Version: 1 Updated: 08/08/2023	IFS ISMS: Statement of Applicability - ISO 27001:2022 Information security controls					
Section	**Information Security Control**	**Control Description**	**Applicability**	**Control Implementation**		
				Implementation Description	**Implementing Dept.**	**Applicable Policy/Procedure**
A5	**Organizational Controls**					
A.5.1	Policies for information security	Information security policy for topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by the relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Applicable	IFS have developed a suite of information security policies, each with ownership and authorisation, and which are made available to all employees and external parties as applicable.	CoS - Security	IFS Information Security Policy
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organisational needs.	Applicable	Roles and responsibilities in relation to the ISMS are defined within information security policies.	CoS - Security	IFS Cloud ISMS Framework
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Applicable	Achieved through using a separate and dedicated security governance team employed within the organisation. Segregation of duties related to in scope services is achieved through different specialist functions within the operational chain and through consultation with customers (e.g. case management, change management).	CoS - Security	IFS Cloud ISMS Framework
A.5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.	Applicable	Management responsibilities in relation to the ISMS are defined within information security policies. General responsibilities towards information security controls are also defined within job descriptions, contracts of employment and are further communicated through information security awareness training.	CoS - Security	IFS Cloud ISMS Framework
A.5.5	Contact with authorities	The organisation shall establish and maintain contact with relevant authorities.	Applicable	Contact with authorities for is handled by specialist teams such as Legal and appropriate escalation routes are in place. This process is linked to IFS incident management and response processes as appropriate.	Legal	IFS Cloud ISMS Framework
A.5.6	Contact with special interest groups	The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Applicable	The Corporate Services team maintain appropriate contact with information security special interest groups and have access to regular updates concerning changing information security trends and threats.	CoS - Security	IFS Cloud ISMS Framework
A.5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Applicable	Internal security teams subscribe to vendor resources that provide information on security vulnerabilities, threats, alerts and remediation activities.	CoS - Security Unified Support - SOC	SOC Documentation
A.5.8	Information security in project management	Information security shall be integrated into project management.	Applicable	Security requirements are raised as part of the project lifecycle as appropriate. Projects may be security-based in nature so as to implement or improve specific security controls within the organisation.	Unified Support - PMO	Project Management Cycle
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Applicable	An inventory of assets detailing asset type, asset information and ownership is in place at a global level and managed by local IT teams as appropriate. Service-based assets (such as cloud environments) are created, managed and maintained by the Unified Support function.	CoS - IT Unified Support	IFS IT Equipment Policy
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Applicable	The IFS Corporate Information Security Framework – All Employees document contains a set of acceptable use policy statements.	CoS - IT	IFS IT Equipment Policy IFS Corporate Information Security Framework – All Employees
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.	Applicable	Policies and processes are in place for the full asset lifecycle, including the return of assets. This is managed via global processes conducted by local IT teams with respect to IFS corporate assets.	CoS - IT	IFS IT Equipment Policy IFS Corporate Information Security Framework – All Employees
A.5.12	Classification of information	Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity and availability and relevant interested party requirements.	Applicable	Information classification is defined within a topic-specific security policy. Classification, handling and use of information is defined related to organisational information assets.	CoS - Security	IFS Information Management Policy
A.5.13	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 organisation.	Applicable	Information classification is defined within a topic-specific security policy. Classification, handling and use of information is defined related to organisational information assets.	CoS - Security	IFS Information Management Policy
A.5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.	Applicable	Information transfer controls are managed through signed data processing agreements with customers. Security policies are in place to govern how information shall be managed over network connections.	CoS - IT	IFS Network and Communications Policy
A.5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Applicable	Policies governing logical access control detail information security requirements for access management across the organisation. Role-based Active Directory access groups are managed by the Corporate Services Identity team. Physical access is managed by IFS Facilities Management teams on a global level.	CoS - IT Facilities Management	IFS Access Control Policy
A.5.16	Identity management	The full cycle of identifies shall be managed.	Applicable	Each IFS employee is setup with a corporate identity within Active Directory which allows or restricts access based on the employee's role and the use of access groups. This is managed by the Corporate Services Identity team. Access to cloud service resources is managed by the Unified Support function who determine the appropriate levels of access for service and support teams.	CoS - IT Unified Support	IFS Access Control Policy
A.5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Applicable	User access provisioning processes ensure authentication information is appropriately managed. Cloud service operations use the Azure key vault for the management of both customer and internal passwords. Creation is done through automation upon creation of new customer environment. This can also be performed manually. Handling of authentication information is defined within security policies.	CoS - IT Unified Support	IFS Access Control Policy

A.5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on rules for access control.	Applicable	A combination of onboarding, mover and leaver processes in place ensure that access rights are appropriately managed within the employment lifecycle. Quarterly access reviews and AD access group verifications are performed. Role based access control (RBAC) and privileged identity management (PIM) is applied for cloud service operations.	CoS - IT Unified Support	IFS Access Control Policy
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Applicable	Policies and processes for the procurement of new suppliers and existing suppliers are in place and are managed by the Procurement function. Such policies include third-party security requirements.	Procurement	IFS Global Procurement Policy
A.5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Applicable	Wherever possible an IFS contract is used for supplier agreements. However if a supplier provided contract has to be used then the clauses are negotiated to ensure they cover all IFS's requirements. The standard IFS contract has standard clauses concerning such areas as confidential data and associated security requirements. A right to audit is also included in the standard contract template.	Procurement	IFS Global Procurement Policy
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Applicable	A standard IFS contract has a schedule detailing sub-contractual arrangements. Outsourced services will be managed by an IFS owner who is responsible for managing the supply-chain. IFS cloud services typically subcontract services related to project work where a Statement of Work (SOW) will be provided by the supplier. Periodic reviews will take place depending on the requirements of the project until work is complete.	CoS - IT Unified Support - PMO	IFS Global Procurement Policy
A.5.22	Monitoring, review and change management of supplier services	The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Applicable	Policies and processes detailing supplier management, review and change have been defined.	Procurement	IFS Global Procurement Policy
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.	Applicable	A policy for the procurement, use of and exit from cloud and cloud computing services is in effect.	CoS - Security Unified Support - SOC Procurement	IFS Corporate Cloud Computing Policy IFS Cloud Network Security Standard
A.5.24	Information security incident management planning and preparation	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Applicable	Incident management and response policies and procedures are defined and implemented within the organisation covering both corporate and service-based elements. Internal Security Operations Centre teams are responsible for planning actions to identify, contain and resolve security-based incidents. Incident playbooks and strategies have been developed in order to deal with known or suspected threats.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A.5.25	Assessment and decision on information security events	The organisation shall assess information security events and decide if they are to be categorised as information security incidents.	Applicable	Incident management procedures include the assessment and decision of identified information security events, including severity ratings and prioritisation.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A.5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Applicable	Incident management procedures include incident response techniques, including defined time KPIs and strategies documented in the form of playbooks.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Applicable	Incident management procedures include event and incident monitoring , trending, problem management techniques and root cause analysis. This contributes to effective corrective actions being applied in order to mature related security controls and minimise recurring events.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A.5.28	Collection of evidence	The organisation shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Applicable	Internal Security Operations Centre (SOC) teams are responsible for the collection of evidence for potential use in legal and regulatory cases. Adequate evidence is gathering and documented within IFS Incident Reports. Appropriate ITSM tools are used to extract necessary information.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A.5.29	Information security during disruption	The organisation shall plan how to maintain information security at an appropriate level during a disruption.	Applicable	Various security considerations are built into playbook templates and information security control considerations are in place within IFS's core service operations. Playbooks have also been tested using third party resources to perform incident response simulations.	CoS - Security CoS - IT Unified Support - SOC	IFS Business Continuity Policy
A.5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Applicable	IFS ensures that all internal critical systems are appropriately backed up and protected in the event of a disruption to the business and/or its services. The cloud platform and service has built-in resilience with a primary/secondary data centre model in place allow failover should a major issue occur at either data centre.	CoS - IT Unified Support	IFS Business Continuity Policy
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date.	Applicable	The IFS Legal team is responsible for identifying applicable legislation and regulations for all markets that they operate in. A suite of legal documentation covering specific geographic regions has been developed, including customer contract templates. A legal register is in place which details specific legislative requirements with respect to IFS's service operations.	Legal	IFS Cloud ISMS Framework
A.5.32	Intellectual property rights	The organisation shall implement appropriate procedures to protect intellectual property rights.	Applicable	Clauses related to intellectual property rights (IPR) of the organisation are present within employment contracts. The Legal team are responsible for managing specific IPR issues working with the appropriate IFS internal functions.	Legal	IFS Cloud ISMS Framework
A.5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	Applicable	The Legal function is responsible for managing the protection of records in line with legislative, regulatory, contractual and business requirements. The HR function is responsible for the protection of employee records. The Security function is responsible for the protection of records that relate to the management of the Information Security Management System (ISMS) and other security compliance requirements.	Applicable in scope functions	IFS HR Records Retention Policy
A.5.34	Privacy and protection of personal identifiable information (PII)	The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Applicable	Policies and procedures are in place to define the requirements for protecting personally identifiable information and detail the processing that is undertaken on personal data.	Legal - Privacy CoS - Security	IFS Data Protection Policy IFS Employee Privacy Policy

A.5.35	Independent review of information security	The organisation's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Applicable	The CoS Compliance team conduct internal audit activities on the implemented security controls of other departments providing an independent assessment from that of operational teams. The internal audit schedule covers all ISO 27001 control and clause requirements. Furthermore, various external security assessments are performed on IFS on an annual basis, including both technical and compliance based reviews.	CoS - Security	IFS Cloud ISMS Framework
A.5.36	Compliance with policies, rules and standards for information security	Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Applicable	Internal audit activities are conducted on cloud implemented security controls by the CoS Compliance team. IFS Cloud Security Board meetings are held to review audit results, compliance status and to evaluate ISMS performance.	CoS - Security Unified Support - SOC	IFS Cloud ISMS Framework
A.5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Applicable	A documentation knowledge base is used as a document repository for standard operating procedures. This platform features controls for creation, review, approval and publishing of documents, and version control.	Applicable in scope functions	Applicable documentation
A6	**People Controls**					
A.6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Applicable	Screening processes are in place such as the completion of DBS checks and the use of third party services to complete pre-employment checks, right to work checks, background verification checks, etc. Senior management roles are subject to more stringent checks.	HR	IFS Recruitment Process
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.	Applicable	Standard employment terms and contracts are used. These include specific information security and confidentiality requirements	HR	IFS Employment Terms
A.6.3	Information security awareness, education and training	Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.	Applicable	All employees undergo formal training as part of their induction to the business, including an information security curriculum and role-based training as applicable. Annual mandatory training is in place for all employees within the organisation delivered through the IFS e-learning portal. Periodic Phishing simulations and tests are performed on new and existing employees.	HR	IFS Code of Conduct
A.6.4	Disciplinary process	A disciplinary process shall be formalised and communicated to take actions against the personnel and other relevant interested parties who have committed an information security policy violation.	Applicable	A global disciplinary policy is in effect. Regional disciplinary policies are implemented where there are specific legislative or regulatory requirements.	HR	IFS Global Disciplinary Policy
A.6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Applicable	Leavers are remined of their on-going security and confidentiality responsibilities during a termination interview. Such requirements are specified in standard employment terms and contracts.	HR	HR Leavers Process
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by the personnel and other relevant interested parties.	Applicable	Non Disclosure Agreements (NDAs) and/or confidentiality clauses are included in all customer, supplier, partner and employee agreements in place.	HR	IFS Employment Terms Associated NDA templates
A.6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	Applicable	A home-working policy is in effect which details how information security requirements should be maintained when staff are working remotely. Various technical security controls have been implemented by corporate IT services to protect against data loss.	HR CoS - IT	IFS Global Home Working Policy
A.6.8	Information security event reporting	The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Applicable	IFS documentation details how information security weaknesses and events should be reported by IFS employees. IFS Cloud services customers have access to report incidents via the IFS support portal.	CoS - Security Unified Support - SOC	IFS Information Security Incident Management Policy
A7	**Physical Controls**					
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Applicable	The Global Facilities function ensures that the appropriate physical perimeter controls are in place to a standard at all IFS facilities. Where IFS operate on a multi-tenanted location, agreements are in place with the landlord to fully-manage external security controls.	Facilities	IFS Physical Security Controls
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Applicable	External doors are access controlled and locked outside of working hours. Visitor processes are in place as appropriate.	Facilities	IFS Physical Security Controls
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Applicable	Offices are secured via building security controls managed by IFS Facilities personnel. Each IFS floor has security features in place to prevent access by unauthorised personnel.	Facilities	IFS Physical Security Controls
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorised physical access.	Applicable	All facilities have CCTV cameras in operation, both externally and internally. Only authorised personnel can access recordings. Main entry points are managed by dedicated reception staff.	Facilities	IFS Physical Security Controls
A.7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Applicable	IFS facilities in scope of certification do not have any significant external or environmental threats associated with them. This is determined and reviewed through a physical security risk assessment.	Facilities	IFS Physical Security Controls
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Applicable	Minimal secure areas exist within IFS facilities. Comms rooms feature access-controlled doors that are either electronically or key operated by authorised personnel only. Building utilities are also secured from unauthorised access.	Facilities	IFS Physical Security Controls
A.7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Applicable	IFS operates a near-paperless working environment. Equipment is in place to securely print and store physical information assets at IFS facilities. End user devices are safeguarded through a screen lock timer to minimise unauthorised access attempts if workstations are momentarily left unsupervised. IFS policies also stipulate the manual locking/storage of unattended devices.	Facilities CoS - IT	IFS Physical Security Controls IFS Corporate Information Security Framework – All Employees
A.7.8	Equipment siting and protection	Equipment shall be sited security and protected.	Applicable	Limited equipment is present within IFS facilities. Critical electronic equipment is located in secure, restricted access rooms.	Facilities	IFS Physical Security Controls
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	Applicable	Policies and procedures are in place to describe the measures that IFS employees and contractors should take to protect equipment and assets off-premises.	CoS - IT	IFS IT Equipment Policy

A.7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.	Applicable	IFS has policies in place to describe the acceptable use of storage media to employees and contractors associated with the classification of information stored on such devices. A Shadow IT Policy is in place detailing equipment or use-cases of equipment which are not permitted.	CoS - IT	IFS IT Equipment Policy IFS Shadow IT Policy
A.7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable	Comms rooms are fitted with air conditioning units as appropriate. UPS's are also in use to protect critical electronic systems/equipment.	Facilities	IFS Physical Security Controls
A.7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damaged.	Applicable	Cabling to comms rooms is secured. Underground cables terminate in the secure comms room and is only accessible to authorised Facilities and IT personnel.	Facilities	IFS Physical Security Controls
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Applicable	Air conditioning, CCTV, comms equipment, etc. are all periodically maintained by contracted services and/or building landlords. Permit to work process is in place.	Facilities	IFS Physical Security Controls
A.7.14	Secure disposal or re-use of equipment	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.	Applicable	The secure disposal process is used to dispose of unwanted or inoperable equipment, storage devices and other information assets.	CoS - IT	IFS IT Equipment Policy
A8	**Technological Controls**					
A.8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Applicable	Policies for the use of information assets and handling of information stored on IFS networks are in effect. Device encryption is used to ensure that information cannot be accessed without an IFS identity. Remote disablement of user devices is also implemented. Policy violations that are detected or reported are investigated and the appropriate action taken.	CoS - IT	IFS IT Equipment Policy IFS Corporate Information Security Framework – All Employees
A.8.2	Privileged access rights	The allocation and use or privileged access rights shall be restricted and managed.	Applicable	The CoS Identity team manage this across the organisation in providing secondary accounts with elevated permissions as required by some roles. The Unified Support teams utilise role-based access control (RBAC) and privileged identity management (PIM) processes to grant/revoke privileged access as it applies to service management and support responsibilities.	CoS - IT Unified Support - Engineering	IFS Access Control Policy
A.8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Applicable	Access provisioning processes are in place and is managed by the CoS Identity Team. Access permissions are based around using role-based access within Active Directory. Access to any other information or resources not applied as standard based on employee role needs to be requested and approved.	CoS - IT	IFS Access Control Policy
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Applicable	Program source code is only accessible to development staff within R&D. There is a clear segregation of responsibilities in place between the Unified Support teams who deploy product packages and Product Development teams who create/amend code.	R&D	R&D Secure Development Process
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Applicable	CoS Identity/Security teams set the standards for passwords/user accounts within IFS. Password/key vault processes within Azure Key Vault are used to manage cloud service related secrets and associated information.	CoS - IT Unified Support - Engineering	IFS Access Control Policy
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Applicable	Strategic and operational capacity management processes are in place.	Unified Support	Security in Operations Procedures
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Applicable	Anti-malware tools are present in the corporate environment and on all end users assets. IFS Cloud hosting environments have anti-malware in place.	CoS - Security Unified Support - SOC	Security in Operations Procedures
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Applicable	Threat and vulnerability details are received from vendors and special interest groups. Broadly vulnerabilities in the operating system and Oracle layers are responded to and appropriate patching applied. For the product layer all patches are included in releases. Customers are responsible for accepting or refusing patches applied by IFS. External penetration tests of major IFS product releases and supporting cloud infrastructure are conducted at least once annually.	CoS - Security Unified Support - SOC	Security in Operations Procedures
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Applicable	A configuration management database (CMDB) is used for both internal and customer-facing environments. Other specific IFS products and applications use various tools to manage deployments and other merges/changes. Access to these tools are restricted to the teams/roles who require them. IFS use hardware/software images to ensure consistent configurations are applied to devices and software..	CoS - IT Unified Support - Engineering	Security in Operations Procedures
A.8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Applicable	Record retention policies are applied in relation to business and regulatory records. Customer data hosted in cloud environments is a responsibility of the customer to manage, however upon succession of the customer contract/service IFS are able to perform deletion or transfer of customer data depending on their requirements.	Applicable in scope functions	Security in Operations Procedures
A.8.11	Data masking	Data masking shall be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Applicable	Techniques such as use of pseudonymisation/anonymisation, encryption, hashing, etc. are used in some areas of the business, mainly in order to safeguard personal identifiable information and records.	CoS - IT Legal HR	Security in Operations Procedures
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Applicable	DLP measures are deployed across internal IT systems (such as email) to alert security teams to any cases of data exfiltration. Security awareness training combined with phishing simulations further reduce the likelihood of data loss.	CoS - Security Unified Support - CSOC	Security in Operations Procedures
A.8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Applicable	Customer data backups are in place and managed for each cloud product offering with differing requirements. Backup retention and restoration targets vary by product.	Unified Support - Operations CoS - IT	Security in Operations Procedures
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Applicable	IFS follows an internal cloud strategy making use of cloud-based services, applications and integrations with IFS applications deployed in-house. IFS applications sold to customers are cloud-based and have resilience and redundancies built in to the service model.	Unified Support - Operations CoS - IT	Security in Operations Procedures

A.8.15	Logging	Logs that records activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Applicable	Cloud monitoring platforms are in place that log information and generate live alerts which are recorded and displayed within an event management dashboard. Alerts are managed through tickets which are assigned to engineers. Periodic reviews take place to identify trends and discuss events.	Unified Support - Engineering Unified Support - CSOC	Security in Operations Procedures
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Applicable	Various monitoring tools and platforms are in place to identify anomalous behaviour. Resolutions are driven through case management and problem management activities. The appropriate incident management and resolution procedures are applied to review, identify and correct any such events and incidents.	Unified Support - Engineering Unified Support - CSOC	Security in Operations Procedures
A.8.17	Clock synchronization	The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.	Applicable	IFS Cloud infrastructure clock synchronisation is part of the hosted service.	Unified Support - Engineering	Security in Operations Procedures
A.8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	Applicable	The CoS Identity team manage this across the organisation in providing secondary account with elevated permissions as required by some roles. The Unified Support Engineering team control the toolsets used by the Unified Support team and govern their access.	Unified Support - Engineering	Security in Operations Procedures
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Applicable	Approved software available to employees is managed within the Software Centre by the Corporate IT team. IFS employees do not have local admin rights to their IFS-issued hardware. A Go to Operations (GTO) process provides a controlled process for the deployment of IFS Cloud products into customer environments.	Unified Support - Engineering CoS - IT	Security in Operations Procedures
A.8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Applicable	Security Operations Centre (SOC) teams are responsible for security standards are implemented and followed. Internal IFS networks are monitored and maintained by the Network Operations Centre (NOC).	Unified Support - SOC CoS - Security CoS - IT	IFS Network and Communications Policy IFS Cloud Network Security Standard
A.8.21	Security of network services	Security mechanisms, service levels and service requirements for network services shall be identified, implemented and monitored.	Applicable	Unified Support manage the security of the cloud platform and customer environments, VMs, etc. and are responsible for ensuring that networks have appropriate security implemented. Microsoft are responsible for the network security of the Azure cloud environment. Security Operations Centre (SOC) teams are responsible for monitoring network services for anomalous behaviour and cyber threats.	Unified Support - SOC CoS - Security CoS - IT	IFS Network and Communications Policy IFS Cloud Network Security Standard
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organisation's networks.	Applicable	Appropriate segregation of customer environments is in place. Internal IFS Cloud networks are segregated from customer environments and managed by different SOC teams.	Unified Support - SOC CoS - Security CoS - IT	IFS Network and Communications Policy IFS Cloud Network Security Standard
A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Applicable	IFS uses a web proxy solution to filter out unwanted traffic on all internet facing servers.	CoS - IT	IFS Network and Communications Policy
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Applicable	Policies exist covering corporate and cloud cryptography requirements and information on the application of cryptographic controls.	Unified Support - Operations CoS - IT	IFS Cryptography Policy
A.8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Applicable	A 7-stage secure development process has been created and is controlled via the IFS R&D department who develop, package and supply products into the Unified Support team for them to be deployed within cloud-hosted environments on behalf of customers.	R&D	R&D Secure Development Process
A.8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Applicable	IFS applications are sufficiently hardened against security vulnerability through internal security assessments based on OWASP top 5 and further validated through external security scans run on each major product release.	R&D	R&D Secure Development Process
A.8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Applicable	A 7-stage secure development process has been created and is controlled via the IFS R&D department who develop, package and supply products into the Unified Support team for them to be deployed within cloud-hosted environments on behalf of customers.	R&D	R&D Secure Development Process
A.8.28	Secure coding	Secure coding practices shall be applied to software development.	Applicable	A 7-stage secure development process has been created and is controlled via the IFS R&D department who develop, package and supply products into the Unified Support team for them to be deployed within cloud-hosted environments on behalf of customers.	R&D	R&D Secure Development Process
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Applicable	A security scan and penetration test of IFS Cloud products are conducted both by R&D for the core application and by the Unified Support team for cloud-deployed products.	R&D Unified Support	R&D Secure Development Process
A.8.30	Outsourced development	The organisation shall direct, monitor and review the activities related to outsourced system development.	Not Applicable	IFS does not use any outsourced development resources for any purpose related to IFS products and applications.	R&D	R&D Secure Development Process
A.8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Applicable	Live production environments are separate from test and development environments. The IFS Cloud product features specific and separate customer-controlled environments used for "Build" and "Use" practices.	R&D	R&D Secure Development Process
A.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Applicable	Change management processes are applied throughout internal and customer-related operations. All service and support related changes performed by IFS employees on behalf of customers are logged within ticketing systems. Where required, customer approval is sought prior to changes being made.	Applicable in scope functions	Applicable Operating Procedures
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	Applicable	Test data, either used by IFS or IFS customers in cloud environments is segregated and protected with appropriate access controls and information backup procedures.	R&D	R&D Secure Development Process
A.8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Applicable	The audit process includes steps whereby audits and their testing approach is planned and agreed between tester and management, including information access requirements.	Applicable in scope functions	IFS Internal Audit Process
		Number of controls	**93**			
		Number of applicable controls	**92**			