PUBLIC

IFS GLOBAL ISMS

IFS INFORMATION SECURITY MANAGEMENT

Date:	28/07/2020
Revision:	1
Owner:	Todd Williams
Approved By:	Richard Rogers

TABLE OF CONTENTS

PURPOSE OF THIS DOCUMENT

This document is made up of two parts:

- **Part 1** Describes IFS general security practices and controls together with any associated security and privacy related audits and certifications received. This is relevant to all customers to all customers of IFS.
- **Part 2** Describes the architecture of, information security policies, controls and processes applied in the delivery of IFS Cloud Services as well as privacy-related audits and certifications received for IFS's Cloud Services. This is relevant to customers of IFS Cloud Services only. They are in addition to the general information security policies, controls and processes described in part 1 of this document. As with part 1, the following section headers follow the control areas defined within ISO 27001. Where an area is not covered, the corresponding section from part 1 applies to IFS Cloud as well..

PART 1 – IFS INTERNAL SECURITY PRACTICES

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 is in the process of certifying its IFS Cloud Service to ISO 27001 to demonstrate the robustness and security focused approach taken to providing and maintaining customer cloud environments. This certification will also include a subset of 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". 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

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.

17 IFS PRODUCT SECURITY

Product development at IFS is conducted by IFS' Research and Development (R&D) organisation only.

IFS operate a Product Security Board within R&D, the purpose of which is to ensure that IFS products are developed/supported with consistently high security assurance and drive our commitment to continuously innovate in this critical area. IFS' approach to product security includes:

- Code reviews designed to ensure adherence to IFS' development standards;
- Software security testing and code scanning to identify and address security vulnerabilities;
- Release reviews and approvals designed to ensure product releases comply with internal process requirements;
- Vulnerability testing and remediation for infrastructure and tools supporting our product development lifecycle;
- Segregation of product development from other technical environments within IFS, with changes to production application systems undergoing authorization, testing, approval and controlled release and distribution.

Industry standard processes and techniques are used throughout the product development lifecycle including:

- Secure development process and practice,
- Security testing (internal and external),
- Security training and awareness,
- Vulnerability management, metrication and maturity measurement.

Any identified security vulnerabilities relating to IFS products, or third party solutions upon which they are dependent, are reported to customers through the IFS Security Portal which forms part of the IFS Customer Portal. Vulnerability notices provide key information that help IFS customers determine the appropriate course of action based upon criticality, potential impact and applicability as well as providing technical information regarding the vulnerability itself and the remediation action required.

IFS customer solutions are established using a formal, controlled release of one of IFS's products to a dedicated deployment environment. Regardless of whether the solution is to be hosted within the customer's own IT environment or within IFS Cloud, the processes used for implementiing and supporting the customer solution preserve the information security throughout. This is achieved using IFS' trusted lifecycle management tools, formal change management processes and coordinated with customer actvity.

Some customer solutions may involve the use of products developed by IFS partners. In such cases, development and support of these products is the responsibility of the IFS partner unless otherwise stated in the IFS agreement with the customer.

IFS GLOBAL ISMS

IFS INFORMATION SECURITY MANAGEMENT

PART 2 – IFS CLOUD SERVICES SECURITY PRACTICES

Part 2 describes the architecture of, information security policies, controls and processes applied in the delivery of IFS Cloud Services as well as privacy-related audits and certifications received for IFS's Cloud Services. This is relevant to customers of IFS Cloud Services only. They are in addition to the general information security policies, controls and processes described in part 1 of this document. As with part 1, the following section headers follow the control areas defined within ISO 27001. Where an area is not covered, the corresponding section from part 1 applies to IFS Cloud as well.

1 IFS CLOUD INFORMATION SECURITY MANAGEMENT

IFS have developed and maintain an Information Security Management System (ISMS) specifically for the IFS Cloud Services which has been produced in accordance with ISO 27001. The IFS Cloud ISMS is fully integrated with the broader IFS ISMS, but itself covers the following key areas of the service:

Cloud Platform and Infrastructure: Hosting platform creation and configuration to support deployment of the customer's IFS product and contracted service level agreement;

Infrastructure monitoring and management: Monitoring and operational management of the technical infrastructure and hosting platform to ensure adherence with contracted service level agreements and to action monitoring events relating to system performance and security;

Application monitoring and management: Monitoring and management of the IFS application(s) to ensure continued availability of the application to its end users and its performance according to contracted service level agreements. This

includes software incident and security incident management, the latter including formal data breach management should such an event occur;

Installation of Support and Consulting software deliveries: IFS product deployment to the hosting platform, including technical configuration to support availability and performance requirements. Support patch deployment to the customer's test and production environments in accordance with releases from IFS Support Services.

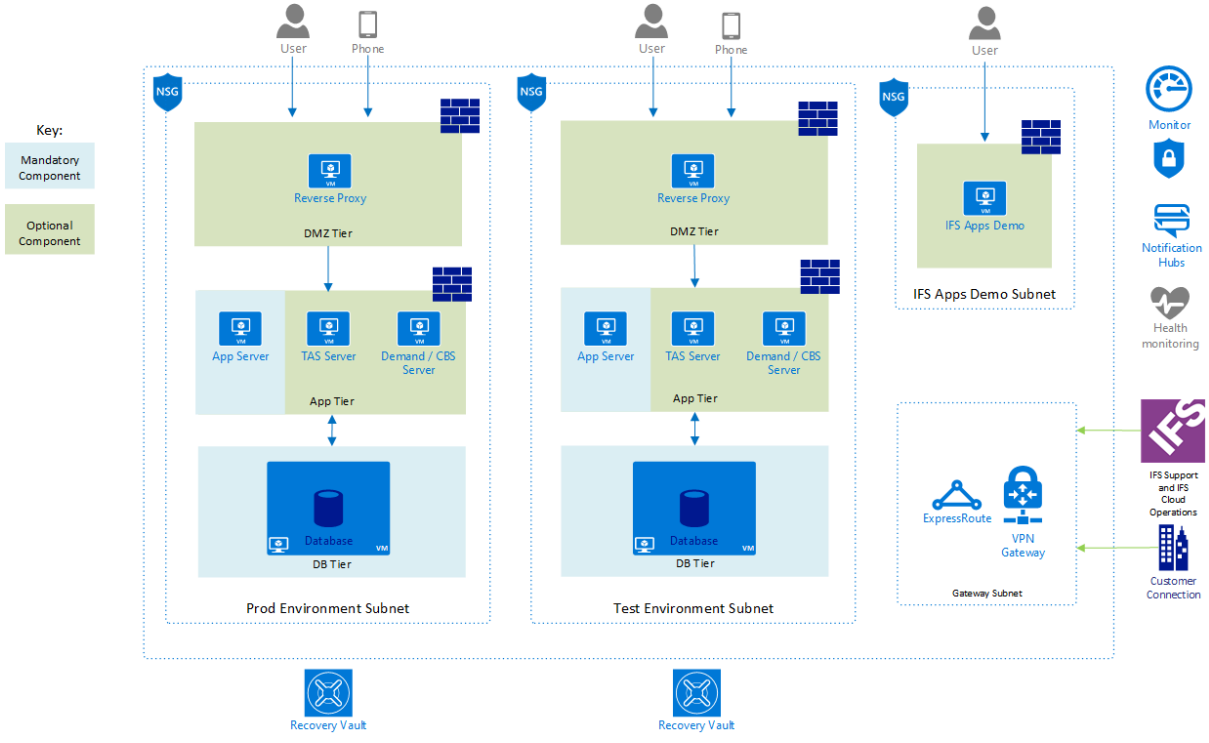
2 IFS CLOUD SECURITY ARCHITECTURE

IFS Cloud is deployed upon Microsoft Azure and is available in a subset of Microsoft's global Azure data centers, allowing customers to select a suitable location for their specific requirements, taking into account factors such as network latency, data sovereignty, etc. The service comprises a primary and secondary data center, the latter being used to facilitate the associated backup and recovery services described in more detail in section 7 below.

The following sections summarize the key architectural elements of each IFS Cloud Services relevant to the IFS software solution, a more complete description being included within the IFS Cloud Service Description.

2.1 IFS Applications

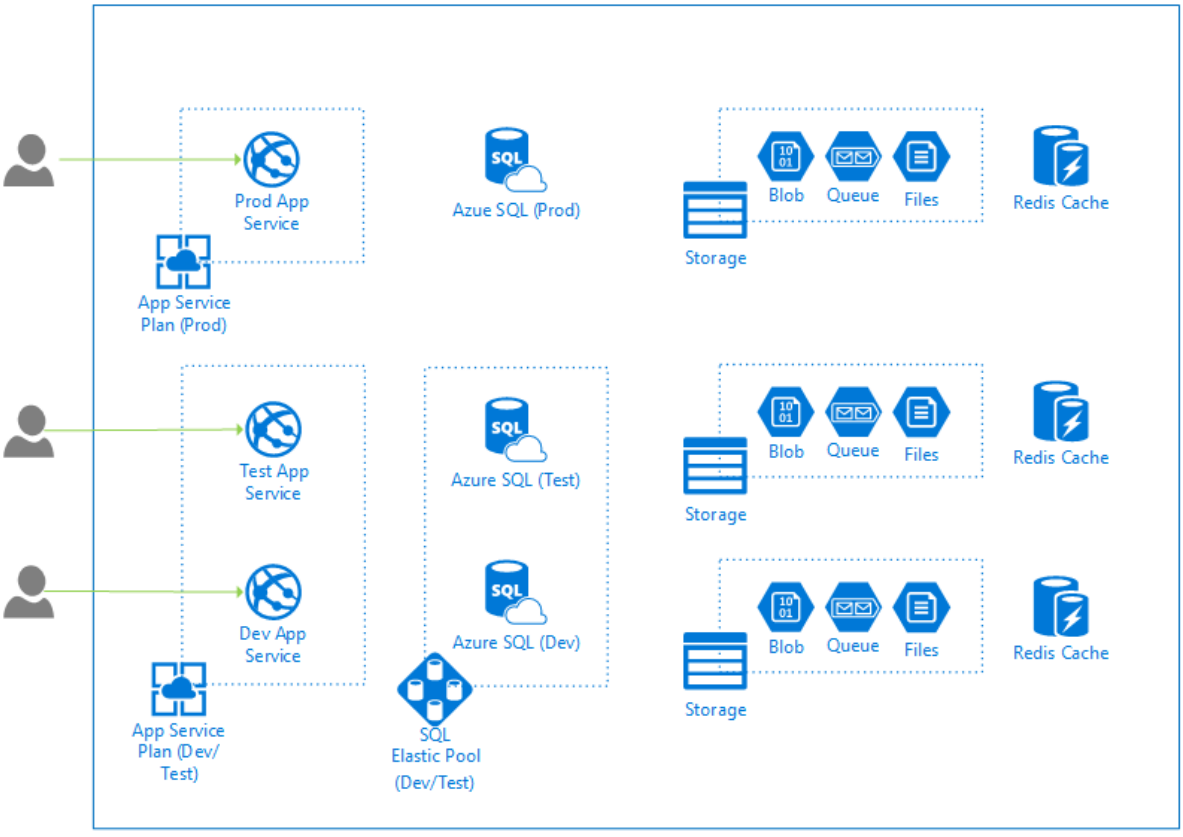
The IFS Applications solution is deployed in a single-tenant Microsoft Azure subscription, the solution comprises separate test and production environments, each comprising a database, application and DMZ tier as shown in the architecture diagram below. The solution also includes an optional demonstration environment, again separated from the test and production environments, and used typically to support the implementation phase of the deployment lifecycle.



Connectivity is provided through a secure communications gateway, enabling service access to customer end users as well as IFS for service delivery and maintenance activities (described in more detail in section 8 below).

2.2 Field Service Management (FSM)

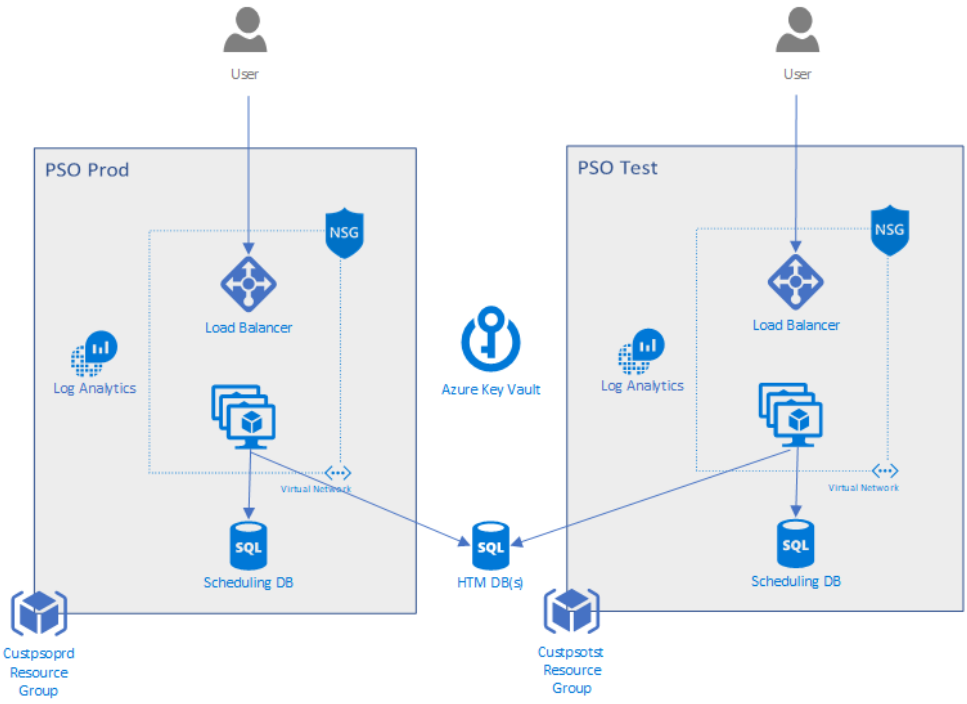
The Field Service Management solution is deployed in a single-tenant Microsoft subscription, comprising separate development/test and production environments, each built with their own Azure SQL database. Secure user access is via the appropriate application service (production or test), with IFS access for service delivery and maintenance being achieved in the same way as for the IFS Applications solution described in the previous section.



2.3 Scheduling

The IFS Cloud scheduling solution is an optional service that can be added to both the IFS Application and IFS Field Service Management solutions. The solution sits within the dedicated customer subscription and includes, as with other solutions, separate test and production environments.

Each environment comprises an underlying SQL Server database and a scalable set of supporting services covering scheduling distribution, a target-base scheduling engine and what-if scenario explorer service managed by a load balancer as shown in the diagram below.



Whilst each of the above services follow a standard "template", the specific deployment will be configured to integrate with the customer's IT landscape, with the utilisation of solution features such as single sign-on and establishment of a single integrated cloud/on-premise virtual domain being dependent upon customer requirements and customer IT landscape constraints.

3 ASSET MANAGEMENT

3.1 IT Assets

The Microsoft Cloud Infrastructure and Operations (MCIO) team manages the physical infrastructure and data center facilities for all Microsoft online services. This includes both the physical and environmental controls within the data centers as well as the outer perimeter network devices (e.g. edge routers). The MCIO themselves have no direct interaction with the Azure services themselves.

Microsoft Service management and service teams, separate to the MCIO, manage the support of the Azure service itself. Made up of numerous teams, each is responsible for a specific aspect of the service and has engineers available 24 x 7 to investigate and resolve failures in the service. Segregation of duty principles are applied, and service teams do not, by default, have physical access to the hardware environments that make up Azure.

The Azure IT assets provided as part of the IFS Cloud Services, and described in the previous section, are managed by the IFS Cloud team. An inventory of all such assets is held in a Configuration Management Database (CMDB) by IFS. Such assets are only managed by the relevant IFS Cloud personnel who are responsible for their establishment, operational monitoring and maintenance and disposal at their end of life.

Customer onboarding comprises the establishment of the Azure virtualised services that host the specific IFS Cloud Services solution. This is followed by the installation of software assets onto the virtualised services then followed by the establishment of the secure customer connection in accordance with the connection method agreed with the customer (e.g. virtual network, private leased line, etc).

During the life of the IFS Cloud Services solution, the IFS Cloud team are responsible for the monitoring and maintenance of the IFS IT assets, including the deployment of changes to the service in response to events such as software updates, security patches and service enhancements/extensions. All such changes are performed under formal change management utilising IFS' IT Service Management tools.

At the end of life of the IFS Cloud Services, all deployed IT assets are securely destroyed using the Azure administrative processes provided by Microsoft Azure and which are certified in accordance with ISO 27001 (as well as other internationally recognised security standards (please see Microsoft's Trust Center for more details).

3.2 Information Assets

IFS Cloud Information assets fall into one of two categories:

- Customer data
- IFS Cloud Service operations data

Processes and responsibilities for managing each of the above data categories are different and are described in the following sections.

3.2.1 Customer Data

Data held within both the production and test applications described in section 3.1 are owned and are the responsibility of the IFS Cloud customer. In execution of the IFS Cloud Services agreement, it is necessary for IFS to process information within these environments, for example when investigating a reported software issue. IFS has implemented procedures designed to ensure that customer data is processed only as instructed by the customer, throughout the entire chain of processing activities performed by IFS and its sub-processors. IFS has entered into written agreements with its sub-processors regarding privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. The document "List of IFS Sub-processors" sets out the current list of sub-processors involved with the delivery of IFS services including IFS Cloud Services.

IFS customers are responsible for managing their data in accordance with its classification and handling requirements determined by any applicable laws or regulations and for complying with the terms of the applicable contract with IFS and any associated data processing terms.

Prior to termination of an IFS Cloud Services agreement, customers may request either the deletion or offboarding and deletion of its data. IFS support customers with the offboarding process by providing backups of the necessary information assets to help customers restore the information onto an alternative platform. This enables customers to implement, verify and validate their chosen new platform in parallel with the existing environments, and to plan off-

boarding and cutover activities to minimize business disruption. The actual technical operational environments are not moved outside the IFS Cloud Service due to commercial, legal and technical factors.

At the point of termination of the IFS Cloud Services agreement, return and deletion of customer data will be in accordance with the terms of the agreement between IFS and Customer. Deletion of data from the Cloud Platform is further described here.

3.2.2 IFS Cloud Service Operations Data

IFS Cloud Service operations data comprises the information associated with the management and operational delivery of the IFS Cloud Services itself for an individual customer. Such data comprises information such as system logs, system configuration files, error dumps etc. All such data is owned and managed by IFS and, with the exceptions of agreed service reporting and other data required to meet any applicable regulatory requirements, is not shared with third parties.

Upon termination of an IFS Cloud Services agreement, all such operations data will be deleted in accordance with the processes used to delete customer data described in the previous section and will therefore not be available post termination/expiration.

4 ACCESS CONTROL

The IFS Cloud Services includes a number of security controls which are used to restrict and protect access to both the IT and information assets that make up the service. Access controls are layered in accordance with the service layers that make up IFS Cloud solutions.

4.1 Microsoft Access to IFS Cloud Services

Employees (and contractors) of Microsoft involved with the delivery of Azure services have their employee status categorised with a sensitivity level that defines their access to Azure hosted services and data utilised as part of the IFS Cloud Services. A list of these role based access permissions can be found on the Azure Trust Centre website and include roles ranging from Data Center Engineer with no access to Azure customer data up to Live Site Engineers who require access to Azure customer data in order to diagnose and mitigate platform health issues using diagnostic tools. All such users have a unique identifier to authenticate onto all assets and devices that make up the Azure environment.

Microsoft's Azure operations personnel are required to use secure admin workstations (SAWs). With SAWs, administrative personnel use an individually assigned administrative account that is separate from the user's standard user account. The SAW builds on that account separation practice by providing a trustworthy workstation for those sensitive accounts.

4.2 IFS Administrative Access

As part of creating, managing and monitoring the IFS Cloud Services, IFS require the use of administrative level accounts which provide access to the Azure services and platforms that underpin the application solutions. These IFS controlled accounts are only made available to IFS personnel actively involved in the provision of the IFS Cloud Services and are allocated on an "as required" basis in accordance with the user's job function, much like the principles applied by Microsoft and described in the previous section. These accounts comprise both Microsoft Azure accounts as well as administration accounts for the various infrastructure components (e.g. Oracle) that make up the particular IFS Cloud

Service. Owing to the elevated permissions that the Azure accounts provide, multi-factor authentication is enabled to serve as an additional identity validation measure.

Access to the Microsoft Azure platforms and infrastructure that make up the IFS Cloud Service is not granted to IFS Customers.

4.3 Customer Controlled Application Access

Access to IFS Cloud Services requires authentication via one of the supported mechanisms described in the IFS Cloud Service Description (e.g. single sign-on using the customer's existing Active Directory). All application level access is managed by the IFS customer, including user accounts provided to IFS in order to execute the services defined within the customer's agreement with IFS (e.g. implementation services, support services, etc). Policies for such accounts are managed in accordance with the customer's own access and identity policies (e.g. password policy enforced by the customer's own Active Directory) subject to any technical constraints imposed by the IFS Cloud Service. The IFS customer can enable and disable such accounts using application administrator accounts provided to them as part of the IFS Cloud Service. It should be recognised that disabling accounts allocated to IFS may prevent delivery of the contracted services or fulfilling any applicable service level agreements.

4.4 Monitoring and Threat Detection

IFS Cloud Services are monitored for unauthorized intrusions using a combination of network and host-based intrusion detection mechanisms. IFS Cloud utilises Azure Security Centre which provides threat protection using facilities including continuous discovery and monitoring of Azure deployed resources and an assessment of their security status and any applicable security vulnerabilities that need remediation.

Microsoft Service teams configure active monitoring tools in accordance with defined requirements and which include Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide alerts to Azure security personnel in situations that require immediate remediation.

The IFS Cloud team utilise Azure monitoring and detection tools as part of their own service monitoring and which are supplemented by further security and health monitoring tools at the application level. Alerts are integrated with IFS Service Management and Incident Management toolsets creating fast, efficient responses to events that require immediate action. Monitoring and detection is an integrated part of IFS' incident management processes – see section 11 below for more details

4.5 Data Segregation

IFS Cloud Services solutions can, dependant on the product, be fully integrated with the customer's corporate IT network using a secure virtual network, thus adding more security by reducing access directly from the internet.

As shown earlier in this document, the production environment is held separately from the test and demonstration environments in Azure, enabling the deployment of system changes to be properly validated in a secure, safe test environment prior to deployment to production. All IFS development and support environments are also separated from the customer's production environment with formal release management processes used to deploy system enhancements and corrections between environments.

5 CRYPTOGRAPHY

Cryptography is used within the IFS Cloud Services to help protect information both in transit and at rest.

5.1 Encryption in Transit

All connectivity to the IFS Cloud Services over the public internet, used for the establishment of the services by the IFS Cloud team, includes the use of RSA 2048-bit key encryption using TLS over HTPS. TLS provides strong authentication, message privacy and integrity (enabling detection of message tampering, interception and forgery), interoperability and ease of deployment and use. Perfect Forward Secrecy (FPS) protects connections between IFS' client systems and Azure cloud services by unique keys. SMB 3.0 is used by Virtual Machines running in Azure, ensuring data transfers are encrypted across Azure Virtual Networks.

Cloud services for IFS Applications are optionally configured to connect to customer IT domains using an Azure Virtual Private Network (VPN) gateway or ExpressRoute circuit. VPNs create a secure, encrypted tunnel (with the public internet as the underlying transport provider) to protect the privacy of data being sent into and out of Azure. Such site-to-site VPNs use IPsec for transport encryption and requires a customer on-premise VPN device with an external-facing IP address assigned to it. ExpressRoute circuits are secure private MPLS lines and do not utilise the public internet as the underlying transport provider.

Azure Key Vault is used to safeguard cryptographic keys and secrets that cloud applications and services use. Permissions to access keys are restricted to authorised users and services only.

5.2 Encryption at Rest

Server-side encryption of data at rest is used for disk storage within the Azure based service and which utilises service-managed keys to securely handle encryption. Disk encryption uses Windows Bitlocker to protect both operating system disks and data disks with full volume encryption. Encryption keys and secrets are safeguarded in the Azure Key Vault.

Where Azure SQL Database is utilised as part of the IFS Cloud Services, server-side Transparent Data Encryption (TDE) is used via the Always Encrypted feature. TDE encrypts data files in real time, using a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery. TDE protects data and log files, using AES and Triple Data Encryption Standard (3DES) encryption algorithms. Encryption of the database file is performed at the page level. The pages in an encrypted database are encrypted before they are written to disk and are decrypted when they're read into memory.

6 PHYSICAL & ENVIRONMENTAL SECURITY

For IFS internal physical and environmental security refer to section 8 of Part 1 which applies to IFS's own sites. Azure data center design and operational management is compliant with a broad range of international and industry standards including ISO 27001, FedRAMP, SOC 1, and SOC 2. Information on standards and certifications can be found at Azure Trust Centre. They also are compliant with country or region-specific standards including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls which these standards mandate.

6.1 Physical Security Access Controls

Azure data centers used by IFS to provide IFS Cloud Services are designed, built and operated by Microsoft in a way that strictly controls physical access to the areas where IFS Cloud customer data is stored. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the data center resources. Azure Data centers have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data center floor. Based on the information made available by Microsoft, layers of physical security are:

- **Access request and approval**. Access must be requested prior to arriving at the data center. Visitors are required to provide a valid business justification for the visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the data centers to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the data center required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

- **Facility's perimeter**. When arriving at a data center, visitors are required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the data centers, with a security team monitoring their videos at all times.

- **Building entrance**. The data center entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the data center and monitor the videos of cameras inside the data center at all times.

- **Inside the building**. After the visitor enters the building, they must pass two-factor authentication with biometrics to continue moving through the data center. If their identity is validated, they can enter only the portion of the data center that they have approved access to. They can stay there only for the duration of the time approved.

- **Datacenter floor**. Visitors are only allowed onto the floor that they are approved to enter. They are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the data center floor. Additionally, video cameras monitor the front and back of every server rack. When a visitor exits the data center floor, they again must pass through full body metal detection screening. To leave the data center, they are required to pass through an additional security scan.

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility. Information on physical security at Azure data center security can be found at Azure Trust Centre.

6.2 Physical Security Reviews

Physical security reviews are conducted periodically of the data center facilities to ensure that they are running in accordance with the specified requirements. All personnel associated with hosting of the physical data center do not have electronic access to the Azure systems within the data center, nor do they have access to the Azure collocation room and associated cages.

6.3 Physical Disposal of Devices holding Data

Customer data is electronically wiped from virtual machines by destroying the encryption keys that protect it, thereby making it inaccessible. The physical storage device upon which data (virtual machine images, data storage files, etc.) are wiped in accordance with NIST 800-88 compliant deletion procedures. For any hardware devices that cannot be wiped (e.g. faulty equipment), these are physically destroyed so as to render recovery impossible. This process comprises one of disintegration, shredding, pulverizing, or incinerating. The method used is determined by asset type. Records are retained regarding the destruction.

7 OPERATIONS

7.1 Monitoring Platforms

Multiple monitoring platforms are used to support IFS Cloud Services operations.

Microsoft Azure Monitor is used to manage and protect the infrastructure hosted in Azure. Azure Monitor collects data from managed sources into central data stores. This data includes events and performance data. After the data is collected, it is used to support the generation of event alert and their subsequent analysis. Azure Monitor also separates the collection of the data from the action taken on that data, so that all actions performed on the data are clearly identified and auditable.

In addition, 3rd party monitoring software is utilised to provide additional service and application monitoring and alerting capabilities to the operations. These platforms are fully owned and managed by IFS, with gathered monitoring data being treated in the same way as described above.

7.2 Automation and Templates

Automation tooling is used to automate frequently repeated tasks so as to reduce likelihood of errors and speed up their execution. This includes routine housekeeping tasks that are scheduled at regular intervals as well as one-off activities such as initial service creation. Automation is used in conjunction with service templates so that consistency, and hence reliability of services is enhanced.

7.3 Backup and Recovery

IFS Cloud Services include a robust, multi-level backup and recovery solution which comprises geographically separated backup storage away from the production environment. Certain aspects of the solution resilience are provided by the Azure services themselves and are built into the IT architecture of Azure. These include redundancy of critical elements of the service including compute, storage, network, power and environmental elements with the ability to automatically recover from a low-level failure should a hardware component develop a fault. Such resilience is provided at both the primary production data center as well as the secondary, geographically separated data center where backup/recovery storage is held. IFS Cloud Services customers are able to choose the primary data center locations from a list of options, this then auto selects an appropriate secondary data center location based on IFS and Azure requirements. The physical separation of the two locations is in accordance with industry best practice so as to provide suitable protection against major events such as natural disasters etc.

Backups are monitored to ensure successful completion and recovery processes are tested regularly so as to ensure that an IFS Cloud Services can be restored following a major system failure.

The standard retention period for backups is 14 days.

7.4 Disaster Recovery

Disaster recovery plans are in place for the IFS Cloud Services and are tested periodically to validate their effectiveness to recover a service in the event of a major failure. Backup and recovery services described in the previous section utilise the physical separation of the primary and secondary data center to enable the recovery of the service back to the primary data center or to a suitable alternative Microsoft Azure data center depending upon the nature of the particular disaster. In the event of a disaster where an entire Microsoft Azure data center becomes unavailable, re-configuration of the customer's connectivity into the service will be necessary and this will be assisted by IFS. Broader aspects of Disaster Recovery falling outside the scope of the IFS Cloud Service availability are a customer responsibility and need to be included within the customer's own Disaster Recovery planning and management processes.

7.5 Security Logging and Monitoring

IFS Cloud Services comprise security logging and monitoring at multiple levels. Microsoft Azure provides logging with associated monitoring at the hardware and infrastructure layer, and alerts and associated remediations are provided by Microsoft as part of the Azure service delivery. The IFS Cloud team monitor the health of the IFS Cloud Service at platform, application and network connectivity level, generating alerts using various monitoring tools that are reported to the IFS service management system for investigation and actioning as part of IFS Cloud Service management.

In additional to service logs and health monitoring provided by IFS, IFS Cloud Services provide the customer capabilities at the application level to log transactional events and utilise these as part of their own internal governance processes. Configurable by appropriate, authorised customer end users, such logging can be used to record system activity associated with sensitive areas of functionality or data. Such logging can then be inspected in order to determine what transactions have been performed in a particular timeframe and by whom. These facilities are in addition to the segregation of duties capabilities available with some of the services where segregation rules can be defined by the IFS Cloud Services customer to identify which system functions should not be executed in combination by a single system user and then report on a defined users who are in non-compliance with these definitions.

7.6 Malware Protection and Patching

The IFS Cloud Services includes the deployment of anti-virus and malware protection services to protect the service components held within the IFS Cloud Services. These protection services are updated regularly with the latest virus definitions to ensure that the service remains protected against constantly evolving threats.

Operating systems and infrastructure components that make up the service are regularly patched to keep them up to date with the latest security vulnerability patches. Such patching is performed in combination by Microsoft and IFS according to defined patching and maintenance responsibilities.

Patching of IFS products, either to correct errors or to address identified security vulnerabilities is performed by IFS in consultation with the IFS Cloud Services customer so as to ensure that there is no conflict with a customer's operational use of the IFS products.

Malware protection and patching of end user computing devices and customer IT infrastructure, including communications equipment within the IFS customers domain providing access to the IFS Cloud Services, is a customer responsibility and is not performed by IFS.

8 COMMUNICATIONS

8.1 Customer connections to an IFS Cloud Service

IFS Cloud Services provide three different connection methods to the service, each suited to different situations:

- Public Internet (with or without IP whitelisting)
- VPN (Site to Site)
- ExpressRoute (MPLS based)

It is important that, whatever connectivity mechanism is chosen by the customer, it is reliable, secure and provides adequate bandwidth and acceptable latency. Not all IFS products support all connection methods, and selection of the appropriate method is agreed between IFS and the IFS Cloud Services customer either during the procurement or service implementation phase.

8.1.1 Public Internet Connections

IFS Applications, FSM and PSO clients can be exposed over the public internet, secured using TLS encryption (HTTPS). This enables users to access the client from anywhere with an internet connection. Public internet access is generally not encouraged for IFS Applications, as it exposes the system to the entire internet bringing a broad range of security challenges. If public internet access is required, IFS strongly recommended that IP whitelisting be implemented. This blocks access from any location except the customer's nominated IP addresses, providing an important additional layer of security. IP white-listing is implemented and managed as part of the service, but may not be viable in certain situations - in particular, if the customer's internet connection has a dynamic IP address or if users need to access the system from many unpredictable locations.

System integrations between IFS Cloud Services and other existing IFS Cloud customers IT services are limited when using only public internet access, as the integration mechanisms must be secure. Typically, only HTTPS based integrations (such as web services) are permitted. Integrations based on file transfers, database links, etc are not permitted over the public internet.

Network bandwidth and latency cannot be controlled when accessing over the public internet, and it is important that the customer's internet connection is extremely reliable.

8.1.2 VPN Connections

VPN provides an encrypted tunnel between the IFS Cloud Services servers and the customer's own network, effectively making the servers accessible at network level as if they were part of the customer's own internal network. Integrations are possible using VPN, as the secure tunnel provides encryption for integration traffic which would otherwise be unencrypted and insecure. A VPN solution is ideal for creating hybrid cloud solutions where customers need to be able to connect to the IFS solution seamlessly - for example, to integrate with a legacy on-premise system.

The public internet is still used as the network bearer, so bandwidth and latency cannot be controlled, and the customer's internet connection must be extremely reliable. The VPN service requires the customer to provide and manage a compatible endpoint on their network. A list of compatible devices can be provided by IFS as part of service implementation. Only "RouteBased" configurations can be used, "PolicyBased" configurations cannot be used. IFS are not able to support customers who uses devices that are not included on the supported device list.

Note that Point-to-Point or Point-to-Site VPNs are not supported.

8.1.3 ExpressRoute Connections

ExpressRoute is the Azure service which enables connections via private MPLS (Multi-Protocol Label Switching) circuits to the customer's internal network. ExpressRoute may be used for IFS Applications, and under some circumstances for FSM. PSO cannot utilise ExpressRoute.

As with VPN, ExpressRoute enables the IFS Cloud Services servers to be accessible at network level as if they were part of the customer's own internal network. ExpressRoute uses a private connection over a local telecoms provider's own network direct to the Microsoft Edge (Azure data center), without traversing the public internet. ExpressRoute/MPLS connections are more complex and costly than VPN or public internet connections, but can provide predictable, higher network bandwidth and lower latency. They also add an additional layer of security since the traffic is contained only within a private network, not the public internet.

Integrations between the IFS Cloud Services and other IFS Cloud customer systems are possible using ExpressRoute, as the connection is encrypted and private.

Both the customer's chosen telecoms provider and the Azure Data Centre being used must be compatible with ExpressRoute. A list of supported providers and data centers can be found on Microsoft’s website. IFS Cloud Services require a 'Private Peering’ ExpressRoute circuit type.

IFS Cloud Services can be linked to an existing customer ExpressRoute circuit subscription if the above requirements are met. ExpressRoute circuits established for the use of Microsoft Office 365 cannot be used for IFS, since these use 'Microsoft Peering'.

8.2 IFS Connection to Customer IFS Cloud Services

The IFS Cloud team need to connect to the customer’s IFS Cloud Services in order to implement, monitor, manage and maintain the service. To do this, IFS connect to the customer’s IFS Cloud Services using SupportNet. IFS SupportNet is secure point of termination for all LAN to LAN based customer connections and is used for both on premise and IFS Cloud Services customers. It utilises the industry standard Internet Protocol Security (IPsec) that authenticates and encrypts

data in transit sent over the internet connection between IFS' and the customer's domain in the form of a Virtual Private Network (VPN).

IPsec includes protocols for establishing mutual authentication between agents at the beginning of a connection session and negotiates the cryptographic keys, used whilst the connection exists, and that will encrypt the data in transit. IPsec provides network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption) and replay protection. If such facilities do not already exist within the customer's IT landscape, an IPsec VPN can be easily implemented using hardware, software or virtual devices, thereby helping provide flexible rapid deployment.

8.3 Internal Azure Communications

Communications between Azure internal components are protected with TLS encryption. In most cases, the X.509 certificates are self-signed. Certificates with connections that can be accessed from outside the Azure network are an exception, as are certificates for the Azure Fabric Controllers (FCs). FCs have certificates issued by a Microsoft Certificate of Authority (CA) that is backed by a trusted root CA. This allows FC public keys to be rolled over easily.

Azure implements host-based software firewalls inside the production network. Several core security and firewall features reside within the core Azure environment and which reflect a defence-in-depth strategy. Customer data in Azure is protected by the following firewalls:

Hypervisor firewall (packet filter): This firewall is implemented in the hypervisor and configured by the fabric controller (FC) agent. This firewall protects the customer's tenant that runs inside the Virtual Machine (VM) from unauthorized access. By default, when a VM is created to host the customer's IFS Cloud Services, all traffic is blocked and then the FC agent adds rules and exceptions in the filter to allow authorized traffic.

Native host firewall: Azure Service Fabric and Azure Storage run on a native operating system, which has no hypervisor and, therefore, Windows Firewall is configured with the appropriate sets of rules.

Host firewall: The host firewall protects the host partition, which runs the hypervisor that manages the Azure services utilised by IFS Cloud Services. The rules are programmed to allow only the FC and jump boxes to talk to the host partition on a specific port.

Firewalls that are implemented on all internal Azure nodes have three primary security architecture considerations:

- Firewalls are placed behind any load balancers and accept packets from anywhere. These packets are intended to be externally exposed and would correspond to the open ports in a traditional perimeter firewall.
- Firewalls accept packets only from a limited set of addresses. This consideration is part of the defensive in-depth strategy against DDoS attacks. Such connections are cryptographically authenticated.
- Firewalls can be accessed only from select internal nodes. They accept packets only from an enumerated list of source IP addresses.

9 IFS CLOUD SERVICE DEVELOPMENT & MAINTENANCE

9.1 Security Testing

9.1.1 IFS Product Development Testing

Security testing is performed at multiple stages within the development of an IFS Cloud Services. IFS Products themselves undergo extensive security testing during their development lifecycle within IFS Research & Development (R&D). Such testing checks for known security risks using industry best practice security frameworks including OWASP. The tests include checks for injection flaws, broken authentication, sensitive data exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), insecure deserialization, inclusion of components in the IFS Product with known vulnerabilities and lack of logging and monitoring facilities.

9.1.2 IFS Cloud Penetration Testing

In addition, IFS Cloud Services systems are tested on a dedicated, production grade environment hosted in Azure, built and maintained using the same architecture, design standards, tooling and processes employed in all IFS customers environments. The security testing environment comprises all standard, core product modules that are used to establish customer specific configured solutions.

Penetration testing of the IFS Cloud Services systems is performed annually or following any substantial change to the environment and is conducted by a trusted third-party security pen test partner. The penetration testing is conducted from the internet to replicate real world use cases. Both infrastructure and application testing is included within the testing scope. A formal report detailing issues found and associated severities is compiled as a result of the testing. Remediation and risk mitigation actions resulting from the penetration testing are identified and agreed corrective action plans established. Customer managed penetration tests are not permitted by IFS.

IFS Cloud Services customers may request a copy of the penetration tests performed on the same release or version that matches their deployment of the IFS Products as deployed in an IFS Cloud Services solution. The report will be provided under an appropriate non-disclosure agreement only and will be for the customer's information only.

9.2 Vulnerability Management

IFS products and services are scanned for known security vulnerabilities. Threat intelligence sources are also utilised to identify known weaknesses in the service elements that make up IFS Cloud Services. As described above, known vulnerabilities in Azure infrastructure and platform services and IFS product infrastructure components are patched automatically as part of IFS Cloud Services management. Security vulnerabilities identified within IFS products are analysed and security bulletins published on the IFS customer's support portal. The Security Bulletin includes:

- A summary of the nature of the security vulnerability;
- A rating of its criticality using industry standard CVSS scoring;
- The conditions required for exploitation (since not all conditions are applicable for all IFS customer solutions);
- Versions of IFS products/services to which the vulnerability applies;
- A description of the vulnerability and how it can be remediated.

Security bulletins will cover vulnerabilities in third party infrastructure components upon which IFS products are built, since these will be important for IFS customers running on-premise solutions. For IFS Cloud Services customers, details of how any risk will be mitigated within the IFS Cloud Services solution are also included within the bulletin. It should be noted that mitigation actions may differ between IFS Cloud Services and on-premise customers depending upon the nature of the specific vulnerability.

10 INFORMATION SECURITY & THIRD PARTIES

IFS operate formal supplier management policies and process which help govern the security of the products and services they provide. From supplier selection, through onboarding and including the day-to-day management of the supplier relationship supplier security is a key aspect of the supplier management process. Such processes include the use of supplier security questionnaires as well as the validation and inspection of any security certifications that may be held and are applicable to their scope of supply.

IFS Cloud Services is dependent upon very few suppliers for service delivery, the main supplier being Microsoft with the provision of the Azure service upon which IFS Cloud Services solutions run. IFS and Microsoft operate in close partnership and supplier management includes frequent meetings between the two parties at both a strategic and operational level. Defined routes for issue escalation exist as well as priority support should a significant incident occur.

11 INCIDENT MANAGEMENT

In accordance with its contractual, legal and regulatory obligations, IFS notify impacted customers without undue delay of any unauthorized disclosure of their respective customer data by IFS of which IFS becomes aware to the extent permitted by law.

IFS Incident Management processes have been designed to ensure that forensic information is preserved during the investigation of a security incident. IFS will not share information regarding the details nor nature of the incident other than with impacted parties unless it is required to do so.

12 COMPLIANCE

12.1 Audits and Reviews

Numerous audits and reviews are conducted on multiple service elements that make up the IFS Cloud Services. Such audits and reviews are conducted by both IFS internal independent audit and review teams as well and external consultancies and accredited organisations. The IFS Information Security Management System, including the IFS Cloud Security Management system is reviewed annually by external specialist agencies. This features as part of IFS' commitment to continuous improvement in the area of information security of its products and services and the assessments are conducted in accordance with industry best practice security frameworks including ISO 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, SANS 20 Critical Security Controls amongst others.

IFS is in the process of certifying IFS Cloud Services to ISO 27001 to demonstrate the robustness and security focused approach taken to providing and maintaining customer cloud environments. This certification will also include within its scope a number of elements of IFS internal shared services including Information Technology, Human Resource Management and Facilities Management.

As part of IFS supplier management processes, IFS reviews the security credentials of its suppliers, ensuring that they meet IFS requirements as part of the supplier onboarding process as well as ensuring that are maintained, which frequently includes validation of compliance by an accredited organisation in accordance with the suppliers certifications.

12.2 Microsoft Azure Compliance and Certifications

Various audits and certifications apply to the Microsoft Azure Platform details of which can be found here: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/. The following key security and privacy-related audits and certifications are:

- ISO27001 – https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27001?view=o365-worldwide
- ISO27018 – https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27018?view=o365-worldwide
- SOC 1, 2, and 3 – https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc?view=o365-worldwide
- Cloud Security Alliance (CSA) STAR Certification – https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-csa-star-certification?view=o365-worldwide
- EU-US and Swiss-US Privacy Shield Frameworks https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-us-privacy-shield?view=o365-worldwide

Further information can be found on Microsoft's Trust Center.

12.3 Exclusions

IFS Products, including IFS Cloud Services, by their nature can be used for many different business purposes. Some of these relate to regulated industries requiring particular certifications. IFS do not certify its products or services in accordance with such regulations and certifications, this being a customer responsibility as part of their procurement process and due diligence regarding supplier and product selection.

DOCUMENT REVISION HISTORY

Rev.	Date	Owner	Remarks
1	28/7/2020	Todd Williams	Initial release including Cloud Security

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.

IFS GLOBAL ISMS

IFS INFORMATION SECURITY MANAGEMENT

ABOUT IFS

IFS develops and delivers enterprise software for customers around the world who manufacture and distribute goods, build and maintain assets, and manage service-focused operations. The industry expertise of our people and solutions, together with commitment to delivering value to every one of our customers, has made IFS a recognized leader and the most recommended supplier in our sector.

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

#forthechallengers

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

Document Reference: CLOUDISMS17