IFS Cloud - Statement of Applicability - ISO 27001:2013

Control Applicability									Control Implementation Documents	
Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.5	**Information Security Policy**	A.5.1	Management direction for information security	A.5.1.1	**Policies for information security** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	**Yes**	**Yes**	Corporate	IFS Cloud Information Security Policy	IFS Cloud Information Security Policy
A.5	**Information Security Policy**	A.5.1	Management direction for information security	A.5.1.2	**Review and evaluation** The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	**Yes**	**Yes**	Corporate	IFS Cloud Information Security Policy	IMS Document Management Process
A.6	**Organisation of Information Security**	A.6.1	Internal organisation	A.6.1.1	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.	**Yes**	**Yes**	Corporate	IFS Cloud Information Security Policy	IFS Cloud ISMS Framework
A.6	**Organisation of Information Security**	A.6.1	Internal organisation	A.6.1.2	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	**Yes**	**Yes**	Cloud	IFS Information Security Strategy.	IFS Cloud ISMS Framework IFS Cloud Operational Change Management Change Management Process (CoS KB)
A.6	**Organisation of Information Security**	A.6.1	Internal organisation	A.6.1.3	**Contact with authorities** Appropriate contacts with relevant authorities shall be maintained.	**Yes**	**Yes**	Cloud	IFS Contact with Authorities	IFS Cloud ISMS Framework IFS Cloud Interested Parties Requirements and Communications Matrix
A.6	**Organisation of Information Security**	A.6.1	Internal organisation	A.6.1.4	**Contact with special interest groups** Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	**Yes**	**Yes**	Cloud	IFS Contact with Authorities	IFS Cloud Special Interest Groups Log
A.6	**Organisation of Information Security**	A.6.1	Internal organisation	A.6.1.5	**Information security in project management** Information security shall be addressed in project management, regardless of the type of the project.	**Yes**	**Yes**	Cloud	CPO PMO Page - My IFS	CoS PMO End 2 End Process. CoS PID Template. Solution Design Template.
A.6	**Organisation of Information Security**	A.6.2	Mobile devices and teleworking	A.6.2.1	**Mobile device policy** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	**Yes**	**Yes**	Corporate	IFS Cloud Information Security Policy IFS IT Equipment Policy	IFS Corporate Information Security Framework – All Employees
A.6	**Organisation of Information Security**	A.6.2	Mobile devices and teleworking	A.6.2.2	**Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	**Yes**	**Yes**	Corporate	IFS Home Working Policy	IFS Corporate Information Security Framework – All Employees
A.7	**Human Resource Security**	A.7.1	Prior to employment	A.7.1.1	**Screening** Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	**Yes**	**Yes**	Corporate	HR / Personnel Policy	IFS Employee Onboarding Process (by region)
A.7	**Human Resource Security**	A.7.1	Prior to employment	A.7.1.2	**Terms and conditions of employment** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	**Yes**	**Yes**	Corporate	HR / Personnel Policy	IFS Employment Terms and Conditions
A.7	**Human Resource Security**	A.7.2	During employment	A.7.2.1	**Management responsibilities** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	**Yes**	**Yes**	Cloud	IFS Cloud ISMS Framework	IFS Employee Handbook IFS Employment Terms and Conditions IFS Corporate Information Security Framework – All Employees IFS Non-Disclosure Agreement
A.7	**Human Resource Security**	A.7.2	During employment	A.7.2.2	**Information security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	**Yes**	**Yes**	Cloud	Information Security Awareness Training Policy	IFS Cloud Information Security Awareness Training Plan

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.7	**Human Resource Security**	A.7.2	During employment	A.7.2.3	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	**Yes**	**Yes**	Corporate	Disciplinary Policy	IFS Employee Handbook IFS Employment Terms and Conditions
A.7	**Human Resource Security**	A.7.3	Termination and change of employment	A.7.3.1	**Termination or change of employment responsibilities** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	**Yes**	**Yes**	Corporate	HR / Personnel Policy	IFS Onboarding Processes (by region) IFS Leavers Process (by region)
A.8	**Asset Management**	A.8.1	Responsibility for assets	A.8.1.1	**Inventory of assets** Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	**Yes**	**Yes**	Cloud	IFS IT Equipment Policy	IFS Local IT Asset Management Process
A.8	**Asset Management**	A.8.1	Responsibility for assets	A.8.1.2	**Ownership of assets** Assets maintained in the inventory shall be owned.	**Yes**	**Yes**	Cloud	IFS IT Equipment Policy	IFS Local IT Asset Management Process
A.8	**Asset Management**	A.8.1	Responsibility for assets	A.8.1.3	**Acceptable Use of Assets** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	**Yes**	**Yes**	Cloud	IFS IT Equipment Policy IFS Shadow IT Policy	IFS Corporate Information Security Framework - All Employees
A.8	**Asset Management**	A.8.1	Responsibility for assets	A.8.1.4	**Return of assets** All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	**Yes**	**Yes**	Cloud	IFS IT Equipment Policy	IFS Employee Leavers Process (by region)
A.8	**Asset Management**	A.8.2	Information classification	A.8.2.1	**Classification of information** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	**Yes**	**Yes**	Cloud	IFS Information Classification and Handling Policy	IFS Information Classification and Handling Policy
A.8	**Asset Management**	A.8.2	Information classification	A.8.2.2	**Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	**Yes**	**Yes**	Cloud	IFS Information Classification and Handling Policy	IFS Information Classification and Handling Policy Transfer & Handling of Sensitive Customer Data Policy
A.8	**Asset Management**	A.8.2	Information classification	A.8.2.3	**Handling of assets** Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	**Yes**	**Yes**	Cloud	IFS Information Classification and Handling Policy	IFS Corporate Information Security Framework - All Employees
A.8	**Asset Management**	A.8.3	Media handling	A.8.3.1	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	**Yes**	**Yes**	Cloud	IFS Shadow IT Policy IFS IT Equipment Policy	IFS Corporate Information Security Framework - All Employees
A.8	**Asset Management**	A.8.3	Media handling	A.8.3.2	**Disposal of media** Media shall be disposed of securely when no longer required, using formal procedures.	**Yes**	**Yes**	Cloud	IFS Secure Disposal of Storage Media	IFS Secure Disposal of Storage Media
A.8	**Asset Management**	A.8.3	Media handling	A.8.3.3	**Physical media transfer** Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	**No**	**No**	n/a	n/a	n/a
A.9	**Access Control**	A.9.1	Business requirements of access control	A.9.1.1	**Access control policy** An access control policy shall be established, documented and reviewed based on business and information security requirements.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS Access Control Policy
A.9	**Access Control**	A.9.1	Business requirements of access control	A.9.1.2	**Access to networks and network services** Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS Employee Onboarding Process IFS User Access Control Policy
A.9	**Access Control**	A.9.2	User access management	A.9.2.1	**User registration and deregistration** A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS Employee Onboarding Process IFS Employee Leaver Process IFS User Access Control Policy
A.9	**Access Control**	A.9.2	User access management	A.9.2.2	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS User Access Control Policy

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.9	**Access Control**	A.9.2	User access management	A.9.2.3	**Management of privileged access rights** The allocation and use of privileged access rights shall be restricted and controlled.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS User Access Control Policy
A.9	**Access Control**	A.9.2	User access management	A.9.2.4	**Management of secret authentication information of users** The allocation of secret authentication information shall be controlled through a formal management process.	**Yes**	**Yes**	Cloud	IFS User Access Control Policy Secured Information Handling Policy	How to Get Passwords from Azure Vault
A.9	**Access Control**	A.9.2	User access management	A.9.2.5	**Review of user access rights** Asset owners shall review users' access rights at regular intervals.	**Yes**	**Yes**	Corporate	IFS Access Control Policy	Access Review Process (KBA)
A.9	**Access Control**	A.9.2	User access management	A.9.2.6	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS Employee Offboarding Process IFS Employee Movers Process
A.9	**Access Control**	A.9.3	User responsibilities	A.9.3.1	**Use of secret authentication information** Users shall be required to follow the organization's practices in the use of secret authentication information.	**Yes**	**Yes**	Corporate	IFS User Access Control Policy Secured Information Handling Policy	IFS Corporate Information Security Framework – All Employees
A.9	**Access Control**	A.9.4	System and application access control	A.9.4.1	**Information access restriction** Access to information and application system functions shall be restricted in accordance with the access control policy.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	Information Classification Policy IFS User Access Control Policy
A.9	**Access Control**	A.9.4	System and application access control	A.9.4.2	**Secure log-on procedures** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	**Yes**	**Yes**	Corporate	IFS Access Control Policy	IFS User Access Control Policy
A.9	**Access Control**	A.9.4	System and application access control	A.9.4.3	**Password management system** Password management systems shall be interactive and shall ensure quality passwords.	**Yes**	**Yes**	Corporate	IFS Access Control Policy IFS User Access Control Policy	Cloud Knowledge Base Articles: How to Get Passwords from Azure Vault. Setting Up a Key Vault for HTTPS. Creating Key Vaults for Existing Customers. Creating Key Vaults for New Customer Environments.
A.9	**Access Control**	A.9.4	System and application access control	A.9.4.4	**Use of privileged utility programs** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	IFS Corporate Information Security Framework – All Employees
A.9	**Access Control**	A.9.4	System and application access control	A.9.4.5	**Access control to program source code** Access to program source code shall be restricted.	**Yes**	**Yes**	Cloud	IFS Access Control Policy	Secure Application Development Process
A.10	**Cryptography**	A.10.1	Cryptographic controls	A.10.1.1	**Policy on the use of cryptographic controls** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	**Yes**	**Yes**	Cloud	IFS Cryptography Policy	IFS Cryptography Policy
A.10	**Cryptography**	A.10.1	Cryptographic controls	A.10.1.2	**Key management** A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	**Yes**	**Yes**	Cloud	IFS Cryptography Policy	IFS Cryptography Policy
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.1	**Physical security perimeter** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.2	**Physical entry controls** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.3	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and applied.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.4	**Protecting against external and environmental threats** Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.5	**Working in secure areas** Procedures for working in secure areas shall be designed and applied.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.11	**Physical and Environmental Security**	A.11.1	Secure areas	A.11.1.6	**Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.1	**Equipment siting and protection** Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.2	**Supporting utilities** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.3	**Cabling security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.4	**Equipment maintenance** Equipment shall be correctly maintained to ensure its continued availability and integrity.	**Yes**	**Yes**	Corporate	IFS Physical & Environmental Security Policy	IFS Physical Security (Regional/Site Procedures)
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.5	**Removal of assets** Equipment, information or software shall not be taken off-site without prior authorization.	**Yes**	**Yes**	Corporate	IFS IT Equipment Policy	IFS Home Working Policy IFS Corporate Information Security Framework – All Employees
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.6	**Security of equipment and assets off-premises** Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	**Yes**	**Yes**	Corporate	IFS IT Equipment Policy	IFS Home Working Policy IFS Corporate Information Security Framework – All Employees
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.7	**Secure disposal or reuse of equipment** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	**Yes**	**Yes**	Corporate	IFS IT Equipment Policy	Secure Disposal of Storage Media Process Cloud Offboarding Process
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.8	**Unattended user equipment** Users shall ensure that unattended equipment has appropriate protection.	**Yes**	**Yes**	Corporate	IFS IT Equipment Policy	IFS Corporate Information Security Framework – All Employees
A.11	**Physical and Environmental Security**	A.11.2	Equipment	A.11.2.9	**Clear desk and clear screen policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	**Yes**	**Yes**	Cloud	IFS Corporate Information Security Framework - All Employees	IFS Corporate Information Security Framework – All Employees
A.12	**Operations Security**	A.12.1	Operational procedures and responsibilities	A.12.1.1	**Documented operating procedures** Operating procedures shall be documented and made available to all users who need them.	**Yes**	**Yes**	Cloud	Cloud KB Document Management Process	Cloud KB Document Management Process Cloud Knowledge Base Articles ISMS Library Document Set IMS Document Control Process
A.12	**Operations Security**	A.12.1	Operational procedures and responsibilities	A.12.1.2	**Change Management** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	**Yes**	**Yes**	Cloud	Change Management Process (CoS KB)	IFS Cloud Operational Change Management IFS Cloud ISMS Framework IFS Support Portal GTO Process
A.12	**Operations Security**	A.12.1	Operational procedures and responsibilities	A.12.1.3	**Capacity management** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.1	Operational procedures and responsibilities	A.12.1.4	**Separation of development, testing and operational environments** Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.2	Protection from malware	A.12.2.1	**Controls against malware** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.12	**Operations Security**	A.12.3	Backup	A.12.3.1	**Information backup** Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	IFS Cloud Backup and Recovery Process
A.12	**Operations Security**	A.12.4	Logging and monitoring	A.12.4.1	**Event logging** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.4	Logging and monitoring	A.12.4.2	**Protection of log information** Logging facilities and log information shall be protected against tampering and unauthorized access.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.4	Logging and monitoring	A.12.4.3	**Administrator and operator logs** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.4	Logging and monitoring	A.12.4.4	**Clock synchronisation** The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.5	Control of operational software	A.12.5.1	**Installation of software on operational systems** Procedures shall be implemented to control the installation of software on operational systems.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process IFS Support Portal GTO Process
A.12	**Operations Security**	A.12.6	Technical vulnerability management	A.12.6.1	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	**Yes**	**Yes**	Cloud	IFS Cloud Security Testing Policy	Cloud Operations Security Process
A.12	**Operations Security**	A.12.6	Technical vulnerability management	A.12.6.2	**Restrictions on software installation** Rules governing the installation of software by users shall be established and implemented.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Cloud Operations Security Process IFS Corporate Information Security Framework – All Employees
A.12	**Operations Security**	A.12.7	Information systems audit considerations	A.12.7.1	**Information systems audit controls** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	**Yes**	**Yes**	Cloud	IFS Security in Operations Policy	Internal Audit Process
A.13	**Communications Security**	A.13.1	Network security management	A.13.1.1	**Network controls** Networks shall be managed and controlled to protect information in systems and applications.	**Yes**	**Yes**	Cloud	IFS Network and Communications Policy	Network Diagrams
A.13	**Communications Security**	A.13.1	Network security management	A.13.1.2	**Security of network services** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	**Yes**	**Yes**	Cloud	IFS Network and Communications Policy	Network Diagrams
A.13	**Communications Security**	A.13.1	Network security management	A.13.1.3	**Segregation in networks** Groups of information services, users and information systems shall be segregated on networks.	**Yes**	**Yes**	Cloud	IFS Network and Communications Policy	Network Diagrams
A.13	**Communications Security**	A.13.2	Information transfer	A.13.2.1	**Information transfer policies and procedures** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	**Yes**	**Yes**	Cloud	IFS Network and Communications Policy	Transfer and Handling of Sensitive Customer Data Policy
A.13	**Communications Security**	A.13.2	Information transfer	A.13.2.2	**Agreements on information transfer** Agreements shall address the secure transfer of business information between the organization and external parties.	**Yes**	**Yes**	Corporate	IFS Network and Communications Policy	Transfer and Handling of Sensitive Customer Data Policy
A.13	**Communications Security**	A.13.2	Information transfer	A.13.2.3	**Electronic messaging** Information involved in electronic messaging shall be appropriately protected.	**Yes**	**Yes**	Cloud	IFS Network and Communications Policy	IFS Information Security Framework - All Employees

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.13	**Communications Security**	A.13.2	Information transfer	A.13.2.4	**Confidentiality or nondisclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	**Yes**	**Yes**	Corporate	IFS Mutual NDAs and DPAs	IFS Mutual NDAs and DPAs
A.14	**System Acquistion, Development and Maintenance**	A.14.1	Security requirements of information systems	A.14.1.1	**Information security requirements analysis and specification** The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.1	Security requirements of information systems	A.14.1.2	**Securing application services on public networks** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.1	Security requirements of information systems	A.14.1.3	**Protecting application services transactions** Information involved in application service transactions shall be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.1	**Secure development policy** Rules for the development of software and systems shall be established and applied to developments within the organization.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.2	**System change control procedures** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.3	**Technical review of applications after operating platform changes** When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Cloud Operational Change Management
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.4	**Restrictions on changes to software packages** Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Cloud Operational Change Management
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.5	**Secure system engineering principles** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.6	**Secure development environment** Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.	**Yes**	**Yes**	Cloud	IFS Secure Application Development Process	IFS Secure Application Development Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.7	**Outsourced development** The organization shall supervise and monitor the activity of outsourced system development.	**No**	**No**	n/a	n/a	n/a
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.8	**System security testing** Testing of security functionality shall be carried out during development.	**Yes**	**Yes**	Cloud	IFS Cloud Security Testing Policy	IFS Support Portal GTO Process
A.14	**System Acquistion, Development and Maintenance**	A.14.2	Security in development and support processes	A.14.2.9	**System acceptance testing** Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	**Yes**	**Yes**	Cloud	IFS Cloud Security Testing Policy	IFS Support Portal GTO Process
A.14	**System Acquistion, Development and Maintenance**	A.14.3	Test data	A.14.3.1	**Protection of test data** Test data shall be selected carefully, protected and controlled.	**No**	**No**	n/a	n/a	n/a

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.15	**Supplier Relationships**	A.15.1	Information security in supplier relationships		**Information security policy for supplier relationships** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	**Yes**	**Yes**	Corporate	IFS Third Party Security Policy IFS Procurement Policy	IFS Supplier Standard TCs
A.15	**Supplier Relationships**	A.15.1	Information security in supplier relationships	A.15.1.2	**Addressing security within supplier agreements** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide Technology infrastructure components for, the organization's information.	**Yes**	**Yes**	Corporate	IFS Third Party Security Policy IFS Procurement Policy	IFS Supplier Standard TCs
A.15	**Supplier Relationships**	A.15.1	Information security in supplier relationships	A.15.1.3	**Information and communication technology supply chain** Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	**Yes**	**Yes**	Corporate	IFS Third Party Security Policy IFS Procurement Policy	IFS Supplier Standard TCs
A.15	**Supplier Relationships**	A.15.2	Supplier service delivery management	A.15.2.1	**Monitoring and review of supplier services** Organizations shall regularly monitor, review and audit supplier service delivery.	**Yes**	**Yes**	Corporate	IFS Third Party Security Policy IFS Procurement Policy	Cloud Supplier Register
A.15	**Supplier Relationships**	A.15.2	Supplier service delivery management	A.15.2.2	**Managing changes to supplier services** Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	**Yes**	**Yes**	Corporate	IFS Third Party Security Policy IFS Procurement Policy	Cloud Supplier Register
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.1	**Responsibilities and procedures** Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.2	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.3	**Reporting information security weaknesses** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.4	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.5	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.6	**Learning from information security incidents** Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	**Yes**	**Yes**	Corporate	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.16	**Information Security Incident Management**	A.16.1	Management of information security incidents and improvements	A.16.1.7	**Collection of evidence** The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	**Yes**	**Yes**	Cloud	IFS Information Security Incident Management Policy. IFS Cloud Incident Management Policy.	IFS Reporting Information Security Weaknesses and Events. IFS Management of Information Security Incidents and Improvements. IFS Security Incident Escalation Process. IFS Breach Notification. IFS Cloud Incident Management Process
A.17	**Information Security Aspects of Business Continuity Management**	A.17.1	Information security continuity	A.17.1.1	**Planning information security continuity** The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	**Yes**	**Yes**	Cloud	IFS Business Continuity Policy	IFS Business Continuity Plan IFS Cloud Backup and Recovery Process
A.17	**Information Security Aspects of Business Continuity Management**	A.17.1	Information security continuity	A.17.1.2	**Implementing information security continuity** The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	**Yes**	**Yes**	Cloud	IFS Business Continuity Policy	IFS Business Continuity Plan IFS Cloud Backup and Recovery Process
A.17	**Information Security Aspects of Business Continuity Management**	A.17.1	Information security continuity	A.17.1.3	**Verify, review and evaluate information security continuity** The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	**Yes**	**Yes**	Cloud	IFS Business Continuity Policy	IFS Business Continuity Plan
A.17	**Information Security Aspects of Business Continuity Management**	A.17.2	Redundancies	A.17.2.1	**Availability of information processing facilities** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	**Yes**	**Yes**	Cloud	IFS Business Continuity Policy	IFS Business Continuity Plan IFS Cloud Backup and Recovery Process
A.18	**Compliance**	A.18.1	Compliance with legal and contractual requirements	A.18.1.1	**Identification of applicable legislation and contractual requirements** All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	**Yes**	**Yes**	Corporate	IFS Cloud ISMS Framework	Data Processing Addendum (Template)
A.18	**Compliance**	A.18.1	Compliance with legal and contractual requirements	A.18.1.2	**Intellectual property rights** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	**Yes**	**Yes**	Corporate	IFS Cloud ISMS Framework	IFS Cloud ISMS Framework
A.18	**Compliance**	A.18.1	Compliance with legal and contractual requirements	A.18.1.3	**Protection of records** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	**Yes**	**Yes**	Corporate	Data Protection Policy	Retention of HR Records Process Control of ISMS Records Process Information Security Management document - Cloud Section
A.18	**Compliance**	A.18.1	Compliance with legal and contractual requirements	A.18.1.4	**Privacy and protection of personally identifiable information** Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	**Yes**	**Yes**	Corporate	Data Protection Policy	IFS Personal Information Management Standard
A.18	**Compliance**	A.18.1	Compliance with legal and contractual requirements	A.18.1.5	**Regulation of cryptographic controls** Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	**Yes**	**Yes**	Corporate	Cryptography Policy	Cryptography Policy

Control Ref.	Category	Control Sub-Ref.	Sub-Category	Control No.	ISO Control Details	Applicable	Implemented	Scope Coverage (Cloud or Corporate)	IFS ISMS Policy	IFS ISMS Document(s)
A.18	**Compliance**	A.18.2	Information security reviews	A.18.2.1	**Independent review of information security** The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	**Yes**	**Yes**	Cloud	IFS Cloud ISMS Framework	IFS Cloud Internal Audit Process IFS Cloud Internal Audit Schedule URM ISO 27001 Risk Assessment Report - IFS - January 2020
A.18	**Compliance**	A.18.2	Information security reviews	A.18.2.2	**Compliance with security policies and standards** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	**Yes**	**Yes**	Cloud	IFS Cloud ISMS Framework	Cloud Security Board Minutes (Monthly) Information Security Board Minutes (Monthly) Management Review Agenda (Annually)
A.18	**Compliance**	A.18.2	Information security reviews	A.18.2.3	**Technical compliance review** Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	**Yes**	**Yes**	Cloud	IFS Cloud ISMS Framework	IFS Cloud Internal Audit Process IFS Internal IT Audit Process