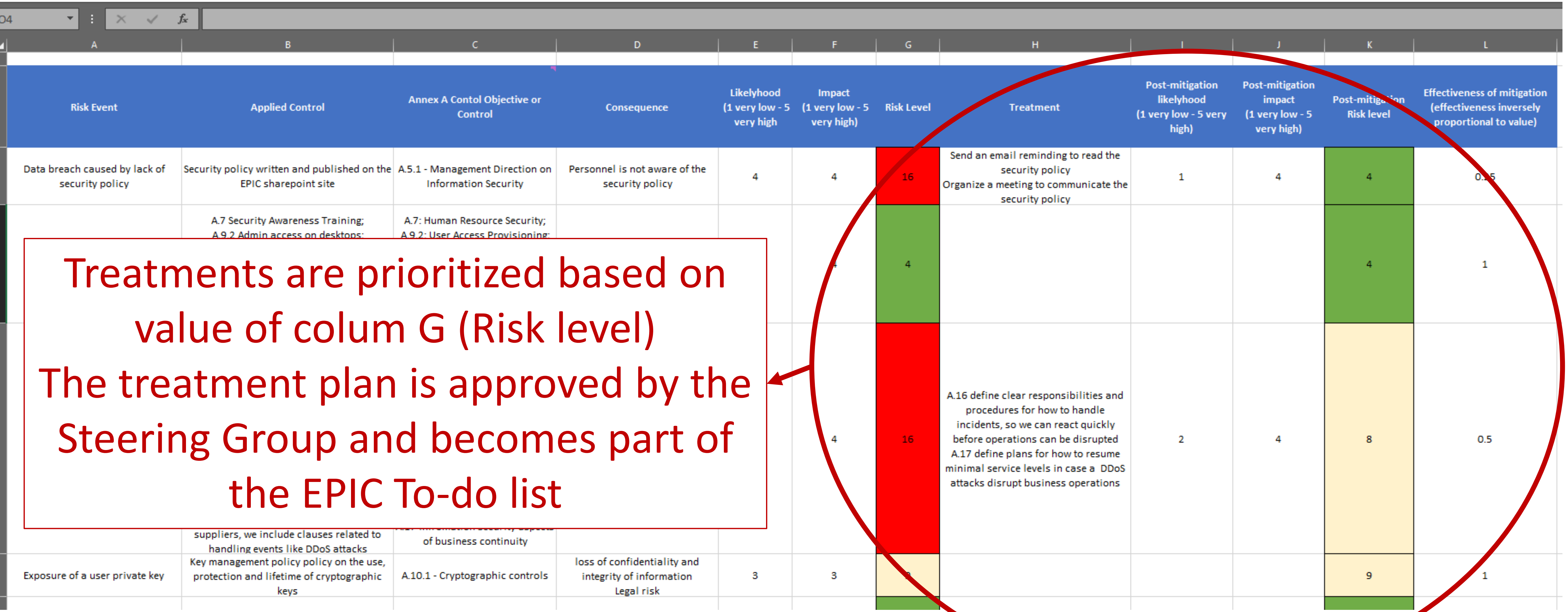
Security Group with Steering Group approval
roup
Steering G
SCOPE, CONTEXT AND RISK CRITERIA ESTABILISHMENT
RISK COMMUNICATION
Risk Assessment
Risk Analysis
RISK IDENTIFICATION (risks and risk owners)
RISK ESTIMATION
RISK EVALUATION
Risk Register
Risk Treatment Plan
Assessment satisfactory?
No
Yes
Statement of Applicability
RISK TREATMENT (including Controls from ISO 27001 27017 27018)
Treatment satisfactory?
No
Yes
RESIDUAL RISK ACCEPTANCE
RISK MONITORING AND REVIEW

SOA: the core document for ISO 27001 certification

These are the same document at CNAF: the Risk Register

Plan

EPIC Risk Register is also our Risk Treatment Plan



Risk Event	Applied Control	Annex A Contol Objective or Control	Consequence	Likelyhood (1 very low - 5 very high	Impact (1 very low - 5 very high)	Risk Level	Treatment	Post-mitigation likelyhood (1 very low - 5 very high)	Post-mitigation impact (1 very low - 5 very high)	Post-mitigation Risk level	Effectiveness of mitigation (effectiveness inversely proportional to value)
Data breach caused by lack of security policy	Security policy written and published on the EPIC sharepoint site	A.5.1 - Management Direction on Information Security	Personnel is not aware of the security policy	4	4	16	Send an email reminding to read the security policy Organize a meeting to communicate the security policy	1	4	4	0.25

	A.7 Security Awareness Training;
	A.9.2 Admin access on desktops;
		A.7: Human Resource Security;
		A.9.2: User Access Provisioning;
					4	4				4	1

	suppliers, we include clauses related to handling events like DDoS attacks	of business continuity			4	16	A.16 define clear responsibilities and procedures for how to handle incidents, so we can react quickly before operations can be disrupted A.17 define plans for how to resume minimal service levels in case a DDoS attacks disrupt business operations	2	4	8	0.5
Exposure of a user private key	Key management policy policy on the use, protection and lifetime of cryptographic keys	A.10.1 - Cryptographic controls	loss of confidentiality and integrity of information Legal risk	3	3	9				9	1

Treatments are prioritized based on value of colum G (Risk level)

The treatment plan is approved by the Steering Group and becomes part of the EPIC To-do list

EPIC SoA

All Controls from

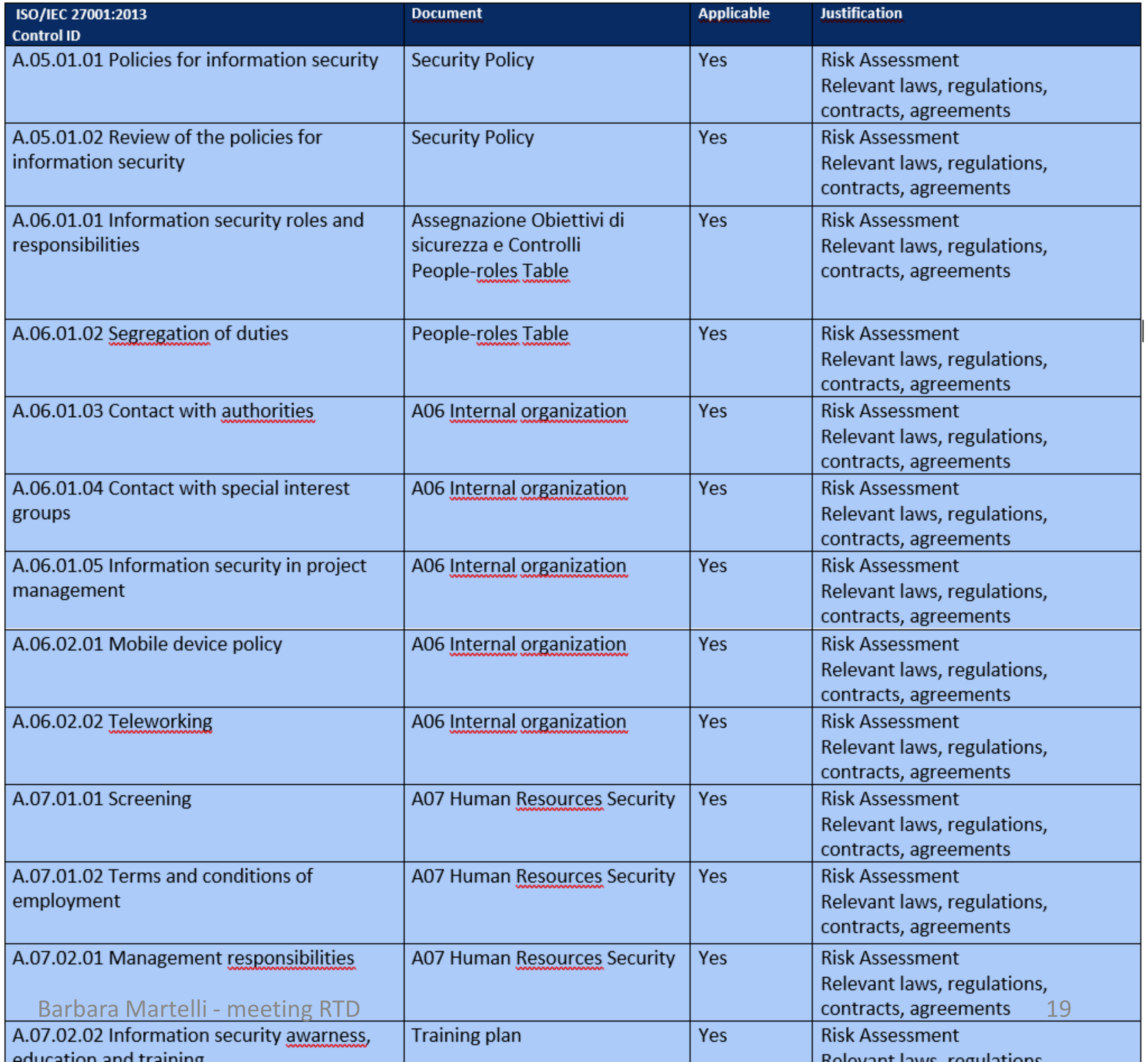
- ISO 27001 (114 controls)
- ISO 27017 (37 controls)
- ISO 27018 (25 controls)

are defined and applicable

SoA Metrics:

- Level of implementation of each applicable Control (fully, largerly, partially, poorly implemented)
- Whole implementation status (sum of Controls implementation levels)

Table 1 Defined controls from ISO/IEC 27001 27017 27018



ISO/IEC 27001:2013 Control ID	Document	Applicable	Justification
A.05.01.01 Policies for information security	Security Policy	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.05.01.02 Review of the policies for information security	Security Policy	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.01.01 Information security roles and responsibilities	Assegnazione Obiettivi di sicurezza e Controlli People-roles Table	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.01.02 Segregation of duties	People-roles Table	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.01.03 Contact with authorities	A06 Internal organization	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.01.04 Contact with special interest groups	A06 Internal organization	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.01.05 Information security in project management	A06 Internal organization	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.02.01 Mobile device policy	A06 Internal organization	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.06.02.02 Teleworking	A06 Internal organization	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.07.01.01 Screening	A07 Human Resources Security	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.07.01.02 Terms and conditions of employment	A07 Human Resources Security	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.07.02.01 Management responsibilities	A07 Human Resources Security	Yes	Risk Assessment Relevant laws, regulations, contracts, agreements
A.07.02.02 Information security awarness, education and training	Training plan	Yes	Risk Assessment Relevant laws, regulations

Do

Performance Evaluation (Clause 9)

- Requirement: evaluate (and document) the ISMS
  - Performance
  - Effectiveness
- Evaluation and monitoring tools
  - Key Performance Indicators (KPI) e.g., systems availability, incident statistics, level of maturity with respect to best practices like ISO 15504 (ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and related Technology), CMMI (Capability Maturity Model Integration), Italian Cyber Security Framework - La Sapienza)
  - Internal audits (at planned intervals, at least once a year)
  - External audits (at planned intervals, at least once a year)
  - Management reviews (at planned intervals, at least once a year)

Check

Performance Evaluation in EPIC

- Management Reviews 4 times a year
  - Identifies improvement areas
  - Review of incident reports, open tasks, nonconformities, corrective actions, monitoring and measurement results
  - Sets Security Objectives and monitors their achievements
- Internal Audit once a year
  - Internal audit plan
  - conducted by an INFN colleague (external to CNAF), with "ISO 27001 lead auditor" certification
  - Identifies and documents nonconformities and opportunities for improvement
- External Audit once a year
  - for the next 3 years will be conducted by KIWA
  - Identifies and document nonconformities and opportunities for improvement
- Some KPIs:
  - Effectiveness of risk treatment (post-mitigation-risk-level/previous-risk-level)
  - Degree of implementation of SoA controls
  - Number, severity and impact of security incidents
  - Availability of systems

Check

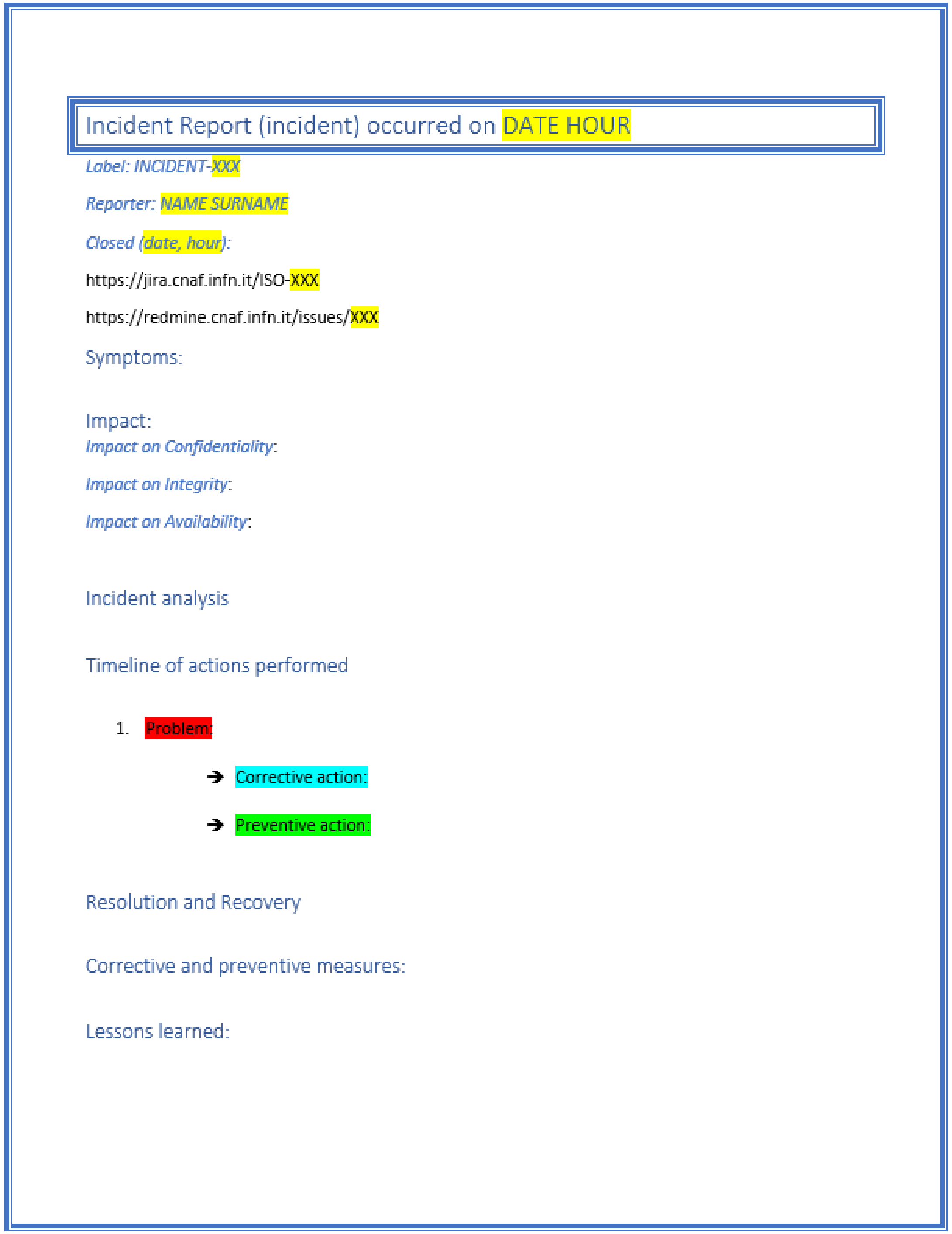
Improvement (Clause 10)

- When a nonconformity occurs ISO 27001 requires to:
  - Correct it (corrective action)
  - Deal with consequences
  - Evaluate to remove the causes of nonconformity (root-cause analysis)
    - Determine if there are similar nonconformities or if they could occur
  - Implement corrective actions
  - Review the effectiveness of corrective actions
  - Change the ISMS if necessary
- It is required to continually improve the effectiveness of the ISMS

Act

Improvement in EPIC

- Nonconformities are tracked in Jira and labeled “NC”
  - Corrective actions are recorded in the comments of the Jira tasks
- Information Security Incidents are tracked in Jira and labelled “incident”
  - An incident report is written including impact on CIA root cause analysis, corrective actions, preventive actions, timeline for recovery, lessons learned
- Incidents and non conformities are reviewed 4 times a year for improvement



Incident Report (incident) occurred on DATE HOUR

Label: INCIDENT-XXX

Reporter: NAME SURNAME

Closed (date, hour):

https://jira.cnaf.infn.it/ISO-XXX

https://redmine.cnaf.infn.it/issues/XXX

Symptoms:

Impact:
Impact on Confidentiality:

Impact on Integrity:

Impact on Availability:

Incident analysis

Timeline of actions performed

1. Problem:
   - → Corrective action:
   - → Preventive action:

Resolution and Recovery

Corrective and preventive measures:

Lessons learned:

Required documented information

A.5.1.1 Information security policy

A.15.1.1 Information Security policy for supplier Relationships

8.1 evidence operational planning and control

9.2 evidence of audit programme and results

A.14.2.1 Secure development policy

A.11.2.9 Clean desk clean screen policy

4.3 Scope

6.1.3 risk treatment process

A.11 Physical and environmental security Policy

A.12.2.1 Controls against malware policy

9.3 evidence of results of management reviews

8.2 risk assessment results

A.12.3.1 Backup Policy and procedures

5.3 Organization chart

A.6.2.1 Mobile device policy

A.8.1.3 Acceptable use of asset policy

A.16.1.4 Assessment of and decision on information security events Policy

A.9.3 Password Policy

A.12.6.2 Restrictions on software installation

A.6.2.2 Teleworking policy

A.8.2.1 Information Classification policy

7.2 evidence of competence

A.17.2 Redundancies Policy

8.3 SoA

A.13.2.1 Information transfer policy and procedures

6.1.2 risk assessment process

10.1 actions resulting from nonconformities and corrective actions

A.9.1.1 Access Control Policy

A.10.1.1 Cryptographic control policy

A8 Asset Management policy

6.2 security objectives

A.10.1.2 Key Management policy

9.1 evidence of monitoring and measurement results

A.14.1 Information Security requirements analysis and specification

Prospettive di utilizzo di EPIC Cloud

- Tre aspetti:
  - Infrastruttura cloud ad alta sicurezza - certificata
    - Progetti di ricerca in campo digital health -> gestione dati personali
    - Progetti di ricerca in collaborazione con aziende o attività TT -> gestione dati confidenziali
  - Infrastruttura cloud gestita secondo linee guida 27001 27017 27018 – NON certificata
    - Qualsiasi progetto che necessiti di risorse cloud esprima requisiti precisi di data availability, integrity
  - Utilizzo delle misure organizzative ISO 27001 in infrastrutture diverse dal cloud – NON certificata e NON cloud
    - Qualsiasi ambito in cui ci siano requisiti di confidenzialità, disponiblità e integrità dei dati da garantire

Sommario e considerazioni finali

- La sicurezza delle informazioni non è ottenibile con sole misure tecniche, sono necessarie anche misure organizzative (ormai richieste da tutti i framework nazionali ed europei)
- ISO 27001 propone una lista best practice accettate a livello internazionale per gestire un SGSI attraverso un approccio basato sui processi e sull'applicazione di metodologie di project management consolidate
- Il fulcro del Sistema di Gestione è il processo di analisi e valutazione dei rischi
- Si punta al miglioramento continuo iterando i processi di Information Security su base annuale
- I requisiti sono un input del sistema: non sono fissati a priori nello standard
  - La Disponibilità è un aspetto chiave dell'Information Security, un SGSI può essere utile anche se non si devono rispettare requisiti di confidenzialità
- La certificazione è necessaria per dimostrare agli stakeholder l'adozione dello standard, è possibile adottarlo anche senza certificarsi

Risorse aggiuntive

- Per la presentazione completa su EPIC Cloud:
  - «CERN Computing Seminar: the ISO/IEC 27001 Information Security Management System at CNAF» https://indico.cern.ch/event/1074445/
- ENISA Threat Landscape 2020 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats
- ENISA Cloud Computing Risks https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
- ENISA On-line tool for the security of personal data processing https://www.enisa.europa.eu/risk-level-tool/risk

Backup slides

Balancing freedom of research and information security

- Combine the ISO 27k model with agile values
  - client collaboration over contract negotiation -> but we need to have clear shared responsibilities between “customer” and provider -> strict collaboration with users, daily communications, co-design of solutions, but the shared responsibility model is strictly applied
  - Working software over comprehensive documentation -> but we need to document very clearly our environment -> documentation as a code, software repository (GitLab), configuration management with Puppet
  - Individuals and interactions over processes and tools -> but we need processes, policies and procedures -> more policies/less procedures, Jira is used to support an agile project management style
  - Responding to change over following a plan -> but we need to plan (plan do check act) -> change management process