

INFN EPIC Cloud: Building ISO/IEC 27001-Certified Secure Cloud Regions for Trustworthy AI and Open Science

Thursday, 19 March 2026 11:20 (20 minutes)

The rapid growth of data-intensive life science research requests infrastructures and services that guarantee security, compliance, and interoperability across federated environments. EPIC Cloud (Enhanced Privacy and Compliance Cloud) represents the highly secure region of INFN DataCloud, representing the backbone of the Italian EOSC national node. Designed to meet stringent privacy and data protection requirements while ensuring FAIRness of scientific data, EPIC Cloud Information Security Management System is certified under ISO/IEC 27001, 27017, and 27018, ensuring a process-based approach to information security, cloud service governance, and personal data protection.

This contribution describes the organizational, architectural and operational principles underpinning the INFN EPIC Cloud, highlighting how ISO-certified information security processes enable trustworthy infrastructures to manage sensitive biomedical data and AI-driven workflows. EPIC Cloud supports critical use cases such as the Italian Health Ministry founded Health Big Data project, addressing the creation of a secure data lake for medical research in Italy, several use cases coming from NRRP-funded projects such as ICSC-Spoke8 and DARE (Digital Lifelong Prevention), the BMMRI-ERIC use case aimed to hosting AI pipelines implemented to analyse digitized tumour tissue samples and exploring the federated authentication, and the BOSCO computational genomics platform, powering large-scale analysis in compliance with GDPR and FAIR principles. By embedding security and compliance into the infrastructure lifecycle, EPIC Cloud advances data sovereignty, fosters secure research collaboration, and aligns with EOSC's vision for global open science.

A distinctive feature of EPIC Cloud is its advanced process-oriented governance model, inspired by ISO/IEC 27022:2021 guidelines for information security process management and strategically aligned with Porter's Value Chain framework. This approach goes beyond compliance, embedding security, and privacy as integral components of INFN's organizational and operational ecosystem.

Security and compliance are not treated as isolated functions but as value-generating activities embedded throughout the chain:

- Primary Activities: Data ingestion, AI-driven analytics, federated authentication, and secure data sharing are reinforced by ISO-driven controls, ensuring trust and reproducibility.
- Support Activities: Infrastructure management, personnel training, and regulatory alignment provide the foundation for operational resilience and scalability.

We will describe how this integration allows INFN to identify critical dependencies, optimize resource allocation (skilled personnel, operational time, and financial resources), and enhance the overall value delivered to stakeholders in EOSC, in life sciences and open science communities.

Moreover, we'll present the ongoing evolution of INFN EPIC Cloud towards a multiregion cloud that today already includes three INFN sites located in Bologna, Bari and Catania and how EPIC process-based governance model delivers tangible benefits: improved operational resilience, enhanced transparency, and readiness for multi-region scalability.

By embedding security into the value chain, EPIC Cloud establishes a replicable blueprint for scientific infrastructures committed to openness without compromising trust.

Primary authors: MARTELLI, Barbara (INFN - CNAF); BRUNENGO, Alessandro (INFN Genova); BELLUMO, Patrizia (INFN Catania); BETTONI, Diego (INFN Governing Council); BOVINA, Stefano (INFN CNAF); BOVO, Eleonora (INFN Central Administration); CARBONE, Luca (INFN Milano Bicocca); CARLETTI, Renato (INFN Central Administration); CARLINO, Gianpaolo (INFN Napoli); CESINI, Daniele (INFN-CNAF); CHIERICI, Andrea (INFN CNAF); COSTANTINI, Alessandro (INFN-CNAF); D'ANTONIO, Domenico; D'ISIDORO, Antonella (INFN Central Administration); DELL'AGNELLO, Luca (INFN CNAF); DONVITO, Giacinto (INFN); ENRICO,

Pasqualucci (INFN Roma1); FALABELLA, Antonio (INFN); FOGGETTI, Nadina (INFN Bari and CNR); GAS-PARETTO, Jacopo (INFN); GIUGLIANO, Carmen (INFN CNAF); GRANDI, Claudio (INFN Bologna); IENTILE, Valentina (INFN Catania); LANZI, Leandro (INFN Firenze); LONGO, Stefano (INFN CNAF); MANZARI, Vito (INFN Governing Council); MAURO, Patano (INFN Bari); MICHELOTTO, Diego (INFN-CNAF); MONFORTE, Salvatore (INFN Catania); MORETTA, Valeria (INFN Central Administration); PELLEGRINO, Carmelo (INFN-CNAF); ROTONDO, Riccardo (INFN Catania); SCARPONI, Luigi (INFN CNAF); SEQUI, Attilio Gaetano (INFN Central Administration); SERGI, Giusy (INFN CNAF); SINISI, Francesco (INFN-CNAF); SPINOSO, Vincenzo (INFN Bari); TELESCA, Giuseppe (INFN Central Administration); TRICOMI, Alessia Rita (INFN Governing Council); VALSECCHI, Veronica (INFN Central Administration); VINCENZO, Ciaschini (INFN CNAF); VISTOLI, Cristina (INFN CNAF); ZANI, Stefano (INFN CNAF); ZOTTI, Stefano (INFN CNAF)

Presenter: MARTELLI, Barbara (INFN - CNAF)

Session Classification: Networking, Security & Operationws - I (11:00 - 12:40)

Track Classification: Track 7: Network, Security, Infrastructure & Operations