PUBLIC

IFS Information Security - Internal Controls

IFS Global ISMS

Date:	18/10/2022
Revision:	2
Owner:	Data Privacy Officer
Approved By:	General Counsel

Contents

1. Information Security Management in IFS

IFS' commitment to protecting its information security as well as that of its staff, customers, partners and suppliers stems from the most senior members of IFS at Board level. IFS have a central Information Security function, the purpose of which is to harmonize and coordinate the activities relating to information security across the entire group of companies.

Adopting a risk-based approach in accordance with best practice, IFS have adopted the ISO 27001 framework upon which to base its own Information Security Management System (ISMS). As the most internationally recognized security standard, ISO 27001 sets a high bar thus helping ensure that the security controls and practices we use best serve to protect the interest of IFS and all those we work with and serve.

The IFS Information Security policies, standards, processes and procedures are global and apply to all members of the IFS group. Since laws, regulations and customer requirements vary slightly across the countries within which IFS operate, the IFS ISMS allows for regional tailoring. Compliant with a common set of global policies and standards, regional offices can augment the corporate ISMS with regional practices to best meet such local requirements.

IFS holds ISO 27001 certification for its IFS Cloud Service to demonstrate our continued security commitment to customers and the robustness and security-focussed approach taken to providing and maintaining customer cloud environments. The certification also includes within its scope a subset of corporate shared services including IT, HR and FM

2. Information Security Policies

IFS' approach to information security is driven by a top-level Information Security Strategy, approved by the IFS Group Chief Digital & Information Officer on behalf of the IFS Board. The Information Security Strategy aligns with IFS' business strategy, operational needs (including legal and regulatory requirements) and information security risks. The Information Security Strategy and ISMS are reviewed annually to ensure that they remain relevant and up to date. Similarly, the relevant aspects of the ISMS will be reviewed in the event of significant changes to business practice or legal requirements.

The ISMS contains the information security policies, standards, processes and work instructions that define our approach to information security.

Each document that forms the ISMS has an owner and an appropriate authorizer who will hold a management position for the topic covered by the document.

3. Information Security Organization

The IFS Information Security Management System is used to manage information security within IFS and is created and maintained by the IFS Corporate Services Business Unit headed up by the IFS Chief Digital & Information Officer (CDIO). Specific responsibility to maintain the ISMS is delegated to the Vice President, IT Projects Office and Cyber Security supported by the Head of IT Security, both of whom are also responsible for supporting the IFS regions and Corporate functions with its execution.

Each IFS Market Unit and Business Unit is required to act in accordance with the IFS Information Security Management System as applicable to their business operations. Execution of Information

Security within each IFS region is ultimately the responsibility of the Managing Director or President of that region.

Compliance is validated through the IFS internal audit process which is independent of the Information Security function and reports to the IFS Audit Committee.

4. Human Resource Security

IFS recognize the importance placed upon people in helping keep our information safe. Consequently, our information security processes consider people related security matters.

Below is a summary of the key activities forming part of IFS HR security practices:

- IFS conduct pre-employment checks on new hires (whether full-time employee or fixed term contractors as permitted by applicable local law and the position being filled. Where required (e.g. for certain Defence customers) specific checks are undertaken to achieve certain security clearances.
- IFS conduct induction training including training on Information Security in accordance with its policies.
- IFS conduct ongoing security awareness training. Taking several forms and targeting different audiences ranging from the entire company to specific teams, examples include company-wide newsletters from the CDIO as well as training on specific topics in the form training videos, classroom training, etc. In addition to the IFS Information Security Intranet, which includes self-help training material on specific subjects, IFS use its internal global communication tools to raise awareness of the latest security threats and encourage the sharing of knowledge and threats across the company.
- IFS onboarding of new employees includes the assignment of permissions and privileges to IFS information systems in accordance with the employee's user role (job ids). Similarly, changes in role throughout the employee's time within IFS are implemented though a similar process, job ids against being used to determine which access permissions should be allocated and which revoked. Use of single sign-on and integrated identity management ensure that user access and identity are coordinated across business systems.
- Upon termination of employment with IFS staff undergo an off-boarding process where company equipment is returned and securely wiped, user accounts disabled and individuals reminded that non-disclosure agreements that have been signed extend beyond their employment contracts.

5. Asset Management

The IFS Information Classification and Handling policy defines four levels of classification – Public, Sensitive, Highly Sensitive and Confidential used to manage our information assets. Information classification is the responsibility of the asset owner and determines what is and is not permitted in the way the asset is stored and transmitted. Information classification applies to assets in both physical and electronic form and is used to help determine the confidentiality, integrity and availability requirements of the associated information asset.

IFS maintain a data inventory of Confidential information assets which is used to help manage compliance with applicable regulations including data protection and privacy regulations such as the General Data Protection Regulation (GDPR).

The “IFS Information Security Framework – All Employees” describes the acceptable use of IFS information assets. The document also describes how assets should be handled including both physical and electronic security, permitted use of removable media, the secure disposal of media, and end user responsibilities generally that ensure information belonging to IFS, its employees, customers, partners, and suppliers is handled securely and appropriately. The return of information assets when an employee leaves IFS is managed in accordance with the off-boarding process described above.

IFS information assets are also accessed by third parties and the processes by which this is managed are described in section 12 below.

6. Access Control

Access is granted on the principle of “least privilege” where access to information assets is determined by job role. Users are provided with unique User ID’s and the use of strong passwords is enforced

Being a multi-national organisation, some information is held on a regional basis, whereas other information must be accessible across the organisation. To ensure operational efficiency, the accessibility of information is determined by its sensitivity (i.e. its information classification), highly sensitive information being restricted to specific individuals or small groups and less sensitive information available to teams, business functions, offices, etc.

Access to information is controlled by:

- Uniquely identifiable user accounts assigned to each user for each user type;
- Single sign-on managed by centralized directory authentication under formal password management policies;
- Multi-factor authentication for user authentication in higher risk environments.
- Privileged access accounts awarded only in accordance with business needs, separate from the user’s normal account; and
- Role based permissions.

User access is reviewed periodically against user account records to ensure that processes for onboarding/offboarding users and managing changes in user roles are being performed correctly. Higher risk user roles are also validated through periodic checks and included as part of IFS’ internal IT controls audits.

7. Cryptography

IFS require that cryptography be used in certain scenarios e.g. when storing highly sensitive or confidential information on mobile devices (including laptops) and when accessing IFS environments from remote working locations etc. This is implemented in several ways within the IFS IT environment. For data at rest, Microsoft Bitlocker encryption is most commonly used, but where necessary, owing to the sensitivity of the information/risk of data loss, stronger certified encryption protection is used (e.g. FIPS 140-2 L3 on removable media).

For data in transit, protection such as site-to-site VPN connections and point-to-site VPN connections are used. Certificate Authorities are used to manage public keys rather than self-signed certificates and encryption keys are centrally managed as corporate assets.

8. Physical & Environmental Security

IFS have office locations in over 30 countries across the world and, whilst the physical security controls applied at each site vary slightly according to the local environment, each meets a minimum standard to prevent unauthorized access to the facility. The physical controls employed include:

- Closed-Circuit Television;
- User Identity Badges;
- Swipe card access control/user clocking systems and auditing;
- Security guard manned entrances and 24 x 7 security; and
- Physical security perimeters and locked gates.

Access to information assets within IFS offices are also physically protected in accordance with their sensitivity and physical nature. Security controls include:

- Safes/secure storage areas for sensitive IT assets;
- Secure filing systems/cupboards for hardcopy highly sensitive information (e.g. personnel information);
- Restricted access locations in accordance with job role (e.g. switch cupboards etc.); and
- Secure archiving facilities for hardcopy records.

IFS operate a mainly paperless office with the following additional controls being used to physically secure electronic information assets:

- A clear screen policy with an enforced screen lock timeout following periods of inactivity;
- Secure office layouts to prevent the overlooking of sensitive information by people outside of the office (e.g. desk locations, use of roller blinds, cubicle partitions, separate offices in areas where highly sensitive information is being processed).

Each employee is responsible for the security of their allocated computing facilities (mobile phones, tablets, laptops, etc.) and in accordance with the security standards, all employees are required to ensure that the devices are protected at all times. This includes ensuring that such devices are not left unattended when outside of the office environment, not stored in the boot of a car overnight and are securely stored when in hotels and other public locations.

Equipment that has held sensitive, highly sensitive or confidential information is securely disposed of at its end of life. Subject to the physical nature of the equipment and its purpose whilst in production, several processes are used to manage its disposal including:

- Secure physical destruction by a certified third-party organisation;
- Secure wipe using utility software certified to trusted security standards; and
- Destruction of the encryption key followed by reformatting of the device in the case of encrypted disks.

IFS operate three primary data centers that host our internal global IT systems and services; located in Sweden, USA and Sri Lanka. All are based in external, professionally managed Colocation datacenters employing resilience and redundancy to ensure continued availability of service. Staff access to IFS datacenters is limited to a very few individuals within Corporate Services and access logs are regularly audited. Business critical systems and services are managed under appropriate maintenance agreements to help ensure their continued availability through life. The physical separation of the datacenters and choice of location helps protect against environmental threat and forms part of our business continuity strategy. See section 14 below for more information.

9. Operations

IT Operations: IFS' corporate IT function is performed by the centralized Corporate Services team who operate out of Sweden, USA and Sri Lanka. Enabled by geographical distribution, Corporate Services implement a "follow the sun" support model to deliver its IT services and support to the IFS offices across the world. This central function is aided by Local Information Systems teams in the IFS regions who help provide local end user support.
Corporate Services operate in accordance with ITIL processes and practices, with their services and operating procedures being documented within the IFS IT service management tool. Such practices include the maintenance of a Service Catalogue and Configuration Management database (CMDB), Service Level Agreements, demand, incident, problem management processes, etc.

Capacity: Service capacity is monitored as part of operational service management and additional resources allocated where required, made easier by the extensive use of virtualisation technology as part of the core infrastructure. High availability of business-critical systems is achieved using several techniques including Cloud technology incorporating service elasticity and self-provisioning.

Change Management: Changes to services are performed under change management which includes both maintenance and service development activities under the governance of Change Advisory Boards (CABs). All significant changes are thoroughly tested by the business prior to deployment to production. IT Project governance is applied through the formation of steering boards comprising key business stakeholders. Development, test and production environments are separated, and maturity gates used to promote changes from one environment to the next.

Virus and Malware Protection: IFS use centrally managed enterprise grade solutions for malware protection deployed across its end user population and server infrastructure. Virus signature updates are applied automatically at regular intervals. Software patching of all managed server and client operating systems is performed centrally using Window Systems Update Services (WSUS) thereby ensuring that critical security patches of Microsoft operating systems and software products are deployed in a timely fashion.

Consistent Computing Platforms: Computing platforms are managed to a consistent corporate standard using Corporate desktop and server builds with Microsoft's configuration management tools being used to push deployments to the local environments. Frequently required business applications for specific user roles are requested through a software self-service portal, which is part of the IFS IT service management toolset (and with an appropriate approval workflow). The Microsoft configuration management tool is used to execute the approved deployment for such requests using a repository of approved software. Software white/blacklisting processes are used to monitor and manage the production builds through life.

Back-up and Recovery: IFS datacenters are operated under a formal backup/recovery policy which applies at multiple levels within the service stack and with backups being held off-site. Retention of daily backups is 40 days, with monthly full backups being retained for 365 days, and yearly full backups for 8 years. Backup monitoring is included as part of daily IT operations. Testing of restoration processes is performed quarterly and are implemented by refreshing test environments from live production environments (sensitive data being obfuscated in the process). Documented processes exist for managing business continuity incidents and disaster recovery procedures are also documented. End client backup processes vary slightly across the IFS regions in accordance with environmental requirements and business needs. Solutions include the use of secure third-party client backup services and IFS' private cloud services.

Monitoring and Logging: Service operations include service monitoring and logging which helps protect our IT environments by scanning for abnormal activity. Such activities include:

- Virus and threat monitoring;
- Deployment of host-based intrusion prevention systems;
- Software Patch reporting (as part of software patch management describe above);
- Internet gateway threat and traffic monitoring;
- Identity based behavioural analytics;
- Application monitoring and inventory management;
- User behaviour logging;
- Deep packet inspection.

System and application logs are protected from normal user access and IT synchronisation of system clocks is applied to ensure that they remain within acceptable tolerances across the IFS IT infrastructure.

Vulnerability Scanning and Penetration Testing: Vulnerability scanning of our key business systems and environments is performed at regular intervals and any necessary remediation is performed as part of IT system/service and maintenance by the Corporate Services operations team. Penetration testing of scoped elements of our IT environments is performed at least annually by external specialists and remediation actions applied as necessary.

10. Communications

The IFS Corporate network is managed centrally by IFS Corporate Services in accordance with our Communications and Network policy. Network service security is tightly controlled by a dedicated team within IFS Corporate Services. Service responsibility comprises all communications between IFS sites across the world, remote connections to IFS services and systems by end users and third parties (including access to IFS' private cloud based services) and IFS' wireless services at each of its offices (including dedicated services for IFS employees, customers and visitors and a dedicated network for mobile devices).

Communications service providers for the IFS Corporate WAN are also managed by Corporate Services including selection of suppliers, management of supplier agreements and monitoring of service performance in accordance with service level agreements.

The IFS corporate WAN is monitored to detect potential and real threats and minimize the risk of data loss as described in the previous section. Network access is managed and access to certain public resources blocked to reduce network security risk. Use of IFS communications services by IFS end users is governed by IFS all employee policies which define appropriate use. Such policies cover use of both our corporate environments and networks as well as the use of social media tools. IFS policies also describe the logging and monitoring performed of our networks and environments by Corporate Services and specifically the capture of information regarding end user activity from the data privacy perspective.

Connection to customer environments to enable the execution of IFS implementation and support services by IFS staff is achieved by default using a standard connection method, SupportNet, agreed with the customer, and which comprises an IPSEC VPN connection. Full details of the SupportNet service can be found in the document "IFS SupportNet – Overview and FAQ" which is available on request. Access by IFS staff to the customer environment is achieved either using this connection or by attendance on customer site.

IFS communications security also covers the transfer of information by non-electronic means (e.g. using removable media, transferred by hand by IFS employees or using postal/courier services). Subject to the sensitivity of the information, encryption techniques described in section 7 above are used or secure transport agents employed as appropriate).

11. Systems Acquisition, Development & Maintenance

All new IFS information systems and services are implemented by IFS Corporate Services or under their supervision by an appropriate, validated supplier. In compliance with data protection laws, risk and impact assessments are conducted when implementing new, or performing significant changes to existing, systems holding sensitive personal information. Development and test environments for new systems and system changes are separated from live production environments. Testing of the systems is performed using appropriate test data by representatives from the business prior to it entering production. The transition into production includes the handover of the new or amended system to the IFS Corporate Services Operations team who are then responsible for its continuing maintenance until end of life.

12. Information Security & Third Parties

12.1. IFS Partners

IFS has established a global partner network of product and services organisations that support with the implementation of customer solutions. Further information regarding IFS partners can be found on the IFS Internet site at http://www.ifsworld.com/corp/partners/.

All such partners are governed under an IFS partner agreement which includes consideration of information security. Under these agreements partner users are required to operate in accordance with the same security controls applicable for IFS' own staff. Partner responsibilities under these agreements include promoting security awareness within their staff as well as ensuring adherence to IFS security standards.

IFS partners normally work as part of an IFS project and operate using IFS systems and processes which ensure the protection of personal data. Access controls are granted in accordance with the partner user role and on a need to know basis using access control mechanisms described in section 6 above.

IFS partner performance is monitored by IFS as part of managing the partner relationship. Should an information security incident occur, IFS partners are required to report them immediately to IFS in accordance with the IFS incident management process described in the next section. In such circumstances IFS customers impacted by the incident will be notified by IFS also.

12.2. IFS Suppliers

IFS only use suppliers who adhere to IFS' global code of conduct which covers ethical business practices. Prior to becoming a key supplier of products or services for IFS, such organisations are verified in accordance with an approved supplier process appropriate to the nature of the products or services they will provide.

IFS agreements with suppliers contain non-disclosure agreements to protect the confidentiality of IFS held information and may require data processing and data transfer agreements to ensure compliance with the applicable laws and regulations of the countries within which IFS operate. Where appropriate (in accordance with the nature of the products or services being supplied), IFS suppliers will also be required to adhere to the relevant aspects of the IFS information security incident management process.

Supplier relationships are managed for the duration of their contractual engagement, including monitoring of performance in accordance with any contractual or quality requirements and information security arrangements. Where deemed necessary, supplier agreements may include the right of IFS to audit the supplier's security processes and practices.

13. Information Security Incident Management

IFS operate a formal Incident Management process which is part of our Information Security Management System (ISMS). The process is used to manage incidents both internal to IFS and those involving customers, suppliers, IFS partners and other third parties. In the event of an incident, including identified weakness in security practice, an incident event is raised which triggers the formal incident management process. Incidents can be raised by anyone; employees, customers. partners, suppliers or members of the general public (using the IFS email address privacy@ifs.com included on the IFS public website). Using this process, all aspects of the incident are managed including:

- Capture of the event and any information relating to its creation, including the preserving of key forensics information that may be required as part of an internal or formal investigation;
- Analysis of the event including the scope of impact and the reason the event occurred;
- Immediate corrective action to prevent the incident continuing or getting worse;
- Communication to the appropriate stakeholders without undue delay and which may include external impacted parties as well as internally within IFS;
- Root cause analysis of why the incident occurred and the identification and implementation of preventative actions that reduce the likelihood of such an event recurring in the future.

Depending upon the nature of the incident, communication above may include the appropriate Supervisory Authorities, law enforcement agencies, etc. in accordance with laws, regulations and good practice. Having contained the incident, a thorough investigation is performed regarding the cause and appropriate preventative actions put in place to limit the likelihood of a recurrence in the future. Stakeholders will be kept informed of events and where the cause of the event originates outside of IFS, we will provide relevant support to assist with recovery where services for which IFS is responsible are involved.

Staff are trained in the incident management process as part of their induction training and this is followed up with periodic reminders including postings on IFS' internal communications platforms, intranet site and training courses within the IFS Academy's learning center.

14. Information Security in Business Continuity

Whilst information security as part of day to day operations is essential to keep IFS and customer information safe, it is equally important that our information security controls are effective when operating in a non-routine manner, such as when responding to a business continuity incident or recovering systems following significant, unplanned failure.

Starting with backup and recovery as described earlier in this document, all IFS backup sets and system recovery activities are performed in a secure fashion. Backup media is held securely in remote locations, separate from the production copy and are accessible only by authorised personnel. Transfer of information to and from the remote locations, both in backup and recovery mode, is performed using a secure transfer method including secure physical handling in the case of physical off-site storage media or using encryption for online remote storage transfer.

IFS also have secure disaster/recovery processes in place to enable the successful recovery of key IT systems and services following a major failure. Provisions for disaster/recovery include:

- use of physically distributed services across multiple IFS data center locations, enabling recovery at alternative locations whilst remaining within the IFS corporate network;

- Use of primary and secondary cloud-based data centers in geographically dispersed locations offering the opportunity for recovery to the original or alternative site;
- Provision of certain global services from multiple locations so as to avoid single point failure as well as provide resilience in the event of a major incident or event;
- Cloud services with contracted recovery point and recovery time objectives and operated in accordance with certified security practices (e.g. ISO 27001).

With regarding to ensuring that business continuity incidents and events do not result in a degradation of information security, IFS' business continuity strategy is underpinned by secure remote working practices and facilities that support it, and which also form an essential requirement for day to day operations for those employees in the organisation who need to be able to perform their job function when outside of the office. Through a combination of cloud-based services, virtualisation, service elasticity and distributed IFS infrastructure, these capabilities enable fail over to alternative locations should a specific site be unavailable without the need to construct new secure environments.

15. Compliance

IFS is committed to complying with all applicable legal and regulatory requirements relating to the operation of the company and the delivery of its products and services.

IFS information security practice is independently reviewed periodically by an appropriately qualified external organisation against multiple internationally recognized security standards, including for example ISO 27001, NIST, SANS 20. The purpose of such external review is to validate that IFS continues to operate in accordance with industry best practice and highlight any areas for improvement where necessary. Findings from such security reviews become improvement actions as part of IFS' commitment to continuous improvement with regarding to its information security practices.

16. Privacy & Data Processing

IFS is committed to complying with all applicable privacy laws relating to the operation of the company and the delivery of its products and services.

IFS have developed its global policies and processes in accordance with the General Data Protection Regulation 2016/679 (GDPR) and maintain a complete data inventory of all processing performed by IFS. These policies are applicable to all IFS regions and country offices regardless of whether or not they are located in Europe. The IFS Information Security Management System includes processes for managing and protecting the rights of the data subjects whose data IFS process (as both controller and processor) as well as incident management and breach notification processes should a data breach occur. The processing of personal information across the IFS group is governed under an IFS Intra-Group Data Processing Agreement which incorporate the Standard Contractual Clauses (sometimes known as Model Clauses) for the transfer of personal data to third countries.

This remainder of this section identifies the IFS Affiliates that make up the group organisation and which are included within the IFS Intra-Group Data Processing Agreement.

16.1. IFS Affiliates

IFS Affiliates located in the EEA

Entity name	Reg no	Service description	Data Processing (see Section 16.2)	Control Measures	Country
IFS Danmark A/S	14 45 34 31	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Denmark
IFS Finland Oy Ab	0721651-7	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Finland
IFS France SA	B 320 508 229	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	France
IFS Deutschland Gmbh & Co KG	HR A 7045	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Germany
IFS Italia S.r.l.	13188440153	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Italy
IFS Benelux BV	17102305	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Netherlands
IFS Norge AS	961073995	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Norway
Industrial and Financial Systems Central and Eastern Europe Sp. z o.o	0000046494	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Poland
IFS Applications Iberica, S.A.	ES-A82573429	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Spain
IFS Nordic AB	556248-4856	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Sweden
IFS Sverige AB	556211-7720	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Sweden
Industrial and Financial Systems, IFS Schweiz AG	CH-020.3.032.813-6	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Switzerland
IFS Industrial and Financial Systems Poland Sp. z o.o.	45818	R&D/Support	Product Support	Intragroup Agreement including SCCs IFS ISMS	Poland
IFS World Operations AB	556040-6042	Corporate Functions, R&D	Global IT Support Product Support	Intragroup Agreement including SCCs IFS ISMS	Sweden

IFS Affiliates located outside the EEA:

Entity name	Reg no	Service description	Data Processing (see Section 16.2)	Control Measures (see Section 5)	Country
IFS North America, Inc.	39-1292200	IFS Corporate IT	Global IT Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	USA
IFS Canada Inc.	1968721	Consulting/Support/ IFS Corporate IT	Product Implement Product Support Global IT Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Canada
IFS Industrial & Financial Systems Canada, Inc.	407396-7	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Canada
IFS Middle East FZ LLC	19443	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	United Arab Emirates
Application Software IFS South Africa (Pty) Ltd	1999/008952/07	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	South Africa
IFS Japan Inc.	0199-01-009361	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Japan
IFS R and D International (Private) Ltd	PV 15891	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
Industrial & Financial Systems Sri Lanka Ltd	PB 1313	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
Industrial & Financial Systems R&D Ltd	PB 1274	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
IFS Research and Development (Private) Ltd	PV 14786	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
IFS Solutions Asia Pacific Pte Ltd	99101628D	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Singapore
IFS Solutions Singapore Pte Ltd	200514639D	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS	Singapore

Entity name	Reg no	Service description	Data Processing (see Section 16.2)	Control Measures (see Section 5)	Country
				Site to Site VPN encryption of the IFS private network	
IFS Australia Pty	98088889703	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Australia
IFS Zealand Pty Ltd	84-936-642	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	New Zealand
IFS Solutions India Pvt Ltd	55-49761	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	India
IFS Astea Ltd	no 51-195654-2	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Israel
LatinIFS Tecnologia da Informação Ltda	35.226.370.061.	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Brazil
Industrial and Financial Systems, IFS UK Ltd	3277022	Consulting/Support	Product Implementation Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	United Kingdom
IFS World Operations AB UK Branch	FC039108	IFS Corporate IT, Cloud Services	Global IT Support IFS Cloud Services, Product Implementation, Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	United Kingdom

Global Third-party service providers located in the EEA

Entity name	Service description	Data Processing (see Section 4)	Control Measures (see Section 5)	Country
Microsoft Corporation	Cloud platform services	Azure Service Provision	Microsoft DPA MS Key Vault secure managemnent of Encryption keys within the EU	Netherlands & Ireland
ServiceNow	Support platform	IT Service Management Toolset	Service Now DPA Security Management System certified in accordance with ISO 27001, SOC 2 Type 2 report	Netherlands & Ireland

Global Third-party service providers located outside the EEA

Entity name	Service description	Data Processing (see Section 4)	Control Measures (see Section 5)	Country
TATA Consultancy Services Limited	Consulting services	IFS Cloud Service Support	IFS Partner DPA Management in accordance with IFS ISMS IFS Monitoring & Detection Containerised environments managed by IFS	India

16.2. Data Processing Descriptions

Project Implementation
In order to support the customer with the implementation of an IFS solution, IFS performs a range of activities, each of which may result in the processing of customer data. Such activities are performed by the IFS regional consulting team for the country in which the solution is to be implemented and may involve the support of other regional consulting teams and IFS Research and Development (R&D) staff as shown in section 1 above. IFS regional and global support teams may also be involved in the implementation phase in resolving any product defects identified during the implementation. IFS follow a standard implementation process using standardized implementation toolsets comprising the following activities:

- Discussion of business processes and practices;
- Design of system customisations;
- Design of Information System interfaces between existing/legacy IT systems used by the data exporter and the new solution;
- Processing of customer production data, including end user information to support data take-on/data migration activities to prepare the product for operational use;
- Processing of customer production data to support end user training;
- Processing of customer production data to support setup for solution verification and validation activities by the customer;
- Processing of customer production data to support the establishment of one or more reference environments to support system testing and live system maintenance and support;
- Processing of customer production system transaction data to support the investigation of a perceived system error or software bug pre-production.

Product Support
In order to implement the customer's IFS support agreement, IFS regional support teams and the IFS Global Support Organisation may require access to customer production or reference environments containing customer production data in order to investigate reported software issues associated with the IFS product. The investigation of certain product issues may require the involvement of IFS R&D.

IFS Cloud Services
IFS uses the IFS Cloud service for internal business operations and the IFS product that forms this solution is hosted in Microsoft Azure datacentres. These data centres are located within the EEA in order to limit the extent of any transfers of personal data outside of the EEA.

The Managed Services Team access the customer environment in Azure in order to perform the services included in the customer's managed services agreement only. Each service comprises the following primary activities:

- Creation of the Azure platform upon which the customer's solution will run;
- Installation of the IFS products that make up the customer solution;
- Configuration of the solution including the establishment of system performance monitoring;
- Monitoring of the system to ensure that it is compliance with its agreed service levels;
- Execution of backups to a secondary data centre, including performing recovery operations should a significant system failure occur;
- Proactive and reactive maintenance activities to address system monitoring alerts and system issues reported by the customer's end users. Such activities include software patching at operating system, middleware and application levels, database administration (where applicable) and performance tuning;
- System changes and enhancements, either to ensure the solution operates in accordance with its service levels or as a result of an agreed change with the customer;
- Service de-commissioning in accordance with a process agreed with the customer.
- Management of encryption keys where a customer has elected to have IFS perform this function for them.

The IFS Cloud Services team are not required to process IFS controlled data as part of their day to day activities. They do however hold administrative level permissions for the hosting environment in order to execute their technical responsibilities of maintaining the Azure platform the associated IFS products.

IFS Cloud Service Support

IFS' partner, Tata Consultancy Services (TCS) Limited, support with the execution of IFS Cloud service activities. These relate to the management of the Azure platform and IFS products hosted within Azure. They do not process IFS data, however they do hold administrative level permissions which potentially allow the ability to access IFS data within the Cloud solution. TCS staff are managed as an integrated part of the IFS Cloud Team under IFS management.

Azure Service Provision

The Azure data centers are managed and maintained by Microsoft in accordance with their ISO 27001:2013 and SOC 2/SOC 3 certified processes. Their responsibilities are to ensure the Azure services utilized by the IFS Managed Cloud solutions remain available and performing in accordance with their specification. The Azure services consumed by the IFS Managed Cloud solutions include:

- Infrastructure as a Service (IaaS) processing, storage, site recovery and network services;
- Platform as a Service (PaaS) database and web services for IFS products which do not require special platform management

Microsoft do not have access to applications within the virtualized environments within which the IFS products that make up our customer solutions run. They therefore do not have access to customer production data held within IFS Cloud solutions. However, since Microsoft staff have elevated permission access to the components of the Azure environment it is theoretically possible that they could process customer data (e.g. by monitoring traffic across a LAN segment of a particular data center in order to investigate performance issues). Microsoft's processes for managing the Azure data centers employ segregation of duty principles that make it extremely difficult to associate information on the physical Azure infrastructure with a specific Azure customer. Consequently, customers have the opportunity if they wish to manage encryption keys themselves rather than have Microsoft perform this for them.

Global IT Support

The IFS Corporate Services business unit is responsible for providing IFS' global IT services which include all IFS mission and business critical IT systems, infrastructure and end user IT equipment that support our global business operations. IT Service Management is mainly provided out of the

United Kingdom and Sweden, with IT operations, application and end user support provided from Sri Lanka. Corporate Services do not process customer data, instead they implement and maintain the internal IT services and equipment that support the IFS business operations. Whilst this includes the use of administrative level accounts, it does not include access to customer solution application accounts.

IT Service Management Toolset

ServiceNow is the Gartner Magic Quadrant leader IT Service Management Tool used by IFS to manage customer support tickets relating to its products and services. The system holds the user identity and business mail address of the nominated few customer users authorised to raise support tickets (typically 5). No customer production data is held within the ticketing system, only details of perceived issues associated with the IFS Cloud service. Ticket Data is held within the EU (Ireland and the Netherlands). Further information can be found in the ServiceNow Cloud Security FAQ document attached below.

ServiceNow FAQ

Document Revision History

Rev.	Date	Owner	Remarks
1	13/10/2021	Stephanie Hsieh	New document established from ”IFS Information Security Management” document and seperating internal security controls (previously ”Part 1”) from IFS Service security controls (previously ”Part 2”) in order to accomodate new IFS service offerings
2	18/10/2022	Stephanie Hsieh	Updates to reflect changes in organisation impacting sub-processing.

Distribution & Document Handling

This document is intended for use by IFS customers and partners and the contents is confidential to IFS.

Authorisation & Approval

This version of the document has been approved by the Owner and authorized for release by the Approver shown on the front cover of this document.

Review & Amendment

This document is reviewed on an annual basis and updated with evolving internal and external requirements and supplier arrangements. This document is subject to change without prior notice and such changes will be performed in accordance with IFS change management processes.

ABOUT IFS

IFS develops and delivers enterprise software for customers around the world who manufacture and distribute goods, maintain assets, and manage service-focused operations. We offer applications that enable companies to respond quickly to market changes and use resources in a more agile way to achieve better business performance and competitive advantages. IFS's products are known for being user friendly, modular in their design and flexible enough to support the customers in their way of working according to their established processes.

Learn more about how our enterprise software solutions can help your business today at ifs.com

Be your best in your Moment of Service!

WHERE WE ARE

AMERICAS
+1 888 437 4968

ASIA PACIFIC
+65 63 33 33 00

EUROPE EAST
+48 22 577 45 00

EUROPE CENTRAL
+49 9131 77 340

UK & IRELAND
+44 1784 278222

FRANCE, BENELUX AND IBERICA
+33 3 89 50 72 72

MIDDLE EAST AND AFRICA
+971 4390 0888

NORDICS
+46 13 460 4000