Piattaforme distribuite certificate: sicurezza e conformità per la gestione dei dati sensibili

Barbara Martelli

on behalf of DataCloud team

EPIC
Enhanced PrIvacy and Compliance Cloud

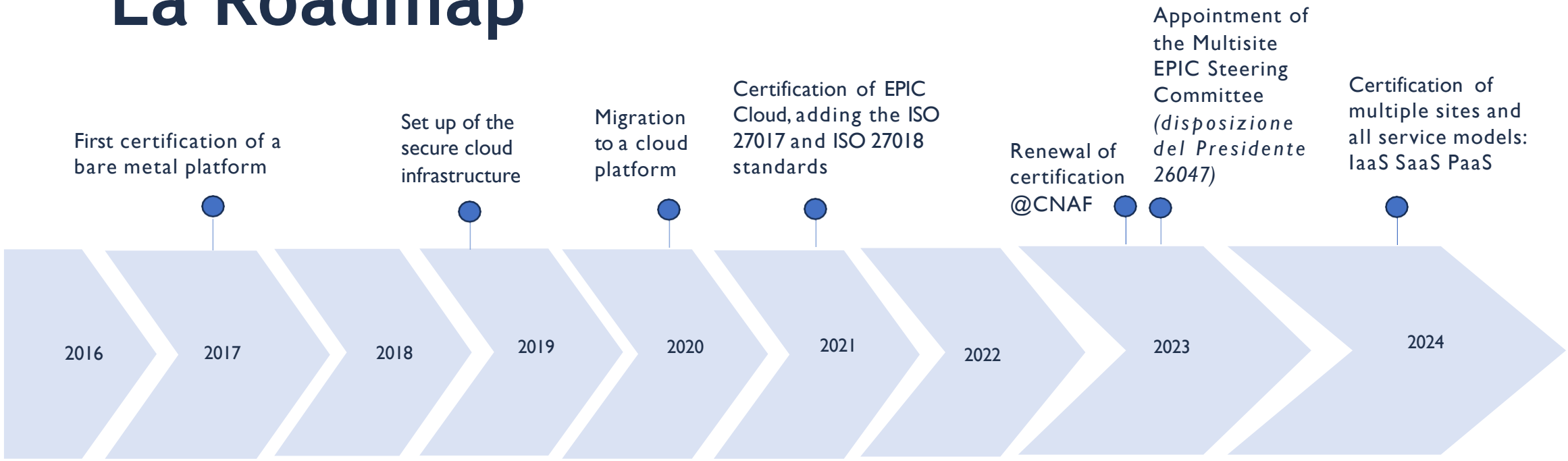
Enhanced PrIvacy and Compliance Cloud is an ISO certified cloud platform	A region of INFN Cloud with a certified Information Security Management System
EPIC Cloud offers an IaaS Community Cloud for the research communities	Biomedical and genomic researchers Industrial researchers

Site locations: Bologna (active now), Bari and Catania sites will be added in October 2024 enabling for high availability and disaster recovery

Resource available today: about 1.5PB of HDD, 600 TB SSD, 1440 cores, 10 TB RAM, 6 GPU A100

On going expansion with 3.2M euro of NRRP resources and ~10M euro of funds from other projects

La Roadmap



- In 2017 we started with a bare-metal that was ISO-27001 certified infrastructure
- In 2019 we moved to a Cloud-based infrastructure
- In 2021 we added the cloud certifications ISO-27017 and ISO-27018 and EPIC Cloud was born
- In 2024 we are going to add multiple sites and certify IaaS, SaaS and PaaS

Lo scope del nuovo certificato

Coprogettazione, sviluppo e manutenzione di soluzioni software di DataCloud per il settore della ricerca.

Erogazione di servizi di DataCloud IaaS, SaaS e PaaS in community deployment model.

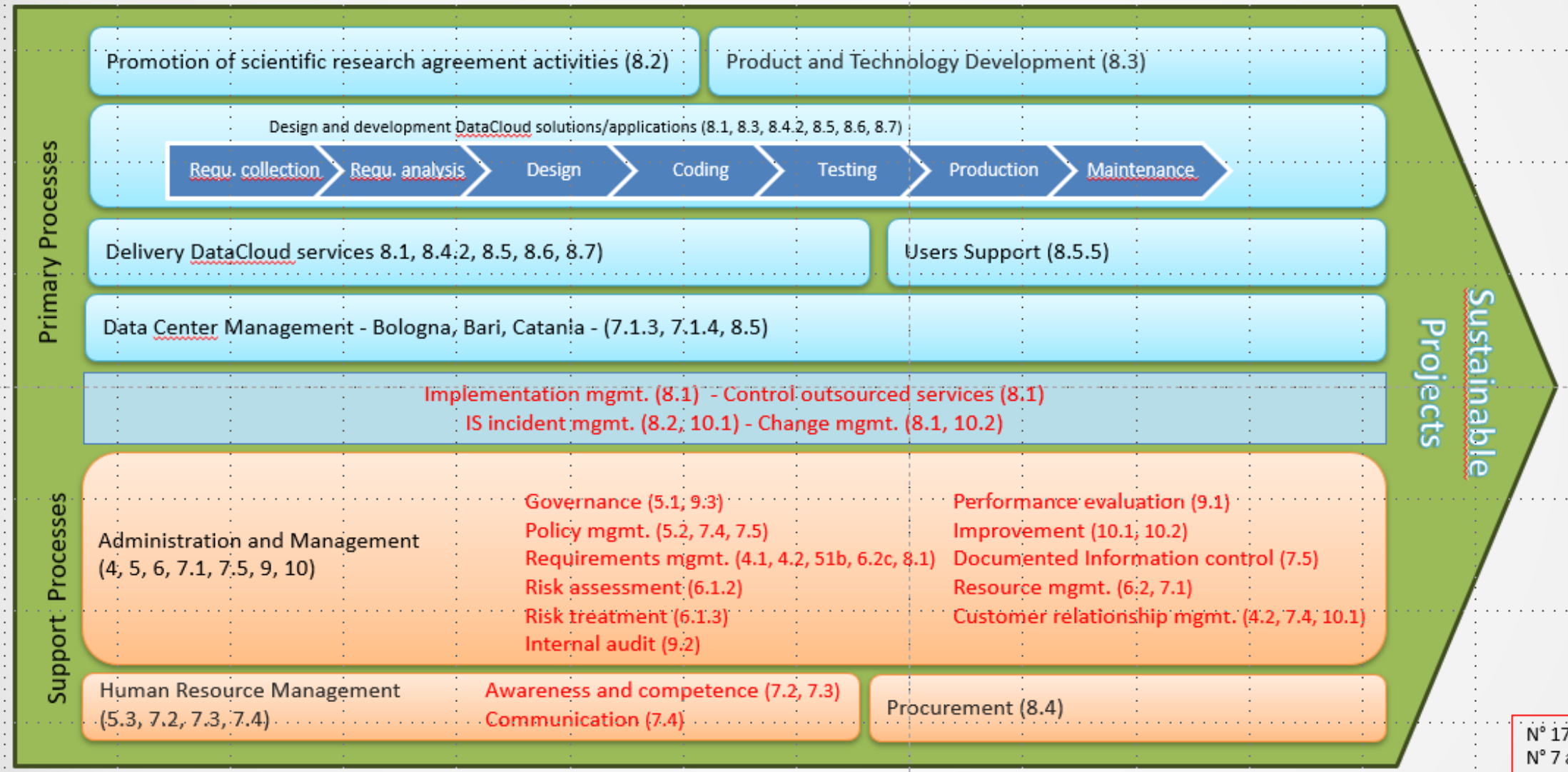
Progetti ospitati su EPIC

Progetto	HW (M€)	FTE
Harmony/Harmony+	Impegno a mantenere attiva la piattaforma anche dopo la fine del progetto	
DARE	3.2 (inseriti in gara TeRABIT)	4 TD CNAF, 1 TD Bari fino a dicembre ’26
ICSC Spoke8	0 (da richiedere a RAC)	1 TD CNAF, 2 TD Catania, 1 borsa Spoke0 dedicata ad attività di S8
HBD	10 (procedure d’acquisto da avviare, spalmati su 7 anni)	7/8 AR senior 7/8 laureandi
Sant’Orsola	0.34 (procedure d’acquisto in fase di avvio)	2 AR senior
AlmaHealthDB	Su risorse DARE e Spoke8	3 persone CINECA (gruppo life science) 3-4 ingegneri IOR-UniBO che collaboreranno con il nostro personale DARE e Spoke8

Percentuale di afferenza variabile in media 10%

Ulteriori dettagli sui progetti (aggiornato a Maggio ’23):
https://agenda.infn.it/event/34683/contributions/197354/attachments/105518/148360/20230523-datacloud-lifescience-v3.pdf

Proces Reference Model



N° 17 Processi ISO27022
N° 7 altri processi

Porter Processes (ISO 9001); IS Processes (ISO27022, ISO27001)

Esempio di scheda processo

Riccardo Rotondo

Communication Process

Riccardo Rotondo

Purpose

Decision makers and other interested parties are adequately informed about information security risks and have a mutual understanding of these risks.

References

- ISO/IEC 27001:2013, 7.4
- ISO/IEC 27003:2017, 9.4.1
- ISO/IEC 27017
- ISO/IEC 27018

KEY Metrics

- Response time
- Adaptability and flexibility
- Accuracy of information
- Reach and engagement
- Consistency and timeliness
- Clarity and understading

Input / Trigger

- From **information security risk assessment process (Carbone):** Documented risks and evaluation of risks in a list of prioritized risks.
- From **information security risk treatment process (Ciaschini)**: Risk treatment and control implementation plan, list with determined controls and control objectives,acceptance of residual risks.
- From **security policy management process (Bovo):** IS policies.
- From **records control process (Magenta):** Appropriate documents and necessary records.
- From **resource management process (Cesini):** reports regarding resource usage for ISMS controls; estimation of necessary resources to operate the ISMS core processes.
- From **requirements management process (Donvito):** Assigned requirements regarding information security.
- From **internal audits (Belluomo) and performance evaluation process (Vistoli)**: Audit and performance reports..
- From **information security incident management process (Peco):** Incident reports.
- From **information security customer relationship management (Pellegrino) process:** Communication plan with customers and reports on information security performance and added value to the customers.

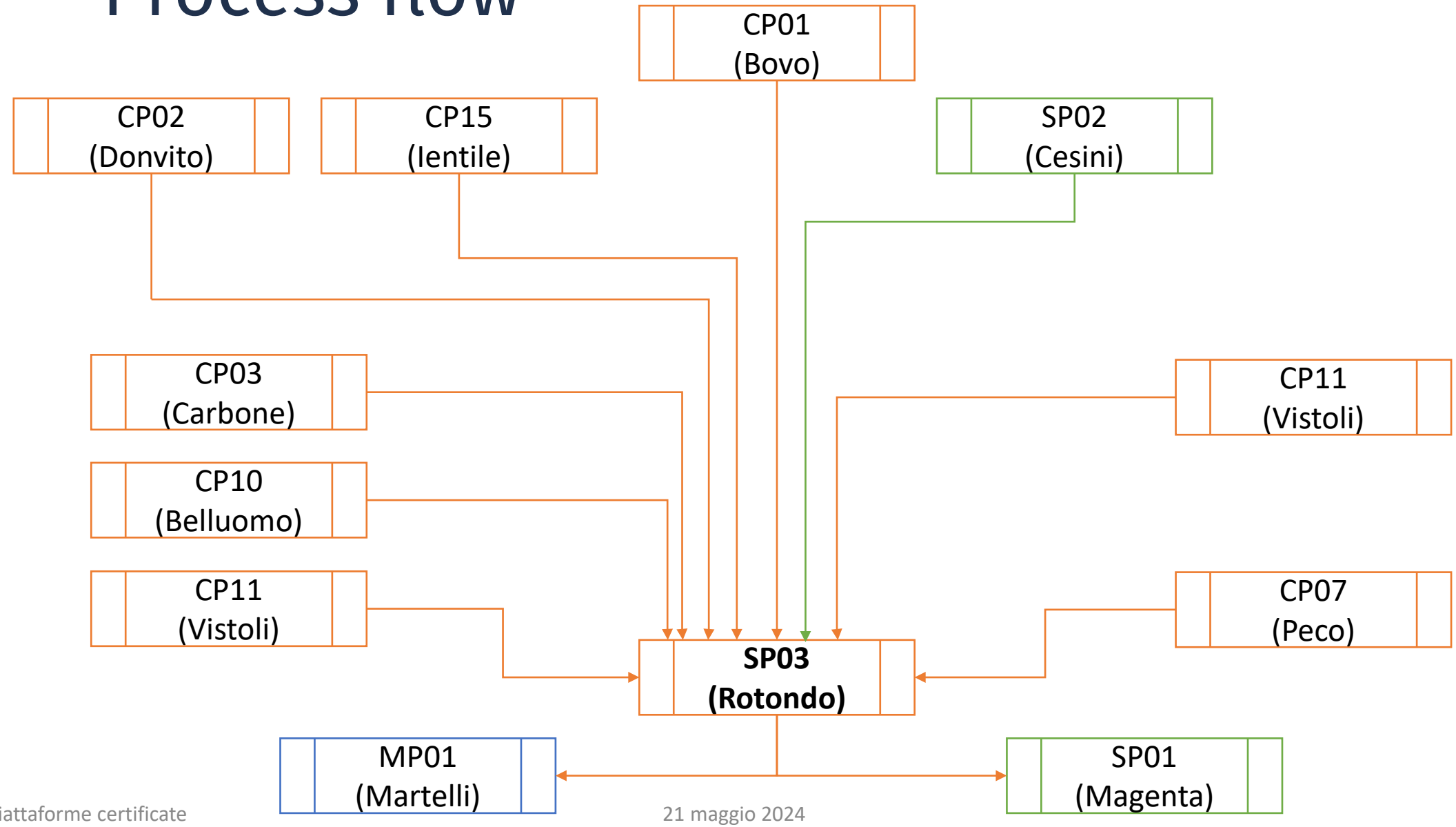
Activities / Functions

- Develop/update risk communication plans for:
  - Normal operation
  - Emergency situation
- Excecute communication plans
- Regularly (at least annual) generate information security managment reports

Results

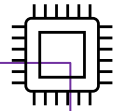
- For **information security governance/management interface process and records control process (Martelli):**
- information security management reports.
- For **records control process (Magenta):**
- communication plan for normal operations and emergency situations;
- information security management reports.

Process flow



Information security governance/management interface process

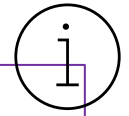
Resources Needed



Hardware

- ……

Information

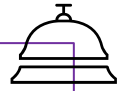


Information created:

- …

Software

Information Managed



Analisi dei Rischi

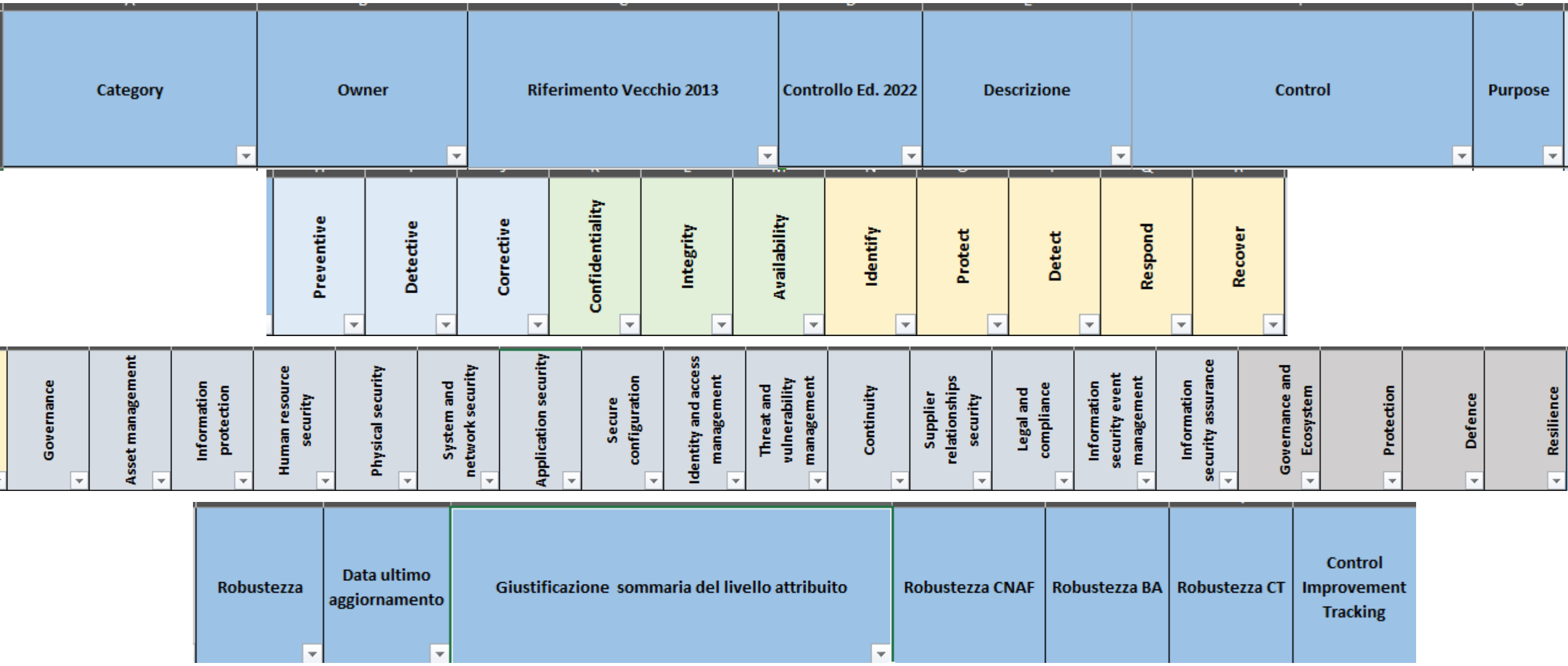
Luca Carbone

Gap Analysis

- 93 controlli di sicurezza nella nuova versione del 2022
- Per ogni controllo, verifica del livello di robustezza della sua implementazione in ogni sito
- Redatto un SoA preliminare

Fragile		Robusto		Intelligente
L1	L2	L3	L4	L5
Iniziale	Definito	Consapevole	Misurato	Ottimizzato
Solo alcune delle azioni previste dalle best practices applicabili (guida operativa) sono implementate. Le risorse coinvolte nelle azioni attuate non hanno una visione d'insieme dei risultati attesi.	Tutte le azioni previste sono riconducibili a regole organizzative ben definite (policy, processi, procedure, ecc). Le regole sono diffuse a tutte le risorse interessate.	È assicurato che tutto il personale coinvolto nell'implementazione delle azioni previste sia consapevole di come quando e perché le regole vadano applicate, anche attraverso l'attuazione di continuativi piani formativi e periodiche comunicazioni.	Sono fissati obiettivi, per lo più quantitativi, per quanto riguarda le performance dei processi, delle procedure e delle soluzioni tecniche alla base delle azioni implementate. Le performance sono sistematicamente monitorate (in modo automatizzato).	Lo stato di implementazione del controllo è sistematicamente monitorato e i risultati sono analizzati in relazione al contesto (interno ed esterno / cambiamenti) dell'organizzazione al fine di individuare in modo proattivo miglioramenti

Informazioni raccolte sullo stato dei controlli



Processo di Sviluppo Sicuro del Software

Marica Antonacci

Plan for adoption of the Best Practices for Secure Software Development

Main guidelines:

- **ISO 27002:2022** is a guideline for information security controls
- **OWASP SAMM** (Software Assurance Maturity Model) is a well-established framework specifically tailored to enhance software security

Work Package	Task
WP1 Governance & Compliance	T1.1 Define Security Standards & Policies
	T1.2 Define Roles, Responsibilities, and Access Control Rules
	T1.3 Security Training and Awareness
WP2 Security Self-Assessment	T2.1 Create the projects inventory
	T2.2 Initial evaluation and plan for improvement
	T2.3 Code review and initial plan implementation
WP3 Continuous monitoring	T3.1 Establish and maintain frameworks and processes for continuous monitoring
	T3.2 Metrics collection and stakeholder feedback

~ 6 months for the adoption

[More details in our ISGC24 presentation]

Project inventory

- Indigo IAM + VOMS Attribute Authority
- Orchestrator
- Cloud Provider Ranker
- Federation Registry + Feeder (ex CMDB + CIP)
- Federation Manager
- orchestrator-dashboard

Performed security assessment on IAM

Preliminary information on the Orchestrator status

Stato delle piattaforme

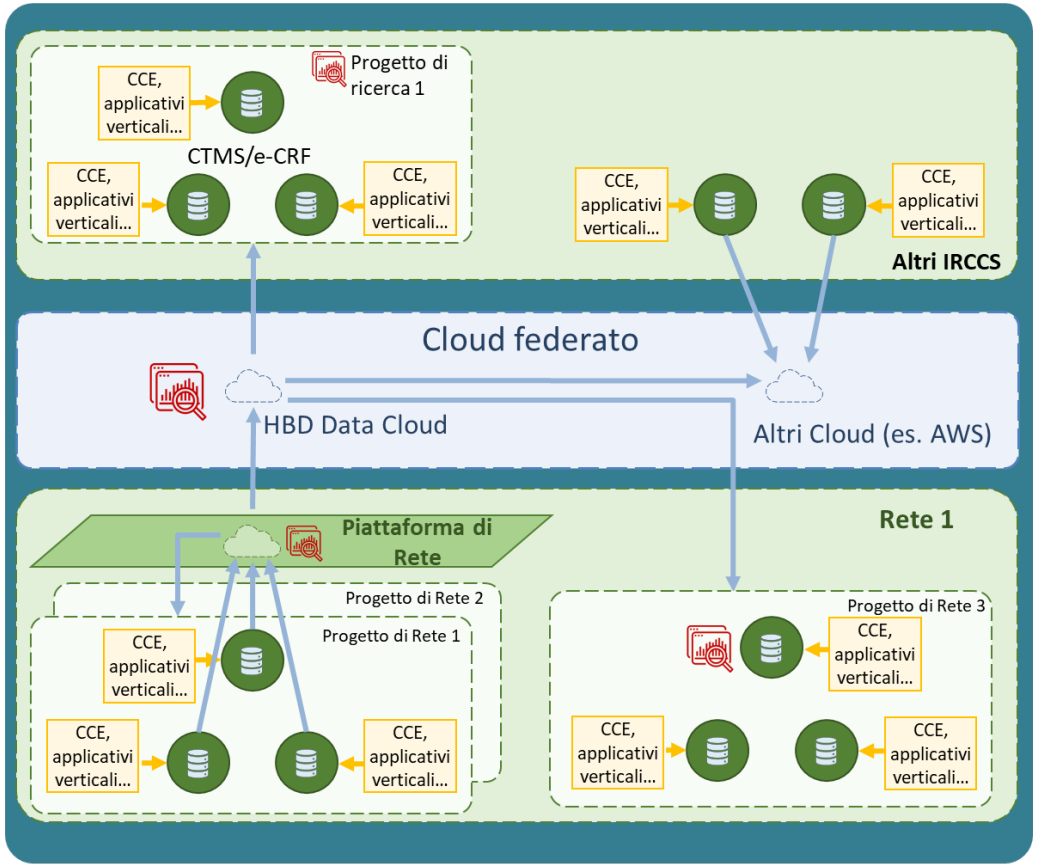
Stato attuale

- ~ 104 VM allocate su una ventina di tenant
- Piattaforma di Genomica Computazionale rilasciata in produzione ~ 150 TB di dati disponibili ai ricercatori (presentazione di Gasparetto oggi pomeriggio)
- Piattaforma di analisi dati per la medicina predittiva rilasciata nell'ambito del Progetto DARE (presentazione di Letizia Magenta oggi pomeriggio)
- Piattaforma di Alleanza Contro il Cancro in produzione dal 2020
- PoC di Consent Management System basato su blockchain (ISGC23)
- PoC di BaaS su INFN Cloud per la gestione di dati scientifici (presentazione di Domingo Ranieri mercoledi')

Prossimo passo: integrare le singole esperienze in una piattaforma cloud per la life science, a sua volta integrata in DataCloud

Next step: PoC of a Life Science as a Service platform

- Computational genomic
  - NextFlow pipelines run on RKE2
- EHR management
  - REDCap
- Radiomics
  - XNAT
- Interoperability tools from OHDSI (OMOP)
- Single Sign On with Keycloak
- DataManagement with RUCIO/FTS
- Resource allocation through Orchestrator



Joint working group including DARE, HBD, ICSC-Spoke8 (INFN, CINECA, UniBO, IEO)

Conclusioni

- Molto lavoro organizzativo svolto ed in corso
- Importante lavorare verso l'integrazione di EPIC con DataCloud sia a livello tecnico che organizzativo per evitare la creazione di silos con conseguente duplicazione degli sforzi
- Prossimi obiettivi:
  - certificazione multisito ad ottobre '24
  - PoC Life Science as a Service a dicembre '24