Posteitaliane

CERT Posteitaliane

CERT
Computer Emergency Response Team

Self Assessment

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. (https://cloudsecurityalliance.org).

The Cloud Security Alliance (CSA) has launched the Security, Trust & Assurance Registry (STAR) initiative at the end of 2011. The CSA STAR is the first step in improving transparency and assurance in the cloud.

This document contains the results of assessments of the Cloud Security Alliance Cloud Controls Matrix (CCM) that Poste Italiane want to publish to guarantee transparency with its customers.

CERT Poste Italiane (www.poste.it; https://www.picert.it)

Document title: SELF_Assessment-CERT Poste Italiane	Version: 1.02	Date: 27-12-2013
	Classification: Public – TLP: O	

Table of Contents

Poste Italiane

Poste Italiane logistics and technology infrastructure is the largest and most extensive in the country, providing, in addition to postal services, integrated communication, logistics, financial, insurance and mobile telephony products and services to consumer, business and public sector.

With its network of post offices located throughout the country, Poste Italiane serves over 37Mln (thirtyseven millions) customers. Its widespread presence around the country, extensive experience and use of new technologies have enabled Poste Italiane to play a leading role in the process of economic and social development in Italy, as well as making it an ideal partner for the public sector in the provision of public services.

Poste Italiane has always focused on security of digital services as a strategic component of its approach to business, and this led the Group to acquire an acknowledged leadership within the national context in the whole area of cyber security.

In order to provide secure services and protect customers, on-line services and transaction, aligning its strategy with the evolving landscape of threats and maximizing value by the different operational security activities, Poste Italiane has established its **Computer Emergency Response Team (Poste Italiane CERT - PI CERT),** which has been conceived as a unique point of coordination of all the activities related to prevention and handling of cyber threats, by an integrated management of all the relevant flows of information coming from each of the already active operation centers.

Poste Italiane CERT's mission

"provide a unique point of coordination of all the activities related to prevention and handling of cyber threats impacting the information assets of Poste Italiane, by an integrated management of all the relevant flows coming from each of the already active operation centers, and to represent, at the same time, a unique interface towards the outer world with reference to all the operative information" exchange activities".

Poste Italiane CERT represents a unique interface towards the outer world with reference to all the operative information exchange activities, and, at the same time, it's a qualified support for the Group and all its different lines of business. Poste Italiane CERT carries out security monitoring, analysis & prevention, modelling & simulation activities.

Figure 1: Poste Italiane CERT services

Information Security in Poste Italiane

Protecting customers is a top priority for Poste Italiane business strategy and providing secure and continuous services is essential to guarantee customer satisfaction. To guarantee confidentiality, integrity and availability of its informations, Poste Italiane has defined, implemented and maintained its Information Security Management Systems and has identified in ISO/IEC 27001:2005 standard it reference model to achieve an effective and efficient management system able to ensure the achievement of defined objectives. Many units have obtained ISO/IEC 27001 certification including Poste Italiane CERT the nature and complexity of which has required a holistic and integrated approach to information security.

Information Security in Poste Italiane CERT

Poste Italiane CERT provides security services to its constituency ensuring adequate level of security. It has an extensive network of contacts, such as Law Enforcement, private or national CERTs, international organizations dedicated to cyber security, with which it has established specific communication protocols and exchange information. Core services such as Early Warning, Information Sharing, Incident Handling treat critical and sensitive information that require high level of protection. For this reason, Poste Italiane CERT has selected, and implemented security controls in accordance with the specific context**,** ISO/IEC 27001 standard and STAR certification. This document provides a self-assessment of Cloud Control Matrix implementation and a reference to ISO/IEC 27001 standard requirements and controls.

Poste Italiane CERT has obtained important awards in the field of information security by independent third parties, providing to its constituency a certified standard of quality and security.

bsi. ISO/IEC 27001 Information Security Management

Information Security Management System implemented by Poste Italiane CERT to manage its “core services” has been certified in accordance with **ISO/IEC 27001:2005 by British Standards Institution (BSI)**

bsi. CSA STAR Cloud Security

Poste Italiane CERT is the first Italian operator that has gained the **Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)** certification, among the top five in the world and the first with a SecaaS (Security as a Service) service certified.

FIRST

Poste Italiane is obtaining membership with **Forum of Incident Response and Security Teams** (**FIRST**), an organization recognized global leader in incident response teams coordination and the reference global network for CERT cooperation.

ACCREDITED BY TRUSTED INTRODUCER

Poste Italiane CERT is accredited by **The Trusted Introducer** is the network of CERTs in Europe, whose aim is to provide support to all the team for responding to security incidents, promoting collaboration and coordination between CERTs in Europe and neighbouring regions and connecting relevant organizations globally

enisa

Poste Italiane CERT is recognized in CERT Inventory maintained by the **European Network and Information Security Agency (ENISA)**, the agency that supports the creation of CERTs in Europe and their collaboration.

Poste Italiane Cloud Offering

Poste Italiane Cloud Services

Poste Italiane provides cloud services to Public Administration, large enterprise, SMEs and professionals. Poste Italiane Group has distinctive capabilities needed to ensure their customers a service to the highest level and address the needs of the market: high technological skills, compliance, competent sales and assistance network, new generation data center that meet the highest security standards.

PosteCloud service offering is divided into three main offerings to meet the different needs of professionals, companies and public administration: “virtualizza”, “digitalizza” and “ comunica e collabora”.

PosteCloud provides the best technologies on the market and the highest security levels also through Poste Italiane CERT services that guarantee a continuous monitoring, analysis and reaction of security events and prevention of incidents.

Poste Italiane CERT “Up Time & Performance Security Monitoring” cloud services

Poste Italiane, through its CERT, provides security services in cloud computing. As defined by ISACA, “Security as a Service – SecaaS” is the next generation of managed security services dedicated to the delivery, over the Internet, of specialized information security services. The adoption of Security as a Service (SecaaS) provides relevant benefits such as cost and resources reduction, ease of management, operations and provisioning, scalability and flessibility, alignment with major compliance requirements, security. The organization does not need more in-house staff with specific security skills and knowledge.

To provide a service with objective and certified level of security and quality, Poste Italiane CERT has certified ISO 27001/STAR Up Time & Performance Security Monitoring services provided in cloud computing.

Up Time & Performance Security Monitoring, provided as a SaaS model, makes available and configurable instruments to detect the status of websites and identify any malfunction or degradation of performance with respect to defined levels in order to promptly identify security events, guarantee continuity of operations and business, plan resource and optimize performance.

Poste Italiane CSA STAR Self-Assessment

Following is provided the self assessment of the Cloud Security Alliance Cloud Controls Matrix (CCM) that Poste Italiane want to publish to guarantee transparency with its customes

Compliance

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	Poste Italiane CERT (PI CERT) periodically performs internal and external audits to assess the security and compliance of its services and the effectiveness of its ISMS and in particular to determine whether the control objectives, controls, processes and procedures of its ISMS: • Conform to the requirements of ISO/IEC 27001:2005 and relevant legislation or regulations; • Conform to the identified information security requirements; • Are effectively implemented and maintained; • Perform as expected. PI CERT has defined and implemented an audit programme, approved by management, and specific audit plans assigning priority to audit activities in accordance with risk assessment results. Results of audit activities are presented to the management that assesses the opportunities for improvement and the needs of changes to the ISMS, treats the risks and takes decisions. Audit activities are carefully planned and agreed upon in advance by stakeholders for each audit plan. Audit team members are selected ensuring the criteria of impartiality and objectivity and the principle of segregation of duties.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.3 e) • Clause 4.2.3b • Clause 5.1 g • Clause 6 • A.15.3.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the	PI CERT performs periodic independent reviews and assessments to verify compliance with policies, procedures, standards and applicable regulatory requirements.	The control is applied also in accordance with the following ISO/IEC 27001

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	In addition with internal audits planned and the periodic vulnerability assessment to identify and mitigate vulnerabilities in the cloud service and infrastructures, external independent audits are planned to guarantee an impartial and objective evaluation.	clauses and controls requirements: • Clause 4.2.3e • Clause 5.1 g • Clause 5.2.1 d) • Clause 6 • A.6.1.8 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	PI CERT contracts with third parties include specific security clauses related to compliance with information security. Non Disclosure Agreements (NDA) are signed by all third parties before to start activities. All contracts include audit right to assess and verify the compliance of service provided by third party with contractual requirements. Periodical project review meeting are performed to evaluate third parties services, deliverables and their compliance with service agreements.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.2.3 • A.10.2.1 • A.10.2.2 • A.10.6.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.	PI CERT has an internal structure dedicated to legal aspects that in conjunction with Poste Italiane's Legal Department ensures compliance with relevant legislative, regulatory, and contractual requirements. Poste Italiane and PI CERT have well-established channels with the main national and European authority such as the Italian Data Protection Authority or Italian and other European Law Enforcements. PI CERT participates in network of expert, international organization about cyber security, information sharing or standardization group, specialist security forums, and professional associations.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.6 • A.6.1.7 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			It participates and is a co-founder with the US Secret Service and Italian Postal & Communication Police of the European Electronic Crime Task Force (EECTF).	
Compliance - Information System Regulatory Mapping	CO-05	Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adapt to new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure and hardware. Each element may be assigned a legislative domain and jurisdiction to facilitate proper compliance mapping.	The information security policy and the specific information security policies define the main security requirements to be implemented by information systems across the organization. The specific requirements for each system are identified through implementation of the risk management process that identifies the security requirements, analyzing risks applying the risk evaluation and acceptance criteria defined. This evaluation has performed in accordance with legislative, regulatory, contractual and business constraints, and with the organizational policies and procedures. PI CERT maintains an updated legal framework that identifies the legislative environment in which the PI CERT cloud service operates.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) • Clause 4.2.3 d) 6) Clause 4.3.3 • Clause 5.2.1 a – f • Clause 7.3 c) 4) A.7.2.1 • A.15.1.1 • A.15.1.3 • A.15.1.4 • A.15.1.6 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Compliance - Intellectual Property	CO-06	Policy, process and procedure shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.	All software used by PI CERT is legally licensed. PI CERT has defined and implemented policies, procedures and instructions, applicable also to third parties, to safeguard intellectual property and guarantee that only authorized and legally licensed software are used. Periodic audit are performed to verify that the software used have a legal license. In addition, agreements with third parties include specific cluases about safeguard intellectual property.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 • A.6.1.5 • A.7.1.3 • A.10.8.2 • A.12.4.3 • A.15.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Data Governance

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	PI CERT has defined and implemented a data classification and treatment policy that sets the baseline requirements to address the protection of information handled. In particular, the policy addresses: • Data classification • Information assets labeling requirements • Information assets handling requirements • Non Disclosure Agreements PI CERT organizational model establishes all roles and responsibilities related to services and information security. In addition, the asset inventory includes: • Asset identification • Asset ownership • Related processes or services • Information treated • License of software PI CERT has also developed and implemented a specific data protection and privacy policy to guarantee compliance with relevant legislation and regulations. Periodic audits are performed to verify the attributions of responsibility and the asset inventory update. An acceptable user policy has been communicated to all internal and external personnel and implemented. An existing policy about use of mobile instruments is implemented and communicated to all employees. Periodical awareness sessions are in place to aware all personnel on information security risks, organizational policies and procedure and their roles and responsibilities on information security.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.3 • A.7.1.2 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Data Governance -	DG-02	Data, and objects containing data, shall be assigned a	See DG-01	The control is applied also in accordance with

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Classification		classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.		the following ISO/IEC 27001 clauses and controls requirements: • A.7.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Data Governance - Handling / Labeling / Security Policy	DG-03	Polices and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that acts as aggregate containers for data.	See DG-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.2.2 • A.10.7.1 • A.10.7.3 • A.10.8.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Data Governance - Retention Policy	DG-04	Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of backups must be implemented at planned intervals.	PI CERT has defined and applied policies, procedures and mechanisms for data retention and storage to guarantee to its customers correct protection of all data and availability of services in accordance with the results of risk assessment and with regulatory, statutory, contractual or business requirements. PI CERT has implemented the followings: • Continuity strategies: continuity strategies, minimum service level sguaranteed, RTO and RPO of service are defined • Backup: all cloud services data, systems and application configurations are backed up to guarantee availability of information when necessary. Backup up media are maintained in other data	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • A.10.5.1 • A.10.7.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			center to reduce physical and environmental risks • Secondary site: a secondary site is located at a several hundred Km away and aligned periodically with the primary, in accordance with RPO defined • Recovery test: periodic test of continuity strategies and restore are performed • Internal audit: continuity strategies and implementation of retention and storage are subjected of periodic internal audit • Compliance: Data retention and storage are compliant with regulatory, statutory, contractual requirements	
Data Governance - Secure Disposal	DG-05	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	PI CERT has defined and implemented information destruction and secure disposal policy, specific procedure and solutions to guarantee a low level cleaning and erasing of information in case of information system disposal or reuse	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.6 • A.10.7.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.	PI CERT ensures physical separation of production, development and test environment. Test data are protected and controlled and non-production data are used in development or test environment. The service is provided to customer by a front end while all information and stored and adequately protected in back end environment. The implementation of changes is controlled and change management policy and procedures are defined and implemented in order to minimize the corruption and compromising of information systems due to the system's changes.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.1.3 • A.10.1.4 • A.12.4.2 • A.12.5.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Data	DG-07	Security	PI CERT ensures confidentiality, integrity and	The control is

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Governance - Information Leakage		mechanisms shall be implemented to prevent data leakage.	availability of information to prevent data leakage. The network is isolated, segregated and special controls are established and implemented to safeguard confidentiality and integrity of information stored on systems or passing over networks. In addition, opportunities for information leakage are prevented through the application of measures to prevent unauthorized network and systems access and to discourage misuse of information systems by internal and external personnel.	applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.6.2 • A.12.5.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Data Governance - Risk Assessments	DG-08	Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	PI CERT has defined and applied a policy and procedures of risk management. It has defined criteria for accepting risks and to identify the acceptable level of risks. PI CERT implements the methodology for Information Security Risk Management defined at enterprise level by application of integrative elements in order to make the methodology appropriate to ISMS, taking into account economic factors that characterize the services. The methodology aims to minimize the risk of loss of confidentiality, integrity and availability of information and maximize investments for information security checking in line with the risk profiles identified. The requirements for systems and all information treated are identified through implementation of the risk management process that identifies the suitable security requirements. Risk assessment results are presented, reviewed and approved by management in order to guarantee a governance of information security aligning information security closely with the goals of the business, deliver value to stakeholders, ensure conformance with internal and external requirements, review performance of information security and assess need for changes to the ISMS or opportunities for improvement. Risk assessment results, the residual risks and	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 c) & g) • Clause 4.2.3 d) • Clause 4.3.1 & 4.3.3 • Clause 7.2 & 7.3 • A.7.2 • A.15.1.1 • A.15.1.3 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			the identified acceptable level of risks, are reviewed at planned intervals or in case of relevant changes to the organization, technology, business, legal and regulatory environment, political and social climate and contractual obligations. Risk management process, as a part of enterprise risk management methodology, includes the following steps: • Enterprise architecture identification and classification • Business impact analysis • Risk analysis and evaluation (considering vulnerabilities, threats likelihood and impact) • Evaluation of acceptable level of risks • Risk treatment that can include: o Risk mitigation applying appropriate controls o Risk acceptance according with the acceptable level of risks identified o Risk transfer to other parties o Risk avoidance • Formal acceptance of residual risk • Risk monitoring	

Facility Security

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Facility Security - Policy	FS-01	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.	PI CERT has implemented a physical security policy and related procedures defined at enterprise level for maintaining a safe and secure working environment in offices, rooms, and facilities and secure areas. The working environment of PI CERT complies with current legislation in the field of physical and environmental security and data protection. The physical security requirements have been identified applying the risk management methodology to be sure to guarantee the adequate level of protection to all areas.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.5.1.1 • A.9.1.3 • A.9.1.5 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.	Physical access to PI CERT areas is protected and controlled 24h per day and seven days a week. In addition to checks to buildings access, there are in place other points of check before to be able to enter in the restricted areas. Physical access card, NFC technique with PIN, electronic keys and other technique are used. A specific physical access management policy is defined for PI CERT and a mechanism is in place to regulate the access of guests and/or visitors to its premises, as well as the treatment of Information and/or data. The PI CERT staff is able to immediately evaluate, the information and / or data that can be shared with the guest / visitor (eg, confidential, internal use) as well as implement and enforce the relevant rules of access to the premises. A register of all persons, who have had access to the areas and the reasons for, is maintained and updated.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.1.1 • A.9.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Facility Security - Controlled Access Points	FS-03	Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems.	Sensitive data and information systems are preserved also adopting physical security perimeters and specific security requirements such as fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols. Physical access cards, NFC technique with PIN, electronic keys and other techniques are used.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.1.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - Secure Area Authorization	FS-04	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	See FS-02	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.1.1 • A.9.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - Unauthorized Persons Entry	FS-05	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to percent unauthorized data corruption, compromise and loss.	PI CERT has service areas and other points are separated from the data processing areas.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.1.6 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - Off-Site Authorization	FS-06	Authorization must be obtained prior to relocation or transfer of hardware, software	See FS-02, FS-03, DG-01 and DG-06	The control is applied also in accordance with the following

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		or data to an offsite premises.		ISO/IEC 27001 clauses and controls requirements: • A.9.2.7 • A.10.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - Off-Site Equipment	FS-07	Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.	See DG01, DG-05	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.5 • A.9.2.6 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Facility Security - Asset Management	FS-08	A complete inventory of critical assets shall be maintained with ownership defined and documented.	See DG-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.1.1 • A.7.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Human Resources Security

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Human Resources Security - Background Screening	HR-01	Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.	The internal structure of Human Resource and Organization of Poste Italiane has defined and implemented policies and procedures related to human resource security prior to, during and in case of termination and change of employment. Critical roles for information security are identified at enterprise level. Prior to employment, specific background verification checks on all candidates, both internal and external, are performed proportionally to the roles and responsibilities that employees/contractors will have in matter of information security. Role and responsibilities of employees, contractors and third party users are defined, documented and clearly communicated during the pre-employment process. All personnel are aware of their employment and its future roles and responsibilities.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.8.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Human Resources Security - Employment Agreements	HR-02	Prior to granting individuals physical or logical access to facilities, systems or data, employees, contractors, third party users and tenants and/or customers shall contractually agree and sign equivalent terms and conditions regarding information security responsibilities in employment or service contract.	The internal structure of Human Resource and Organization of Poste Italiane has defined and implemented policies and procedures related to human resource security prior to, during and in case of termination and change of employment. Terms and conditions of employment are agreed and signed by employees, contractor and third party users. Terms and conditions include information security and confidentiality clauses, legal responsibility and rights for information security.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.5 • A.8.1.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Human Resources - Employment Termination	HR-03	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented and	The internal structure of Human Resource and Organization of Poste Italiane has defined and implemented policies and procedures related to human resource security prior to, during and in case of termination and change of employment. Contractual cluases define responsibilities of employees and external parties roles and	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements:

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		communicated.	responsibilities for termination or change in employment. Policies and procedures are in place to aware employees and external parties to their roles in information security. Periodical awareness, education and training sessions provide to all personnel appropriate knowledge about organizational information security policies and procedures, legal responsibilities, correct use of information systems and disciplinary process. Development professional course are provided to develop and maintain specific skills and knowledge.	• A.8.3.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Information Security

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Information Security - Management Program	IS-01	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	The nature and complexity of the services provided by the PI CERT require"governance" that must necessarily refer to a structured model for the management of information security. PI CERT has identified, in ISO/IEC 27001:2005 standard, the requirements to inspire itself to achieve an effective and efficient management system for information security able to ensure the achievement of the objectives set. Therefore Poste Italiane has decided to certify ISO/IEC 27001:2005 the "core" services provided by the PI CERT, including cloud services. The ISMS has established, implemented, operated, monitored, maintained and improved considering the characteristics of the business, the organization, its location, assets and technology, legal and regulatory environment, political and social climate, stakeholders needs. Following the management's commitment, an information security policy gives principles, minimum requirements and a common direction about information security across the organization. The information security policy is reviewed annually or in case of relevant changes to the organization, technology, business, legal and regulatory environment, political and social climate and contractual obligations. It is aligned to best practices, regulatory, federal/state and international laws where applicable. Information security roles and responsibilities have been clearly assigned across the organizations and adequate resources have been located. Policies and procedures have been developed and implemented in the main security topics as the following:	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2 • Clause 5 • A.6.1.1 • A.6.1.2 • A.6.1.3 • A.6.1.4 • A.6.1.5 • A.6.1.6 • A.6.1.7 • A.6.1.8 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			• Information security policy • Organization of information security • Risk management • Asset management • Access management • Incident Management • Business continuity • Security Audit • Human Resource Security • Development of secure systems • Data classification and treatment • Compliance with legal requirements • Physical and environmental security Policies and procedures are communicated to all personnel on regular basis and periodic awareness sessions are performed. Information system documentation is made available to authorized personnel to guarantee the effective use of the system's security features and to configuring, installing and operating the information systems.	
Information Security - Management Support / Involvement	IS-02	Executive and line management shall take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution	Poste Italiane management has always considered the information security a top priority of the organization. For this reason, it has decided to adopt ISO/IEC 27001:2005 standard and obtain the related certification considering it the best framework to achieve an effective and efficient management system for information security. The management has provided objective evidence of its commitment by: • Establishing and operating the Information Security Policy • Ensuring that ISMS objectives and plans are established;	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5 • A.6.1.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			• Establishing roles and responsibilities for information security across the organization • Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy; • Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS; • Deciding the criteria for accepting risks and the acceptable levels of risk; • Ensuring that internal ISMS audits are conducted and • Conducting management reviews of the ISMS	
Information Security - Policy	IS-03	Management shall approve a formal information security policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy shall be supported by a strategic plan and a security program with well defined roles and responsibilities for leadership and officer roles.	See IS-01 and IS-02	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 • Clause 5 • A.5.1.1 • A.8.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - Baseline	IS-04	Baseline security requirements shall be established and	See IS-01, IS-02 and CO-05	The control is applied also in accordance with the following

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Requirements		applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements. Compliance with security baseline requirements must be reassessed at least annually or upon significant changes.		ISO/IEC 27001 clauses and controls requirements: • A.12.1.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - Policy Reviews	IS-05	Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	See IS-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.3 f) • A.5.1.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - Policy Enforcement	IS-06	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures.	Policies and procedures are in place at enterprise level to establish disciplinary process. Periodical awareness, education and training sessions provide to all personnel appropriate knowledge about organizational information security policies and procedures, legal responsibilities, correct use of information systems and disciplinary process in the event of a violation.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.8.2.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - User Access Policy	IS-07	User access policies and procedures shall be documented, approved and implemented for	PI CERT has defined and implemented an access control policy and the related procedure to guarantee a correct management of customer and user access.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements.	They address the following aspects: • Account creation • Account maintenance • User account termination • Periodic account review The creation or the modification of an account, and its related authorization profile, both normal or privileged account, requires a formal and documented approval iter. Only after the approval the access to systems is provided. All accesses are documented within the audit log and are maintained for the time needed for future investigations. Relevant legislation and any contractual obligation related to protection of access to data or services are respected. Access right is assigned in accordance with need to know and segregation of duties principles. Access rights, existing account and related profiles are reviewed at planned intervals. There are in place mechanisms to revocate or modify account in case of termination of employment, contract or agreement, change of employment or transfer within the organization.	requirements: • A.11.1.1 • A.11.2.1 • A.11.2.4 • A.11.4.1 • A.11.5.2 • A.11.6.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - User Access Restriction / Authorization	IS-08	Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted.	See IS-07	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.2.1 • A.11.2.2 • A.11.4.1 • A 11.4.2 • A.11.6.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Information Security - User Access Revocation	IS-09	Timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.	See IS-07	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • ISO/IEC 27001:2005 • A.8.3.3 • A.11.1.1 • A.11.2.1 • A.11.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Information Security - User Access Reviews	IS-10	All levels of user access shall be reviewed by management at planned intervals and documented. For access violations identified, remediation must follow documented access control policies and procedures.	See IS-07	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.2.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Training / Awareness	IS-11	A security awareness training program shall be established for all contractors, third party users and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates	See HR-01 and HR-03	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.2.2 • A.8.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		in organizational procedures, process and policies, relating to their function relative to the organization.		
Information Security - Industry Knowledge / Benchmarking	IS-12	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	PI CERT participates in network of expert, international organization about cyber security, information sharing or standardization groups, specialist security forums, and professional associations. It participates and is a co-founder with the US Secret Service and Italian Postal & Communication Police of the European Electronic Crime Task Force (EECTF).	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.7 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Roles / Responsibilities	IS-13	Roles and responsibilities of contractors, employees and third party users shall be documented as they relate to information assets and security.	See IS-01 and IS-02	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.1 c) • A.6.1.2 • A.6.1.3 • A.8.1.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Management Oversight	IS-14	Managers are responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility.	See IS-01 and IS-02	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.2.2 • A.8.2.1 • A.8.2.2 • A 11.2.4 • A.15.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information	IS-15	Policies, process	To reduce the risk of system misuse,	The control is applied

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Security - Segregation of Duties		and procedures shall be implemented to enforce and assure proper segregation of duties. In those events where user-role conflict of interest constraint exist, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.	appropriate strategies of segregation of duties are implemented.	also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.1.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - User Responsibility	IS-16	Users shall be made aware of their responsibilities for: • Maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements • Maintaining a safe and secure working environment • Leaving unattended equipment in a secure manner	See HR-01 In addition, an acceptable user policy has been communicated to all internal and external personnel and implemented. A specific policy about use of mobile instruments exists, is implemented and communicated to all employees.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.2.2 • A.8.2.2 • A.11.3.1 • A.11.3.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Workspace	IS-17	Policies and procedures shall be established for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.	See DG-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.2.2 • A.8.2.2 • A.9.1.5 • A.11.3.1 • A.11.3.2 • A.11.3.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information	IS-18	Policies and	A specific security policy for data	The control is applied

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Security - Encryption		procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).	encryption is defined and implemented. Based on classification, and in accordance with the data classification and treatment policy, Information are stored or transmitted encrypted to protect their integrity and confidentiality.	also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.6.1 • A.10.8.3 • A.10.8.4 • A.10.9.2 • A.10.9.3 • A.12.3.1 • A.15.1.3 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Encryption Key Management	IS-19	Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.	Cryptographic controls are impelmeted to encrypt data in storage and trasmissions. Key management process is in place to guarantee key integrity, confidentiality and availability.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • A.10.7.3 • A.12.3.2 • A.15.1.6 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Vulnerability / Patch Management	IS-20	Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical	PI CERT has defined and implemented a change management policy and procedure. The implementation of changes is controlled in order to minimize the corruption and compromising of information systems due to the system's changes. Technical review and test of applications are implemented after operating system changes. Timely information about technical vulnerability are collected and analyzed. Technical vulnerability management process is implemented to ensure that	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.12.5.1 • A.12.5.2 • A.12.6.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		patches.	vulnerabilities are appropriately addressed, periodic vulnerability assessment is performed and mitigation plans are defined, documented and implemented.	
Information Security - Anti-Virus / Malicious Software	IS-21	Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.	PI CERT has implemented controls against malicious software providing protection from all malware types.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.4.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Incident Management	IS-22	Policies and procedures shall be established to triage security related events and ensure timely and thorough incident management.	PI CERT has defined and implemented an incident handling policy and specific incident handling procedures. Security events are collected, monitored, aggregated and correlated to timely identify and response to security incidents. PI CERT incident handling procedure cover the following topics: • Communications channels and modalities in which report an incident • Event monitoring • Triage • Identification of system and services involved • Impact evaluation • Incident categorization, classification and prioritization • Incident analysis • Incident response • Post-incident analysis • Lesson learned Contractors, employees and third party users are aware of their responsibility to report all information security events in a	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • A.13.1.1 • A.13.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			timely manner Communication with all stakeholders, including customer, is maintained during all incident life cycle. Specific procedures are identified in case of legal actions are required. All incident handling activities are in accordance with legislative, contractual and regulatory requirements. Escalation procedures are activated in case of necessity and according to the criteria defined.	
Information Security - Incident Reporting	IS-23	Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.	See IS-22	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • Clause 5.2.2 • A.6.1.3 • A.8.2.1 • A.8.2.2 • A.13.1.1 • A.13.1.2 • A.13.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Incident Response Legal Preparation	IS-24	In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the	See IS-22	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • Clause 5.2.2 • A.8.2.2 • A.8.2.3 • A.13.2.3 • A.15.1.3 For more details, please review the

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		relevant jurisdiction.		ISO/IEC 27001 and 27002 standard documents
Information Security - Incident Response Metrics	IS-25	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	PI CERT has a process in place to learn from security incident. The post-incident analysis involves the identification of the real cause of the incident, the evaluation of effectiveness of the actions taken to resolve the incident, reconstruction of the scenario of cause and effect, assessment of the impacts in the short and long term and development of recommendations to prevent the recurrence of a similar incident. Types, volumes, and costs of information security incidents are monitored in order to identify trends and predict possible attacks scenarios.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.13.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Acceptable Use	IS-26	Policies and procedures shall be established for the acceptable use of information assets.	PI CERT has defined and implemented a data classification and treatment policy that sets the baseline requirements to address the protection of information handled. An acceptable user policy has been communicated to all internal and external personnel and implemented. A specific policy about use of mobile instruments exists, is implemented and communicated to all employees. Periodical awareness sessions are in place to aware all personnel on information security risks, organizational policies and procedures and their roles and responsibilities on information security.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.1.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Asset Returns	IS-27	Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.	There are in place mechanisms to guarantee the return of assets and to revocate or modify account in case of employment termination, contract or agreement, change of employment or transfer within the organization. Asset inventory with the ownership of the assets is updated and reviewed regularly	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.1.1 • A.7.1.2 • A.8.3.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Information Security - e/ Transactions	IS-28	Electronic commerce (e-commerce) related data traversing public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.	N/A – No e-commerce service is provided in the cloud service by PI CERT	N/A
Information Security - Audit Tools Access	IS-29	Access to, and use of, audit tools that interact with the organizations information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	PI CERT has identified Information system audit tools and adequately it protects them to prevent compromise and misuse of log data.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.15.3.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Diagnostic / Configuration Ports Access	IS-30	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	To protect information integrity, confidentiality and availability, PI CERT systems has hardened. Network security mechanisms, like IDS and firewall, are in place to prevent unauthorized network access.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.6.1 • A.11.1.1 • A.11.4.4 • A.11.5.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Network / Infrastructure Services	IS-31	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer	See CO-03	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.2.3 • A.10.6.2

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		requirements.		For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	A specific policy about use of mobile instruments exists, is implemented and communicated to all employees. Access to organizational mobile devices is restricted. PI CERT has also defined and implemented information destruction and secure deletion policy, specific procedure and solutions to guarantee a low level cleaning and erasing of information in case of information systems disposal or reuse	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.7.2.1 • A.10.7.1 • A.10.7.2 • A.10.8.3 • A.11.7.1 • A.11.7.2 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Source Code Access Restriction	IS-33	Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.	PI CERT has defined a procedure for processing and storing information. Furthermore, access to program source code is restricted to reduce the potential for corruption of computer programs	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • A.12.4.3 • A.15.1.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Information Security - Utility Programs Access	IS-34	Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	To protect information integrity, confidentiality and availability, PI CERT systems has hardened. Use of network services and system utilities is regulated and periodically checked.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.4.1 • A 11.4.4 • A.11.5.4

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
				For more details, please review the ISO/IEC 27001 and 27002 standard documents

Legal

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Legal - Non-Disclosure Agreements	LG-01	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented and reviewed at planned intervals.	PI CERT contracts with third parties include specific security clauses related to compliance with information security. Non Disclosure Agreement (NDA) is signed by all third parties before to start activities. All contract include audit right to assess and verify the compliance of service provided by third party with contractual requirements. Periodical project review meeting are performed to evaluate third parties services, deliverables and their compliance with service agreements.	ISO/IEC 27001:2005 Annex A.6.1.5 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Legal - Third Party Agreements	LG-02	Third party agreements that directly, or indirectly, impact the organizations information assets or data are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	See LG-01	A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents

Operations Management

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Operations Management - Policy	OP-01	Policies and procedures shall be established and made available for all personnel to adequately support services operations role.	See IS-01 and IS-03	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.1 • A 8.1.1 • A.8.2.1 • A 8.2.2 • A.10.1.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Operations Management - Documentation	OP-02	Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	See IS-01 and IS-03	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.3 • A.10.7.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Operations Management - Capacity / Resource Planning	OP-03	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	The availability, quality, and adequate capacity and resources needed for the systems have been planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Detecting systems are in place to identify problems in due time. Monitoring systems verify the performance, use of resource and the state of health of all systems real time. In case of problems, the systems generate	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.3.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			and notify an alert.	
Operations Management - Equipment Maintenance	OP-04	Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.	See OP-3 In addition, strategies, policies and procedures have been established to guarantee continuity and availability of operations. Equipment is maintained in accordance with the supplier's recommended specifications where possible, and maintenance agreements signed by provider guarantee the support in case of needs.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Risk Management

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
Risk Management - Program	RI-01	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	PI CERT has defined and applied a policy and procedures of risk management. It has defined criteria for accepting risks and to identify the acceptable level of risks. PI CERT implements the methodology for Information Security Risk Management defined at enterprise level applying integrative elements in order to make the methodology appropriate to ISMS, taking into account economic factors that characterize the services. The methodology aims to minimize the risk of confidentiality, integrity and availability loss of information and maximize investments for information security checking that these are in line with the identified risk profiles. The requirements for systems and all information treated are identified through implementation of the risk management process that identifies the suitable security requirements. Risk assessment results are presented, reviewed and approved by management in order to guarantee a governance of information security aligning information security closely with the goals of the business, deliver value to stakeholders, ensure conformance with internal and external requirements, review performance of information security and assess need for changes to the ISMS or opportunities for improvement. Risk assessment results, the residual risks and the identified acceptable level of risks, are	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 c) through g) • Clause 4.2.2 b) • Clause 5.1 f) • Clause 7.2 & 7.3 • A.6.2.1 • A.12.6.1 • A.14.1.2 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
			reviewed at planned intervals or in case of relevant changes to the organization, technology, business, legal and regulatory environment, political and social climate and contractual obligations. Risk management process, as a part of enterprise risk management methodology, includes the following steps: • Enterprise architecture identification and classification • Business impact analysis • Risk analysis and evaluation (considering vulnerabilities, threats likelihood and impact) • Evaluation of acceptable level of risks • Risk treatment including: o Risk mitigation applying appropriate controls o Risk acceptance according with the acceptable level of risks identified o Risk transfer to other parties o Risk avoidance • Formal acceptance of residual risk • Risk monitoring	
Risk Management - Assessments	RI-02	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all	See RI-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 c) through g) • Clause 4.2.3 d)

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
		risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).		• Clause 5.1 f) • Clause 7.2 & 7.3 • A.6.2.1 • A.12.5.2 • A.12.6.1 • A.14.1.2 • A.15.1.1 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Risk Management - Mitigation / Acceptance	RI-03	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.	See RI-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.1 c) through g) • Clause 4.2.2 b) • Clause 4.3.1 • Clause 5.1 f) • Clause 7.3 • A.6.2.1 • A.12.5.2 • A.12.6.1 • A.15.1.1 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Risk Management - Business / Policy Change Impacts	RI-04	Risk assessment results shall include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective.	Risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective. Specific controls are identified to mitigate risks. The control selection is based on controls and control objectives provided by ISO/IEC 27001:2005 standard	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.2.3 • Clause 4.2.4 • Clause 4.3.1 • Clause 5 • Clause 7

Control Area	Control ID	Control Specification	Poste Italiane response	Applicable ISO/IEC 27001:2005 controls
				• A.5.1.2 • A.10.1.2 • A.10.2.3 • A.14.1.2 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Risk Management - Third Party Access	RI-05	The identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	See RI-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.2.1 • A.8.3.3 • A.11.1.1 • A.11.2.1 • A.11.2.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Release Management

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
Release Management - New Development / Acquisition	RM-01	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	PI CERT considers security as a top priority and an integral part of the information systems. Security aspects are addressed during whole life cycle of the information systems from design, implementation and maintenance to disposal phase. PI CERT identified security requirements that reflect the value of the information assets. For new and existing systems, the requirements for each system are identified through implementation of the risk management process that identifies the security requirements, analyzing risks applying the risk evaluation and acceptance criteria defined. This evaluation happens in accordance with legislative, regulatory, contractual and business constraints, and with the organizational policies and procedures. A specific policy is established to develop secure applications and formal processes are in place for the acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities. Organizational and technical measures are in place to guarantee correct processing of the systems and to prevent errors, loss, unauthorized modification or misuse of information in applications.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.4 • A.6.2.1 • A.12.1.1 • A.12.4.1 • A.12.4.2 • A.12.4.3 • A.12.5.5 • A.15.1.3 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Release Management - Production Changes	RM-02	Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring	The implementation of changes is controlled and change management policy and procedures are defined and implemented in order to minimize the corruption and compromising of information systems due to the system's changes.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.1.4

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		patches, service packs, and other updates and modifications.	To reduce risks of unauthorized accesses or changes, development, test and production environments are separated and controlled	• A.12.5.1 • A.12.5.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Release Management - Quality Testing	RM-03	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release.	PI CERT considers security as a top priority and an integral part of the information systems. Security aspects are addressed during whole life cycle of the information systems from design, implementation and maintenance to disposal phase.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.3 • A.10.1.1 • A.10.1.4 • A.10.3.2 • A.12.1.1 • A.12.2.1 • A.12.2.2 • A.12.2.3 • A.12.2.4 • A.12.4.1 • A.12.4.2 • A.12.4.3 • A.12.5.1 • A.12.5.2 • A.12.5.3 • A.12.6.1 • A.13.1.2 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Release Management - Outsourced Development	RM-04	A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all outsourced software development. The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by	There isn ’t software developed by outsourced but the acquired open source software package is evaluated by Vulnerability Assessment to check its security strength. In order to evalute the compliance to Poste Italiane Policy “Sviluppo degli applicativi sicuri”, the packge have to satisfy a specific control check list. The most important security testings lead on software are:	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.1.8 • A.6.2.1 • A.6.2.3 • A.10.1.4 • A.10.2.1 • A.10.2.2

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as either a ISO/IEC 17024 accredited certification or a legally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile.	• Testing for input validation • Injection Flow Testing • Testing to prevent spoofing • Failure testing The goal is to discover and prevent security compromises and to reduce vulnerabilities and the possibility of data corruption.	• A.10.2.3 • A.10.3.2 • A.12.1.1 • A.12.2.1 • A.12.2.2 • A.12.2.3 • A.12.2.4 • A.12.4.1 • A.12.4.2 • A.12.4.3 • A.12.5.1 • A.12.5.2 • A.12.5.3 • A.12.5.5 • A.12.6.1 • A.13.1.2 • A.15.2.1 • A.15.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents
Release Management - Unauthorized Software Installations	RM-05	Policies and procedures shall be established and mechanisms implemented to restrict the installation of unauthorized software.	See RM-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.1.3 • A.10.4.1 • A.11.5.4 • A.11.6.1 • A.12.4.1 • A.12.5.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Resiliency Management

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
Resiliency - Management Program	RS-01	Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.	PI CERT considers continuity as a top priority and an integral part of the information systems. For these reason, has identified potential continuity risks and has evaluated business impacts of interruptions on the organization. Specific continuity strategies have been defined and are periodically tested to reduce consequences and guarantee early resumption of essential operations. All cloud services data, systems and application configurations are backed up to guarantee availability of information in case of need. Backup up media are maintained in other data center to reduce physical and environmental risks A secondary site, located at a several hundred Km away, is aligned periodically with the primary, in accordance with RPO defined, ensuring continuity.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 4.3.2 • A.14.1.1 • A 14.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Resiliency - Impact Analysis	RS-02	There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners and	PI CERT considers security as a top priory and, to guarantee a correct management, has defined and implemented a documented categorization model to prioritize security activities and to address correctly security requirements. PI CERT identifies for each service: the associated criticality level, the risk exposure, the acceptable risk level and a priority level.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • ISO/IEC 27001:2005 • A.14.1.2 • A 14.1.4 For more details, please review the

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	A specific methodology has been defined and implemented to evaluate business impacts caused by loss of confidentiality, integrity and availability (in time) of the information processed by the service. On the basis of this assessment are identified the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for the services. PI CERT applies the business continuity management process defined at enterprise level, that includes the following steps: • Definition of business continuity strategies • Identification and implementation of business continuity solutions • Definition of documented business continuity plans • Test and improvement of business continuity plans • Management of continuity events • Improvements of business continuity management process Business continuity process is constantly aligned with the processes of risk management, change management and incident handling.	ISO/IEC 27001 and 27002 standard documents.
Resiliency - Business Continuity Planning	RS-03	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for	See RS-01 and RS-02	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • Clause 5.1 • A.6.1.2 • A.14.1.3 • A.14.1.4 For more details, please review the

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update and approval • Defined lines of communication, roles and responsibilities • Detailed recovery procedures, manual work-around and reference information • Method for plan invocation		ISO/IEC 27001 and 27002 standard documents.
Resiliency - Business Continuity Testing	RS-04	Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness.	See RS-05	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.14.1.5 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Resiliency - Environmental Risks	RS-05	Physical protection against damage from natural causes and disasters as well as deliberate attacks including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear mishap, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed	Cloud service infrastructure is located in locations that guarantee the adequate protection from physical and environmental risks. The physical security requirements implemented have been identified applying the risk management methodology to be sure to guarantee the adequate level of protection to all areas. The architecture and related facilities have been planned to guarantee high reliability adopting specific redundancy and protection measures. Cloud services data, systems and	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.1.4 • A.9.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		and countermeasures applied.	application configurations are backed up to guarantee availability of information. Backup media are maintained in other data center to reduce physical and environmental risks. The secondary site, aligned periodically with the primary, is located at a several hundred Km away.	
Resiliency - Equipment Location	RS-06	To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located a reasonable distance.	See RS-05	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Resiliency - Equipment Power Failures	RS-07	Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.).	See RS-05	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.2 • A.9.2.3 • A 9.2.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Resiliency - Power / Telecommunications	RS-08	Telecommunications equipment, cabling and relays transceving data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.	See RS-05	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.9.2.2 • A.9.2.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Security Architecture

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
Security Architecture - Customer Access Requirements	SA-01	Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.	PI CERT considers security and respect of contractual and regulatory obligations as a top priority. It takes care its customers, wants to satisfy their expectations, meets their needs and add value to all its stakeholders. PI CERT has internal structure dedicated to legal aspects that in conjunction with Poste Italiane Legal Department ensures compliance with relevant legislative, regulatory, and contractual requirements. Compliance with privacy and data-protection law is ensured and all identified legislative, regulatory, and contractual requirements are addressed prior to guarantee customer access to data, assets and information systems.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.6.2.1 • A.6.2.2 • A.11.1.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - User ID Credentials	SA-02	Implement and enforce (through automation) user credential and password controls for applications, databases and server and network infrastructure, requiring the following minimum standards: • User identity verification prior to password resets. • If password reset initiated by personnel other than user (i.e., administrator), password must be immediately changed by user upon first use. • Timely access revocation for terminated users. • Remove/disable inactive user accounts at least every 90 days. • Unique user IDs and disallow group, shared,	PI CERT has implemented strong measures to prevent unauthorized access. Organizational and technical controls are in place to guarantee the correct level of service protection. Automated controls for user credential and password are implemented and periodicicaly checked. PI CERT has defined and implemented an access control policy and the related procedure to guarantee a correct management of customer and user access. All accesses are documented within the audit log and are maintained for the time needed for future investigations and in accordance with the relevant legislation and any contractual	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.8.3.3 • A.11.1.1 • A.11.2.1 • A.11.2.3 • A.11.2.4 • A.11.5.5 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		or generic accounts and passwords. • Password expiration at least every 90 days. • Minimum password length of at least seven (7) characters. • Strong passwords containing both numeric and alphabetic characters. • Allow password re-use after the last four (4) passwords used. • User ID lockout after not more than six (6) attempts. • User ID lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • Re-enter password to reactivate terminal after session idle time for more than 15 minutes. • Maintain user activity logs for privileged access or access to sensitive data.	obligations.	
Security Architecture - Data Security / Integrity	SA-03	Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.	PI CERT ensures confidentiality, integrity and availability of information. The network is isolated, segregated and special controls are established and implemented to safeguard confidentiality and integrity of information stored on systems or passed over networks. Based on classification, and in accordance with the data classification and treatment policy, specific security measures, such as encryption, are implemented to protect their integrity and confidentiality. PI CERT contracts with third parties include specific security clauses related to compliance with information security and Non Disclosure Agreements (NDA) are signed by all third parties before to start activities.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.8.1 • A.10.8.2 • A.11.1.1 • A.11.6.1 • A.11.4.6 • A.12.3.1 • A.12.5.4 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
Security Architecture - Application Security	SA-04	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.	See RM-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.5.6 • A.11.6.1 • A.12.2.1 • A.12.2.2 • A.12.2.3 • A.12.2.4 • A.12.5.2 • A.12.5.4 • A.12.5.5 • A.12.6.1 • A.15.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Data Integrity	SA-05	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data.	See RM-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.9.2 • A.10.9.3 • A.12.2.1 • A.12.2.2 • A.12.2.3 • A.12.2.4 • A.12.6.1 • A.15.2.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Production / Non-Production Environments	SA-06	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	See RM-01	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.1.4 • A.10.3.2 • A.11.1.1

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
				• A.12.5.1 • A.12.5.2 • A.12.5.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Remote User Multi-Factor Authentication	SA-07	Multi-factor authentication is required for all remote user access.	Two-factor authentication mechanisms are in place in accordance with results of risk assessment.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.1.1 • A.11.4.1 • A.11.4.2 • A.11.4.6 • A.11.7.1 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Network Security	SA-08	Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.	The network is isolated, segregated and special controls are established and implemented to safeguard confidentiality and integrity of information passing over networks. Network security devices (e.g. Firewalls and IDSs) are in place and configured to prevent unauthorized access to internal network and to detect possible attacks. All their relevant events are suitably logged, monitored and recorded.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.6.1 • A.10.6.2 • A.10.9.1 • A.10.10.2 • A.11.4.1 • A.11.4.5 • A.11.4.6 • A.11.4.7 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Segmentation	SA-09	System and network environments are separated by firewalls to ensure the following requirements are adhered to:	See SA-08	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements:

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		• Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Preserve protection and isolation of sensitive data		• A.11.4.5 • A.11.6.1 • A.11.6.2 • A.15.1.4 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Wireless Security	SA-10	Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.). • Logical and physical user access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	N/A – No wireless networks are used in the cloud service provided by PI CERT	N/A
Security Architecture - Shared Networks	SA-11	Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the	See SA-08	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.8.1 • A.11.1.1 • A.11.6.2 • A.11.4.6

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
		compensating controls used to separate network traffic between organizations.		For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Clock Synchronization	SA-12	An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference, in this event the jurisdiction or platform is treated as an explicitly defined security domain.	PI CERT uses clock synchronization protocols to ensure that time of systems events is synced and that the timestamp reflects the real date/time to ensure the accuracy of audit logs for future investigations.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.10.1 • A.10.10.6 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Equipment Identification	SA-13	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	PI CERT uses equipment identification protocols to authenticate connections and to prevent presence of unauthorized systems.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.11.4.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.

Control Area	Control ID	Control Specification	Poste Italiane CERT response	Applicable ISO/IEC 27001:2005 controls
Security Architecture - Audit Logging / Intrusion Detection	SA-14	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	Monitoring activities are performed to detect unauthorized information processing activities. Systems logs recording user activities and security events are collected and maintained in accordance with the relevant legislative and contractual obligations. In addition, log information are appropriately protected against tampering and unauthorized access. Security events are collected, monitored, aggregated and correlated to timely identify and response to security incidents and to mitigate existing weaknesses or vulnerabilities.	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.10.1 • A.10.10.2 • A.10.10.3 • A.10.10.4 • A.10.10.5 • A.11.2.2 • A.11.5.4 • A.11.6.1 • A.13.1.1 • A.13.2.3 • A.15.2.2 • A.15.1.3 For more details, please review the ISO/IEC 27001 and 27002 standard documents.
Security Architecture - Mobile Code	SA-15	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.	Mobile code installation is not authorized in the cloud service provided by PI CERT	The control is applied also in accordance with the following ISO/IEC 27001 clauses and controls requirements: • A.10.4.2 • A.12.2.2 For more details, please review the ISO/IEC 27001 and 27002 standard documents.