CAIQv3.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			The Ifin Sistemi SDLC incorporates industry best practices, includes threat modeling and completion of a risk assessment, formal software security audits at all stages of design. Ifin Sistemi implements procedures in line with the ISO 9001 and ISO/IEC 27001 standards, whose validated and certified by an independent auditor. For further details on the controls in place, refer to the SoA of the ISMS
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Ifin Sitemi follows a structured code development and release process. As part of this process, all code is peer reviewed. also performs continuous post-production tests based.
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	X			Ifin Sistemi does not rely on software suppliers. All software is developed by Ifin Sistemi, using a mature software development process.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modelling, manual code reviews, and other techniques.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			Ifin Sistemi communicates its security and control environment to customers through industry certifications and third-party attestations. Access to data, and application solutions is provided to customers in line with compliance with the GDPR 2016/679.
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	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	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Ifin Sistemi conducts data integrity controls maintained through all phases including transmission, storage and processing.
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Ifin Sistemi has been validated and certified by an independent auditor to confirm alignment with ISO/IEC 27001 certification standard.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			Ifin Sistemi periodically perdorms internal and external audits to assess the security and compliance of its services and effectiveness of its ISMS, conform to the requirements of ISO/IEC 27001, ISO 9001 and rilevant legislation or regulations.
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Ifin Sistemi makes its ISO 9001 and ISO/IEC 27001 certificates report available to customers. They are published on the institutional website.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			

		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Penetration tests are performed regularly by independent security firms.
		AAC-02.4		Do you conduct internal audits at least annually?	X			Ifin Sistemi maintains an internal audits program and risk assessments
		AAC-02.5		Do you conduct independent audits at least annually?	X			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	X			Ifin Sistemi Security Policy prohibits sharing this information but executive Summary is available upon request or contract obligation
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X			Ifin Sistemi publishes and makes available its ISO/IEC 27001, ISO 9001 and other certification report online. Detailed information of some confidential reports can be obtained under NDA.
Audit Assurance & Compliance *Information System*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			With Reference to ISO/IEC 27001 standard Annex 18, Ifin Sistemi monitors relevant legislative and regulatory requirements. Have established channel with the main
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	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, maintenance, and information security requirements. Requirements for 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	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			Ifin Sistemi have a business continuity plan. Are in place a documented strategy Backup and for restoring IT
		BCR-01.2		Do you have more than one provider for each service you depend on?		X		Ifin Sistemi relies on a single qualified CSP infrastructure as service provider.
		BCR-01.3		Do you provide a disaster recovery capability?	X			
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			Ifin Sistemi monitors the CSP infrastructure as service provider SLA fulfillment. In the event of provider failure
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?	X			Available for tenants upon request.
		BCR-01.6		Do you provide a tenant-triggered failover option?		X		SaaS platform
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?	X			Available for tenants upon request
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Business Continuity policies and procedures have been developed and verified in line with ISO/IEC 27001 standards. Ifin Sistemi performs regular testing of its business continuity plans.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.
		BCR-03.2	effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) 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	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			With reference to ISO/IEC 27001 Appendix A Domain 12, information System Documentation is made available internally to Ifin Sistemi authorized personnel.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	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 accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of	Is physical damage anticipated and are countermeasures included in the design of physical protections?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.

Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.
		BCR-07.2		Do you have an equipment and datacenter maintenance routine or plan?			X	The SaaS platform is implementd on Qualified Certification Service Provider infrastructure which guarantees high reliability and availability of information by adopting specific redundancies and protection measure.
Business Continuity Management & Operational Resilience *Equipment Power*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?			X	The SaaS platform is implementd ON CSP infrastructure that has implemented redundancies and safeguards in its datacenters to minimize the impact of service outages
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			Are defined cloud service level agreement
		BCR-09.2	• 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	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			Business continuity planning starts with an analysis and assessment of threats and risks for a company and initial business impact analysis activities (are Identified the most critical systems for the main operations of our business)
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Policies and Procedures have been established through Ifin Sistemi Security framework based upon ISO/IEC 27001 and ISO 9001 standard. Roles and responsabilities are axplicity assigned, pubblished, and well-understood by all employees.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical capabilities to enforce tenant data retention policies?	X			Considering a multi-tenant SaaS platform
		BCR-11.2		Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			Specific policies regarding data retention and destruction are in place
		BCR-11.3		Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			
		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Ifin Sistemi implements virtual private cloud on qualified CSP that guarantee the replacement of the assigned
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	X			
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	X			Customers can request to export their data from the application offered as a SaaS service
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X			Recovery test is periodically performed
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			Policies and Procedures have been established through Ifin Sistemi Security framework based upon ISO/IEC 27001, ISO 9001 standard.
Change Control & Configuration Management *Outsourced*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			Release notes are documents that are distributed with software products

Development		CCC-02.2	service management processes).	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			Periodical release notes are available
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			Ifin Sistemi has internal procedures to communicate to its customers vulnerabilities, threats likelihood and impact of its applications.
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Ifin Sistemi incorporates standards of quality as part of the system development lifecycle processes.
		CCC-03.5		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	Ifin Sistemi does not generally outsource development of software.
		CCC-03.6		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			A specific policy is established to develop secure applications anf formal process is in place. System development lifecycle incorporates industry best practices. Debugging features are available during appropriate stages.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			Access to product infrastructure is tightly controlled. The ability to install unapproved software is not allowed and this activity is heavily monitor.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		Generally, information related to ifin Sistemi applications and software system effort is internal documentation. Anyway, Ifin Sistemi can provide a documentation of the continuous implementation model adopted (change management process) on request.
		CCC-05.2	Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			
		CCC-05.3		Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			The virtual machines include tags/metadata in order to describe the data classification and purpose of the service.
		DSI-01.2		Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	Ifin Sistemi is a SaaS solution provider, and only uses virtual infrastructure in production environment on qualified CSP
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			Ifin Sistemi implements the service offered and collects tenants data at primary DataCenter of the qualified CSP located in ITALY and secondary site in EU region. Ifin Sistemi will not move tenant content from the physical region without notifying the tenant, unless required to comply with the law or requests of governmental entities. Ifin Sistemi developed and implemented a specific data protection in accordance to compliance with relevant legislation and regulations.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X			
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses 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	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Ifin Sistemi uses qualified CSP that allow access to secure cloud infrastructures (e.g. SSH, VPN).
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Interactions are generally made via API request and requests are encrypted.

Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	X			Ifin Sistemi has defined and implemented a data classification and treatment policy that sets the baseline requirements to address the protection of information handled, in accordance with the ISO/IEC 27001 standard and data protection regulation.
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	X			
		DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	X			
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Production data are not replicated into non-production environments. if necessary it is mandatory the explicit permission of the customer. Production and non-production environments are segregated. No-production data are used in development or test environment.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			Ifin Sistemi organizational model establishes all role and responsabilities related to service and informaztion security. Customer responsabilities are documented in our term of service, privacy policy and related documents. Accetpable user policy has been communicated to all internal and external personnel and implemented.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Ifin Sistemi performs secure deletion.
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Tenant may exit the service according to the Terms of our Service Agreement. See the Term of Service and Service Manual for details.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			Ifin Sistemi implements the service offered and collects tenant data at primary DataCenter of the qualified CSP, which ensures that phisical infrastructure are inventory process and supply chain are compliant with ISO/IEC 27001. Ifin Sistemi maintains inventory virtual assets
		DCS-01.2		Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., 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.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			Ifin Sistemi implements the service offered and collects tenant data at primary DataCenter of the qualified CSP, which ensures that physical security controls are compliant with ISO/IEC 27001
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	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.	Do you have a capability to use system geographic location as an authentication factor?		X		
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			Ifin Sistemi implements the service offered and collects tenant data at primary DataCenter of the qualified CSP which ensures that manages equipment identification are compliant with ISO/IEC 27001
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			Adeguate procedures are in place
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure	Can you provide tenants with your asset management policies and procedures?	X			Ifin Sistemi is SaaS provider that implements the application offered and collects tenant data at primary DataCenter of the qualified CSP. Both are aligned with ISO/IEC 27001 standard, follows the Annex A domain 8.

Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			confirm alignment with ISO/IEC 27001 certification standard. Refer to Annex A, domain 11 for further details.
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			In alignment with ISO/IEC 27001 standard, team members complete periodic security education, based on their role. Compliance audits are periodically performed to validate that team members understand and follow the established policies.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?			X	Ifin Sistemi is a SaaS solution provider, and only uses virtual infrastructure in production environment on qualified CSP
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	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	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Ifin Systems implements the service application (SaaS in Private Cloud) and collects the data of the holders at the primary Data Center of the qualified CSP, which provides high levels of physical and network security and maintain various levels of audited (internal and extrernal) security mechanism, including ISO/IEC 27001 compliance and other standards.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			Ifin Sistemi has defined a key management policy to support encryption of data in transit and at rest (the latter option, on request)
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	X			In accordance with Client
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			In accordance with Client
		EKM-02.3		Do you maintain key management procedures?		X		Procedures must be updated
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?		X		Procedures must be updated
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	X			Ifin Sistemi uses an internal framework to create and manage encryption keys. Key management process are reviewed periodically in accordance with ISO/IEC 27001 standard. They are also used organization CA that provide cryptographic and symmetric and asymmetric key management services.
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of 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) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			On Client request, in accordance with the data classification and treatment policy, information could be stored encrypted to protect their integrity and confidentiality. ifin Sistemi leverages several technologies to ensure stored data is encrypted at rest
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			Ifin Sistemi leverages advantage of the robust machine image protections. If necessary, virtual machines are encrypted during transport
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?		X		Documentation must be updated
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			Open encryption standards
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Key are maintained using qualified CSP infrastructure

		EKM-04.3	the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you store encryption keys in the cloud?	X			Private keys are stored in separate vault storages or others places, in accordance with clients
		EKM-04.4		Do you have separate key management and key usage duties?		X		Ifin Sistemi manages all encryption keys created
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			In alignment with ISO 27001 standards, Ifin Sistemi maintains system baselines for critical component
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			The recommendations of the European Commission followed and GDPR
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Risk assessments occur at least annually
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			The ISMS has established, implemented, monitored, maintained and improved considering the characteristics of the business, the organization, its location, asset and technology, legal and relulatory environment and stakeholders needs In accordance with ISO/IEC 27001 standard, compliance audits are performed so that employees understand and follow the established policies
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be 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 shall include, but not be limited to, the following areas insofar as they relate to the	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			Ifin Sistemi is ISO/IEC 27001 certified by external auditors. Certification is available on website.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	X			ISMS is reviewed on an annual basis.
Governance and Risk Management *Management Support /*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			Formal guidelines and procedures are in place
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			Security policy are communicated to all interested parties
		GRM-06.2		Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			Roles and responsibilities related to the security policy are clearly defined and allocated in accordance with ISO/IEC 27001 standard
		GRM-06.3		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			Ifin Sistemi information security and privacy policies align with industry standards. Contractual relationship are in place to verify and monitor supplier compliance with industry standards
		GRM-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			Evidence arising from internal audit and third party ISO 27001 activities are documented
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			Ifin Systems compliance information are is published on our website
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	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 disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			This is established by internal policies, standards, training, and processes.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			

Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			Updates security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO/IEC 27001 standard. Risk assessments and risk management produce as output security updates and treatment plan
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Tenants are informed through the Ifin Sistemi institutional website and by email in relation to changes regarding information security and privacy policies
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			Security policies are reviewed at least annually. The privacy policy is updated and reviewed by the internal DPO
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			Regular risk assessments are conducted according to ISO 31000 standard. These include likelihood and impact for all identified risk categories using qualitative and quantitative methods
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			
Governance and Risk Management *Program*	GRM-11	GRM-11.1	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 stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	X			Ifin Sistemi is ISO/IEC 27001 certified by external auditors. This certification is available to tenants and has different control points which focus on quality assurance and identify risks to implement appropriate measures
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Procedures should be clearly defined
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	X			
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Staff with a relevant role for the organization data security are subject to background checks. Employment education are performed for all employees
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			Prior to up taking their duties employees is asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.
		HRS-03.2		Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			The internal structure of HR of Ifin Sistemi has defined and implemented policies and procedures related to human resource security prior to, during and in case of termination and change of role. Critical roles for imformation security are identified at enterprise level. All staff are aware of their roles and responsabilities
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			A specific policy about use of mobile instruments exists, in implemented and communicated to all staff. Many protections are in place to govern access from mobile devices
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified,	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			All policies and procedures are reviewed on at least an annual basis

Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			All roles and responsibilities relating to information security and environment operations are documented
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			Procedures are defined and documented which establish clear rules for the correct use of IT components, including the management of mobile and portable devices
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?		X		
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	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 in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			In alignment with ISO/IEC 27001 standard, security awareness training is made available to all staff. Additional traing occur when significant upadates to policies occur, and multiple levels of security training are provifed to staff, based on their roles.
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			As Ifin Sistemi is SaaS provider, training materials speak extensively to cloud security models
		HRS-09.3		Do you document employee acknowledgment of training they have completed?	X			Staff must acknowledge completion of training and this acknowledgment is documented and stored
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			In alignment with ISO/IEC 27001 standard, security awareness training is made available to all staff
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			Additional traing occur when significant upadates to policies occur, and multiple levels of security training are provifed to staff, based on their roles
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			Ifin Sistemi implements various methods of internal communication to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. Employees receive notification on the importance of security, asset security via email, online resources an other ways. Security awareness training is made available to all employees. The security team and internal procedures helps provide additional security awareness, especially regarding ensuring instruments is no left in unsecured space
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			
		HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			In line with ISO/IEC 27001 standard, formal policies and procedures for logical access to internal systems have been defined (granted access to based on role). In particolar, access to security systems is restricted to only administrators.

		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Production systems are monitored and audit log is collected to separate server
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			In line with ISO/IEC 27001 standard, ISMS access rights are reviewed at least annually or when users' roles changes. Refer to Annex A, domain 9 for additional details
		IAM-02.2		Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			Specific access control rights are allocated to each role following the need to know principle
		IAM-02.3		Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			Role-based access control is used and the principle of least privilege is followed
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			
		IAM-02.5		Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			On Request is possible to setted MFA
		IAM-02.7		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			Systems access is removed within three business days as when change in the user's role takes place or when access is no longer required.
Identity & Access Management *Diagnostic / Configuration Ports*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Activity of the HR function
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Ifin Sistemi is certified for ISO/IEC 27001 and follows the Annex A 6.1.2 domain on this. Access to the production system is limited only to named administrators and the audit log is collected to separate the server. If required, tenants are empowered to create and manage to create and manage users of their portals and assign appropriate privileges to those users. Refer to the service agreement contractual and manual documentation
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Ifin Sistemi source code is stored in the version control system and access is limited to authorized members of the software development
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Strict authorization rules govern access to all parts of the internal Ifin Sistemi product infrastructure
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	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	Does your organization conduct third-party unauthorized access risk assessments?	X			
		IAM-07.2		Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access?	X			
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			

		IAM-08.2	and replication limitation only to users explicitly defined as business necessary.	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	X			
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			In alignment with the certified ISO/IEC 27001 standard, Ifini Sistemi has access control policies in place and approval is needed from the management before getting access to any assets. Any entitlment follows organizational changes
		IAM-09.2		Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			Only if deemed necessary and for a limited time with registred logs
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			Ifin Sistemi performs regular access reviews (depending on the criticality of the system). All administrators participate in periodic safety training courses and periodic access checks are performed to validate appropriate access provisioning. Access is revoked if the employee is terminated.
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X			All user-privilege changes are recorded to task management system
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			When necessary, security issues are communicated to tenants in accordance with appropriate confidentiality methods.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			In accordance with the ISO/IEC 27001 standard, user access rights are reviewed after any change in the status of employee (e.g., transfer or termination), and to revoke accounts and access where needed.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?		X		Is an optional feature
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?				
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		X		Is an optional feature
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		X		
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			

		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			On Request is possible to setted MFA
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?		X		
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			Ifin Sistemi, in the virtual environment, uses IDS and Web Application Firewall
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			In alignment with the certified ISO/IEC 27001 standard, logs are accessible to authorized personnel only
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			Ifin Sistemi Incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO/IEC 27001 standard, system utilities are appropriately restricted and monitored.
		IVS-01.4		Are audit logs centrally stored and retained?	X			Ifin Sistemi stores audit logs in secure storage vaults with restricted access to the information security team
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Ifin Sistemi utilizes automated monitoring systems to provide a high level of service performance and availability. Alarmas are configured for key security events
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Server images are protected from unauthorized access and any configuration changes to virtual machines are logged and collected
		IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Acces to the Ifin Sistemi product infrastructure is limited to a small subset of staff, and the infrastructure is purpose-built to be rapidly de-provisioned, and re-provisioned in short time. Server istance configuration is managed through console, and access to console configuration files is tightly controlled. The response to identified tampering or other server-level integrity question is a re-provisioning of the machine
		IVS-02.3		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			Ifin Sistemi takes care of the virtual machine integrity. Tenant do not interact with our products at the hypervisor or server infrastructure
Infrastructure & Virtualization Security	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			In alignment with ISO 27001 standards, Ifin Sistemi information systems utilize internal system clocks synchronized via NTP

Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	X			Server instances are not oversubscribed. Ifin Sistemi manages capacity and utilization data in alignment with ISO/IEC 27001 standard
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			
		IVS-04.3		Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			Ifin Sistemi manages capacity and utilization data in alignment with ISO/IEC 27001 standard. Service scaling is performed in in an optimized way
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			The systems are continuously monitored
Infrastructure & Virtualization Security	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X	Does not offer IaaS services
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Security documentation is updated in regular basis
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			Access control lists and firewall rules are programmatically monitored against a standardized configuration baseline.
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			Firewall rule sets and access control lists with business justification are documented and reviewed whenever any changes needs to be made.
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			Ifin Sistemi implements least privilege throughout its infrastructure components. Server instances are configured to perform a particular function.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Tenants access only production but Ifin Sistemi creates and maintain separate test environment for SaaS platform testing. (these are not separate per tenant). These are not generally available to customers: tenant can provision non production environment via requests, contractual agreement
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	Does not offer IaaS services
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			Ifin Sistemi network segmentation is aligned with ISO 27001 standards. Refer to ISO/IEC 27001 standard, Annex A. domain 13 for further detail. Physical segregation cannot be guaranteed because of the cloud environment
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			In alignment with the ISO/IEC 27001 standard, all services are protected by firewall
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			
		IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			Software resources rely on logical strong isolation mechanisms to protect their data
		IVS-09.4		Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer data is logically segregated between tenants. Ifin Sistemi uses data encryption mechanisms both during transmission
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			

Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Ifin Sistemi uses always secured and encrypted communication channels when data is in transit. Ifin Sistemi does not manage any physical servers
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			
Infrastructure & Virtualization Security *VMM Security -*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Access to hypervisor features is restricted to a few employees whose roles require access and user permissions are limited to performing their job function
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures 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, and SNMP community strings)	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Qualified CSP IaaS does not permit the use of wireless networks thus, Ifin Sistemi SaaS Porvider does not have the ability to implement wireless in the environment
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks)	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			In alignment with the ISO/IEC 27001 standard, components that have regulatory or compliance impacts are well-designated, documented, and protected
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?		X		
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Ifin Sistemi icludes procedures to managing antivirus / malicious software in the training, in alignment with ISO/IEC 27001 standard
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files) .	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Ifin Sistemi is ISO/IEC 27001 compliant based on ISO/IEC 27002 controls. There is a list of applications that can be used by mobile devices for access to company resources, limited to access to groupware services
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			
		IPY-03.2		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?			X	Service application of Ifin Sistemi is offered as a SaaS service. Tenants do not have the ability to introduce or manage virtual machines in the this environment
		IPY-03.3		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			More information about building integrations and consuming the Ifin Sistemi APIs is available on technical manual documentation
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Interactions with the Ifin Sistemi's application (e.g., API calls, login, etc.) are encrypted in transit
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			SaaS platform uses qualified CSP IaaS for virtualization
		IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?			X	Service application of Ifin Sistemi is offered as a SaaS service. Tenants do not have the ability to introduce or manage virtual machines in the this environment
		IPY-05.3		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			X	Tenants do not interact with our products at the hypervisor or server infrastructure

Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			Ifin Sistemi icludes procedures to managing antivirus / malicious software in the training, in alignment with ISO/IEC 27001 standard
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			Ifin Sistemi is ISO/IEC 27001 compliant based on ISO/IEC 27002 controls. There is a list of applications that can be used by mobile devices for access to company resources, limited to access to groupware services
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	X			Acceptable use policy prohibits the installation of non-approved applications. Are enforced minimal controls on employee mobile devices
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	BYOD is not permitted to connect to customer environments or to store customer data
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			In alignment with the certified ISO/IEC 27001 Standard. Part of the acceptable use policy
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?		X		
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?		X		
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	X			BYOD is not permitted to connect to customer environments or to store customer data
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			Asset inventory with the ownership of the assets is updated and reviewed regularly, in accordance with the ISO/IEC 27001 standard
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			A specific policy about use of corporate mobile DEVICES exists, is implemented and communicated to all employees, in according with clauses and controls requirements ISO/IEC 27001. There are some minimal checks on employees' mobile devices
Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?		X		A specific policy about use of corporate mobile devices exists, is implemented and communicated to all employees, in according with clauses and controls requirements ISO/IEC 27001. Sensitive data is not permitted on mobile devices
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			Circumvention of built-in security controls is prohibited in the Acceptable Use policy
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?		X		Generally, Laptops includes the preventative controls but mobile phones don't
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X	BYOD is not permitted to connect to customer environments or to store customer data

		MOS-13.2	BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	X			On corporate mobile devices are in place policy and device management
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X	
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	X			Policy specifies that automatic/regural updates must be enabled
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X	BYOD is not permitted to connect to customer environments or to store customer data
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			X	
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X	
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			Ifin Sistemi uses remote wipe on corporate mobile devices
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	X			
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	X			
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X	BYOD is not permitted to connect to customer environments or to store customer data
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X	
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			Ifin Sistemi maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO/IEC 27001 standard
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			Ifin Sistemi maintains procedures and contacts
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	X			Ifin Sistemi has an incident response program, plans and procedures have been developed in alignment with ISO/IEC 27001 standard

		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X		Generally, tenant involvement is not necessary.The terms of service cover roles and responsibilities. When a security incident is identified, security team immediately begin investigating to identify, track, communicate, and resolve the root cause of the incident. Security issues are communicated in accordance with appropriate confidentiality methods
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			The organization of Ifin Sistemi, ensure that all employees understand their responsibilities and obligations related to security events. The supplier who are processing personal data are subject to specific documented confidentiality/ non-disclosure agreements
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Default channel adopted are: PEC and Trouble Ticketing System
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			Ifin Sistemi can support valid request for specific tenant data from law enforcement. Ifin Sistemi with "LEGAL ARCHIVE" service offered is "Conservatore Accreditato" AgID, standard and applicabile regulatory requirements
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			From the snapshot the environment can be created for forensic purposes where focus can be one tenant only
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?		X		Multi-tenancy SaaS architecture. Data are separated via unique data keys
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			All Information security incidents are recorded and analyzes to determine impact, cause and opportunities for corrective action
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	X			Upon request or contract obligation, Ifin Sistemi can provide statistical information about security metrics and security incidents
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	X			The ISO/IEC 27001 compliance certification of Ifin Sistemi demonstrates the controls in place to provide a secure service application including controls related to supply chain
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			

Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			In alignment with the certified ISO/IEC 27001 and internal procedure, information about security incidents (if any) is communicated in accordance with appropriate confidentiality methods: directly via email or in-product notifications
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Ifin Sistemi manages capacity and utilization data in alignment with ISO/IEC 27001 standard
		STA-03.2		Do you provide tenants with capacity planning and use reports?		X		Ifin Sistemi is a SaaS platform; capacity planning and usage reports are for internal use ony or upon request
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Ifin Sistemi performs periodic indipendent reviews and assessments to verify compliance with policies, procedures, standard and applicabile regulatory requirements
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Ifin Sistemi for the SaaS platform uses only one qualified CSP Infrastructure. Ifin Sistemi does not generally outsource development. However, agreements with any sub-processors are subject to all applicable laws and regulations
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			
		STA-05.3		Does legal counsel review all third-party agreements?	X			
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			In alignment with the certified ISO/IEC 27001 Ifin Sistemi ensures that appropriate security and privacy are in place
		STA-05.5		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Multi-tenancy SaaS architecture. Data recovery is done for the whole application. Ifin Sistemi implements redundancy mechanism in its systems to prevent permanent data loss
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Ifin Sistemi implements the service on qualified CSP infrastructure with primary site in Italy and secondary site in other European Community countries
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	X			Primary tenants data is stored in datacenter located in italy; Secondary datacenter is located in Europe region
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			
		STA-05.9		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X		Tenants are not allowed to choose the geographical location
		STA-05.10		Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Data breach procedure is in place within the GDPR compliance system. Privacy Policy is aligned with industry and country requirements and is continuously monitored for update

		STA-05.11	portability requirements for application development and information exchange, usage, and integrity persistence	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		Ifin Sistemi has a formal access control policy that is reviewed and updated annually. Ifin Sistemi has been validated and certified by an independent auditor to confirm alignment with ISO/IEC 27001. Ifin Sistemi may access tenant data only if requested by tenant for support purposes. Tenant data doesn't collects for inspection technologies. Also refer to Privacy Policy documentation and System maintenance procedures document
		STA-05.12		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		In alignment with the certified ISO/IEC 27001, Ifin Sistemi maintains all required subprocessing agreements and makes them available to clients upon request.
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	X			Ifin Sistemi maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. In addition, Ifin Sistemi has selected Aruba SpA as a qualified cloud provider because of the compliance ISO/IEC 27001 and many other security standards
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			In alignment with the certified ISO/IEC 27001, Ifin Sistemi maintains formal agreements with third party suppliers and those agreements are reviewed periodically and updated as needed are. The customer terms of services are reviewed and updated as needed are
		STA-07.2	The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X			Ifin Sistemi ensures that its supply chain is regulated by the required contractual requirements. The security policy can provide on-site inspections, if necessary, to confirm compliance
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Ifin Sistemi makes avaible on request to its customers performace report of SLA
		STA-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?		X		
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			Ifin Sistemi makes avaible on request to its customers performace report of SLA
		STA-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	X			Ifin Sistemi data management policies are in alignment with ISO/IEC 27001 standard. Most potential confilcts of interest would be handled through contractual agreements while service level conflicts of interest would be resolved via operational management
		STA-07.8		Do you review all service level agreements at least annually?	X			
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			In alignment with the certified ISO/IEC 27001, Ifin Sistemi maintains formal agreements with third party suppliers and those agreements are reviewed periodically and updated as needed are
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?		X		Currently, qualified CSP is the only provider on which the Ifin Sistemi's service application depend on

Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			On request
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			Ifin Sistemi uses independent third party to perform penetration tests and audit security hardening practices
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	X			In alignment with the certified ISO/IEC 27001 standard, Ifin Sistemi has anti-malware installed on virtual machines
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X			Updates are in place for new malware or virus signatures
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Authorized technical staff, periodically checks the operating systems software applications installed. The vulnerabilities are scanned and the necessary patches applied, as well as system updates. The services are exposed only in the connectivity ports essential for use to reduce the attack surface. All this in line with the ISO/IEC 27001 standard and annexed controls
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			Ifin Sistemi collaborates with third-party penetration testing vendors recognized by the industry to perform regular penetration tests against the application layer
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			In alignment with the certified ISO/IEC 27001, Ifin Sistemi has defined and implemented a change management policy and procedure
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	X			The results of the vulnerability tests are used internally; tenants can request the report under NDA
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			In alignment with the certified ISO/IEC 27001 standard, Ifin Sistemi follow security feeds for emerging threats and monitors upcoming patches continuously. Ifin Sistemi maintains and updates at the server istance and package level to meet internal compliance measures, in accordance with the criticality of the risks evaluated
		TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X			A typical and rational division of responsability (terms of service)
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations,	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	No mobile code in use in the service
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	