PUBLIC

IFS Information Security – IFS Cloud Services Controls

IFS Global ISMS

Date:	30/08/2023
Revision:	7
Owner:	Director Cloud Engineering
Approved By:	Global Portfolio Director

Contents

1. IFS Cloud Information Security Management

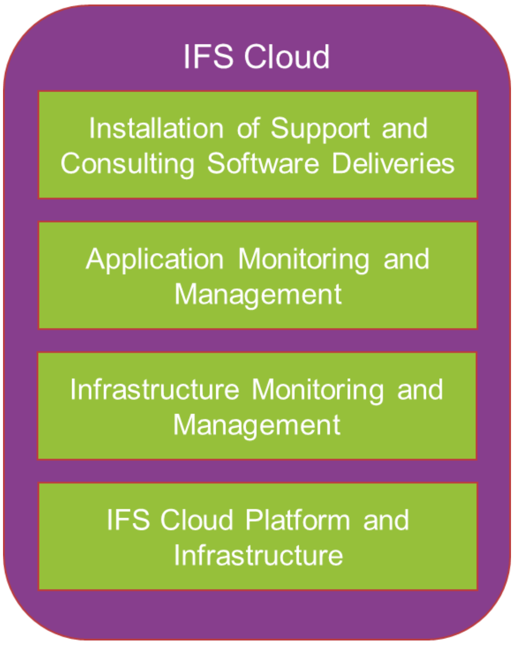
IFS' commitment to protecting its information security as well as that of its staff, customers, partners and suppliers stems from the most senior members of IFS at Board level. IFS have a central Information Security function, the purpose of which is to harmonize and coordinate the activities relating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

IFS have developed and continually improve an Information Security Management System (ISMS) specifically for the IFS Cloud Services which is certified to the requirements of the ISO 27001 Information Security standard. The IFS Cloud ISMS is fully integrated within the broader IFS ISMS, but itself covers the following key areas of the service:


IFS Cloud
Installation of Support and Consulting Software Deliveries
Application Monitoring and Management
Infrastructure Monitoring and Management
IFS Cloud Platform and Infrastructure

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 Services 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, considering 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.

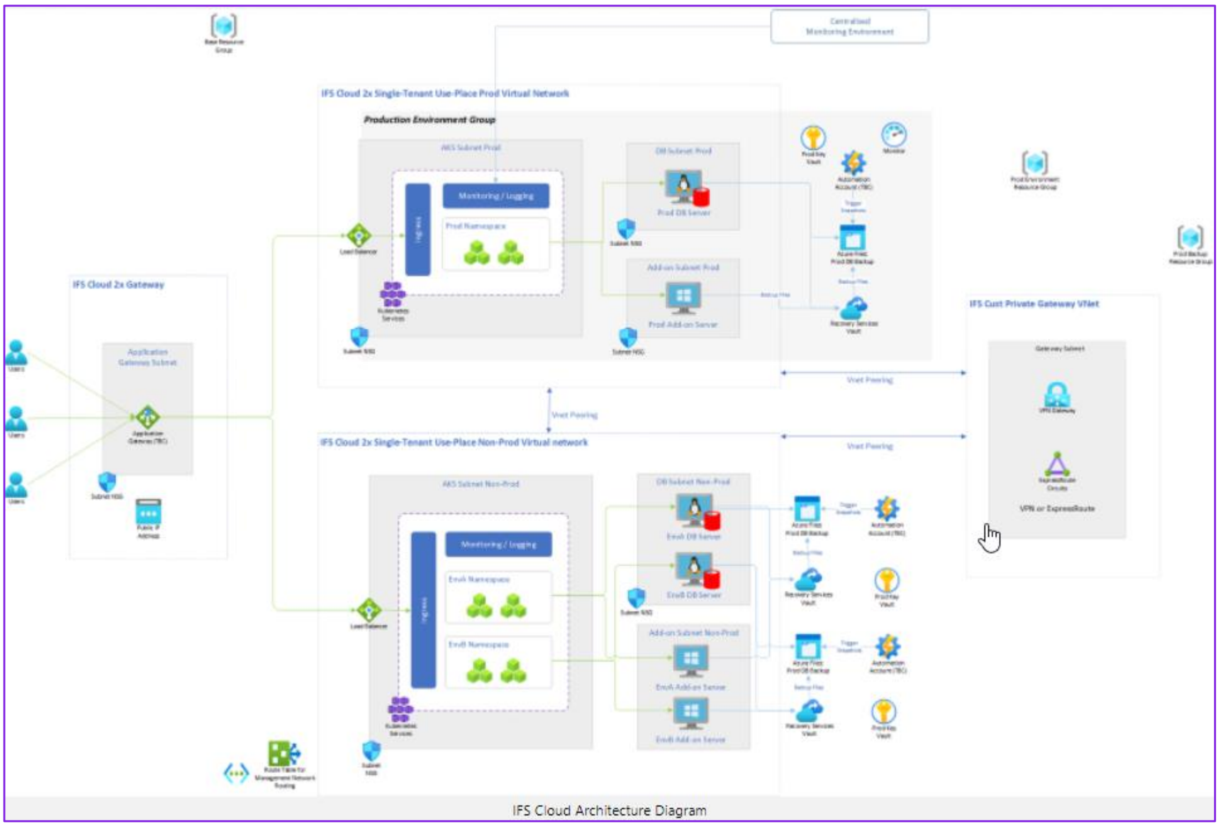
2.1. IFS Cloud

The IFS Cloud solution is deployed in a single-tenant Microsoft Azure subscription. The IFS Cloud Architecture Diagram below shows the default installations of the IFS Cloud software for the customer environment.

Environments provided by default:

- One (1) Production (PRD)
- Two (2) Non-Production
  - Support Testing (UAT)
  - Configuration (CFG)

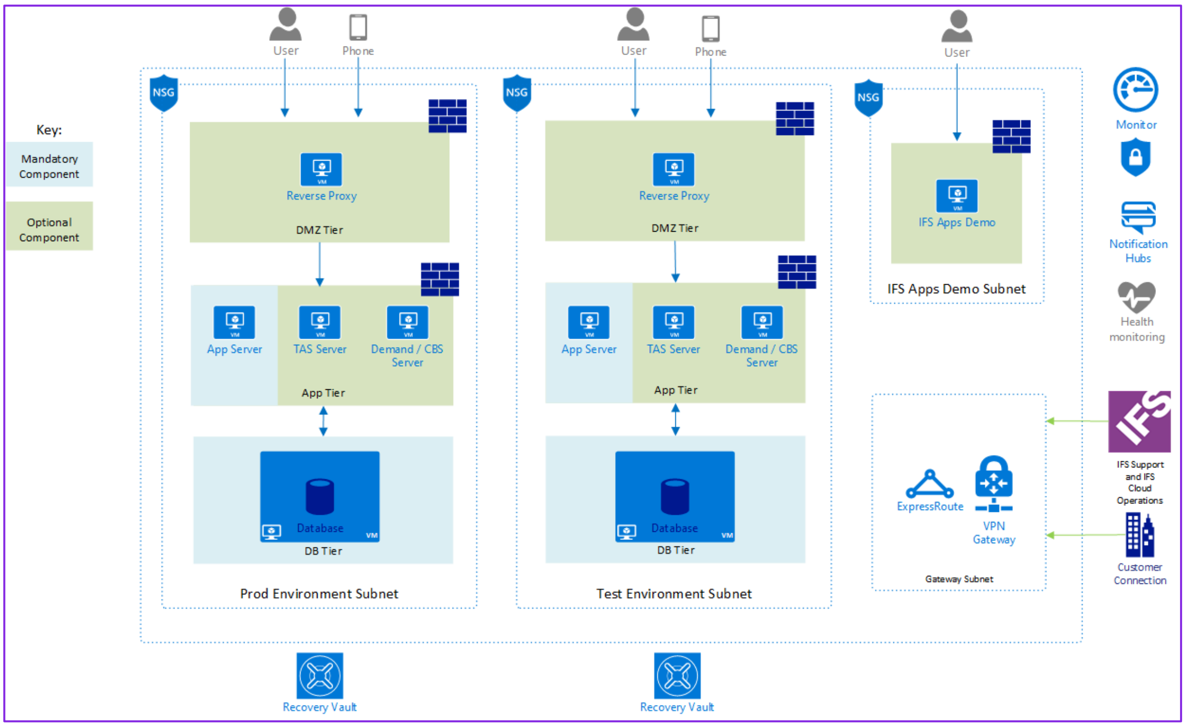
The solution comprises separate two non-production environments and production environment, each environment is comprising a database, application tier that is containerized and running in an AKS Cluster as shown in the architecture diagram below.



IFS Cloud Architecture Diagram

2.2. IFS Applications

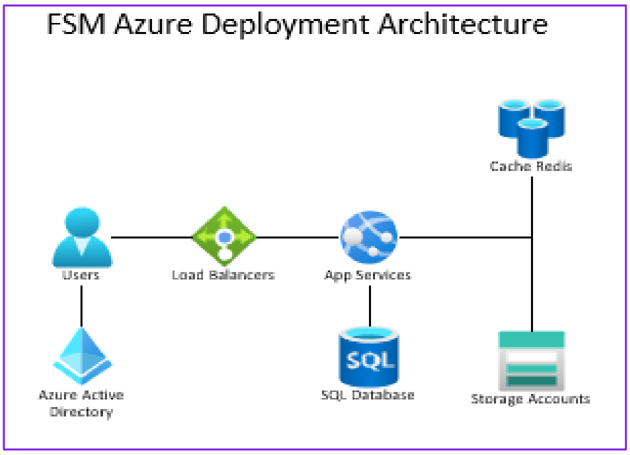
The IFS Applications solution is deployed in a single-tenant Microsoft Azure subscription. The solution comprises separate test and production environments, each comprising a database, application and DMZ tier as shown in the architecture diagram below. The solution also includes an optional demonstration 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).

2.3. Field Service Management (FSM)

The Field Service Management solution is deployed in a single-tenant Microsoft subscription, comprising of separate development, test and production environments, each built with their own dedicated Azure App Service & SQL database. Secure user access to application services is via HTTPS connection, 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.



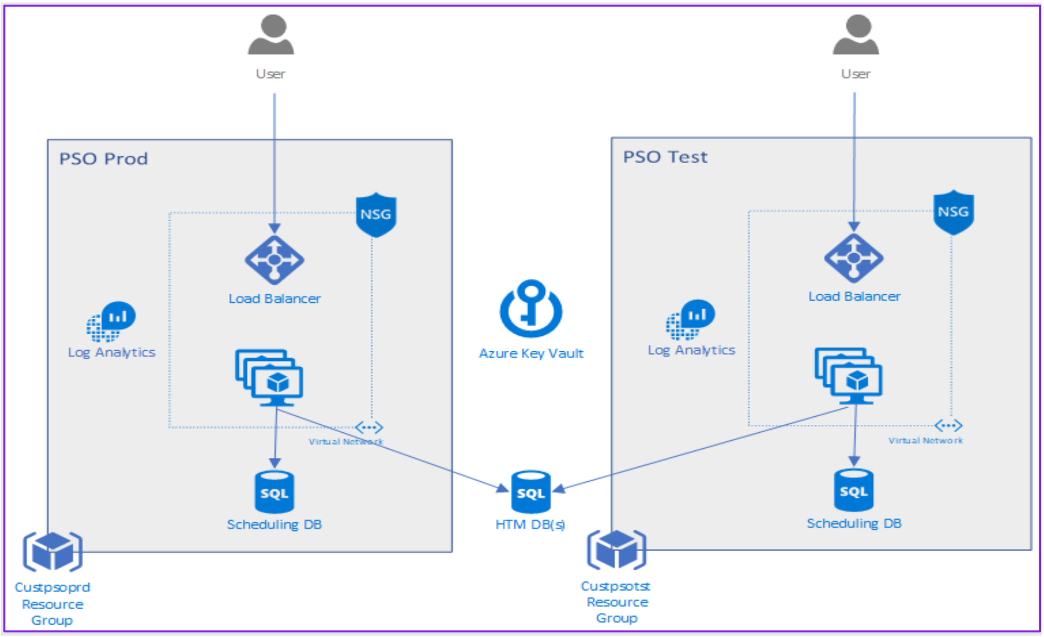
2.4. Scheduling (PSO)

The IFS Scheduling solution "PSO" (Planning & Scheduling Optimization) is offered standalone or connected to other IFS products utilising a default, but configurable connector as follows:

- IFS Applications
- Field Service Management
- IFS Cloud

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 where required, 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.

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. Section 14 below sets out the current list of sub-processors involved with the delivery of 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.

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 Center 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 Microsoft Defender For Cloud (MDFC) Azure service 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 (PFS) 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 require the customer's on-premises VPN device with an external-facing IP address. ExpressRoute circuits are secure private MPLS lines and do not utilize 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 Center. 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 Center.

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 gathers data which can be used to manage and protect the infrastructure hosted in Azure. This data includes events and performance data. After the data is collected, it can be used to support the generation of event alert and their subsequent analysis.

Third party monitoring software is utilised to provide additional service and application monitoring and also alerting capabilities to the operations teams. These platforms are fully owned and managed by IFS, details of which are described below.

IFS Cloud

The IFS Cloud application and the infrastructure it runs on are monitored via a Prometheus based platform used for event monitoring and alerting. Prometheus records real-time metrics in a time series database, with flexible queries and real-time alerting. The Prometheus server queries a list of data sources at a specific polling frequency. Data is aggregated across the data sources.

There is a Prometheus instance deployed in each customer environment as part of the Kubernetes cluster where the IFS Cloud application is running. Metrics are collected into a central data-store. Regardless of the source, incoming data is handled and alerted on based on defined rules that handle queries coming in from an analytics application which is used by the support teams. Data is transferred between the various endpoints via a private network link.

The only publicly accessible part of the platform is the UI which is the visualisation layer that allows users to view dashboards and, depending on their role and assigned permissions, may also query the data directly. Access to the UI is managed via Azure Active Directory. Only registered IFS users who have been granted access to the application will be able to login.

IFS ERP/EAM/PSO Applications

All IFS applications prior to the release of IFS Cloud, and the infrastructure they are hosted on are monitored by a system, network and infrastructure monitoring application. This provides monitoring and alerting services for services, switches, applications, and services. It provides alerts to user when a problem occurs and alerts a second time when the problem has been resolved. Alerts are notified to ServiceNow where they are handled by the Event Management Team.

Access to the monitoring application’s configuration is restricted to the monitoring and logging team, though configurations relating to newly onboarded customers is deployed via automated processes.

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. The timeframe from the point of enacting Disaster Recovery (DR) to the point where the services become available in the new location is defined under the Recovery Time Objective (RTO). The maximum amount of time between the most recent recovery point and point of failure is defined as the Recovery Point Objective (RPO). Both RTO and RPO objectives are included in the customer's contract. 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.

Utilizing the rapid evolution of the Microsoft Cloud security capabilities, IFS Cloud services are fully monitored by the Microsoft Defender for Cloud (MDFC). The state-of-the-art advance security features and recommended advisories are followed as per industry best practises. These features are embedded in the MDFC.

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, subject to the specific service version, provide three different connection methods:

- Public Internet
- 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.

Public Internet Connections

IFS Cloud 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. For IFS Cloud 21R1 and later, Public Internet – Open is the only supported connectivity type. For IFS Applications 9 and 10 Cloud services and FSM 6, IP whitelisting is supported. IP whitelisting is not supported and not required for IFS Cloud 21R1 and later since these services include other integrated protection methods to secure the internet connection.

Integrations 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 reliable.

VPN Connections

VPN provides an encrypted tunnel between the cloud 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 reliable. The VPN service requires the customer to provide and manage a compatible end-point on their network. Please note that only "RouteBased" configurations can be used, "PolicyBased" configurations cannot be used. IFS cannot support a customer who uses a device that is not listed as supported by Microsoft.

Note that Point-to-Point or Point-to-Site VPNs are not supported. Note also that VPN connections are not applicable for FSM and PSO services.

ExpressRoute Connections

As with VPN, ExpressRoute enables the cloud servers to be accessible at the 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 Azure Data Centre, 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 are possible using ExpressRoute, as the connection is encrypted and private.

ExpressRoute requires the customer to procure an ExpressRoute circuit from a local telecoms provider (physical link/connectivity). Both the customer's chosen telecoms provider and the Azure Data Centre being used must be compatible with ExpressRoute. IFS can link to an existing customer ExpressRoute circuit subscription provided the compatibility requirements are met. ExpressRoute circuits established for the use of Microsoft Office 365 cannot be used for IFS Cloud services, since these use 'Microsoft Peering'.

Note that ExpressRoute connections are not applicable for FSM and PSO services.

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. These security features reflect a defense-in-depth strategy within the Azure environment. 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

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.

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:

10. IFS Secure Product Development Lifecycle

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.

IFS customer solutions are established using a formal, controlled release of one of IFS's products to a dedicated deployment environment. 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.

- 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.

11. 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.

12. Security 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.

13. Compliance

13.1. 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 Cloud Services are included within the scope of our SOC 1 Type II (ISAE3402) and SOC 2 Type II (ISAE3000) annual reporting. A third-party accredited organisation performs an examination of IFS' system and suitability of the design and operation effectiveness of controls. Reporting periods typically follow a cycle of 1st October – 30th September and can be requested by customers to fulfil parts of their annual financial and security-based audit activities.

As part of the ISO 27001 certification of the IFS Cloud Service, included within its scope are a number of elements of IFS internal shared services that are subject to internal and external audit, 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.

More information on compliance and certifications can be found on the IFS Trust Center.

13.2. Microsoft Azure Compliance and Certifications

Various audits and certifications apply to the Microsoft Azure Platform details of which can be found here: Azure Trusted Cloud Compliance. The following key security and privacy-related audits and certifications are:

- ISO27001 – Information Security Management
- ISO27018 – Information Technology Security
- SOC 1, 2, and 3 – System and Organization Controls Reports
- Cloud Security Alliance (CSA) STAR Certification

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

13.3. 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.

14. Data Processing

This section identifies the data processing performed in connection with the operation and maintenance of the IFS Cloud services including the sub-processors involved. Sub-processors involved with the implementation of the solution are not included within this document since they may vary on a customer-by-customer basis and consequently will be described in a separate statement of work.

14.1. IFS Affiliates

IFS Affiliates located in the EEA

Entity name	Reg no	Service description	Data Processing (see Section 4)	Control Measures	Country
IFS World Operations AB	556040-6042	Corporate Functions	Global IT Support	Intragroup Agreement including SCCs IFS ISMS	Sweden

IFS Affiliates located outside the EEA:

Entity name	Reg no	Service description	Data Processing (see Section 4)	Control Measures (see Section 5)	Country
IFS World Operations AB UK Branch	FC039108	IFS Corporate IT, Cloud Services	Global IT Support IFS Cloud Services R&D Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	United Kingdom
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 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 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

14.2. Global Third-party Sub-processors

Global Third-party service providers located in the EEA

None

Global Third-party service providers located outside 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 management of Encryption keys within the EU	Data center location will be specified in the contract with customer
TechMahindra	Consulting services	IFS Cloud Service Support	IFS Partner DPA Management in accordance with IFS ISMS IFS Monitoring & Detection Containerised environments managed by IFS	India
ServiceNow	Support platform	IT Service Management Toolset	Service Now Security Management System certified in accordance with ISO 27001, SOC 2 Type 2 report	Netherlands & Ireland

14.3. Third-Party Software and Software as a Service Providers

None

14.4. 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

Where IFS customers choose the IFS Cloud service, their IFS products that form their solution are hosted in Microsoft Azure datacentres. For European customers, these data centres will be located within the EEA in order to limit the extent of any transfers of personal data outside of the EEA. Selection of the datacentres that form the solution is made with the agreement of the IFS customer.

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 customer 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.

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

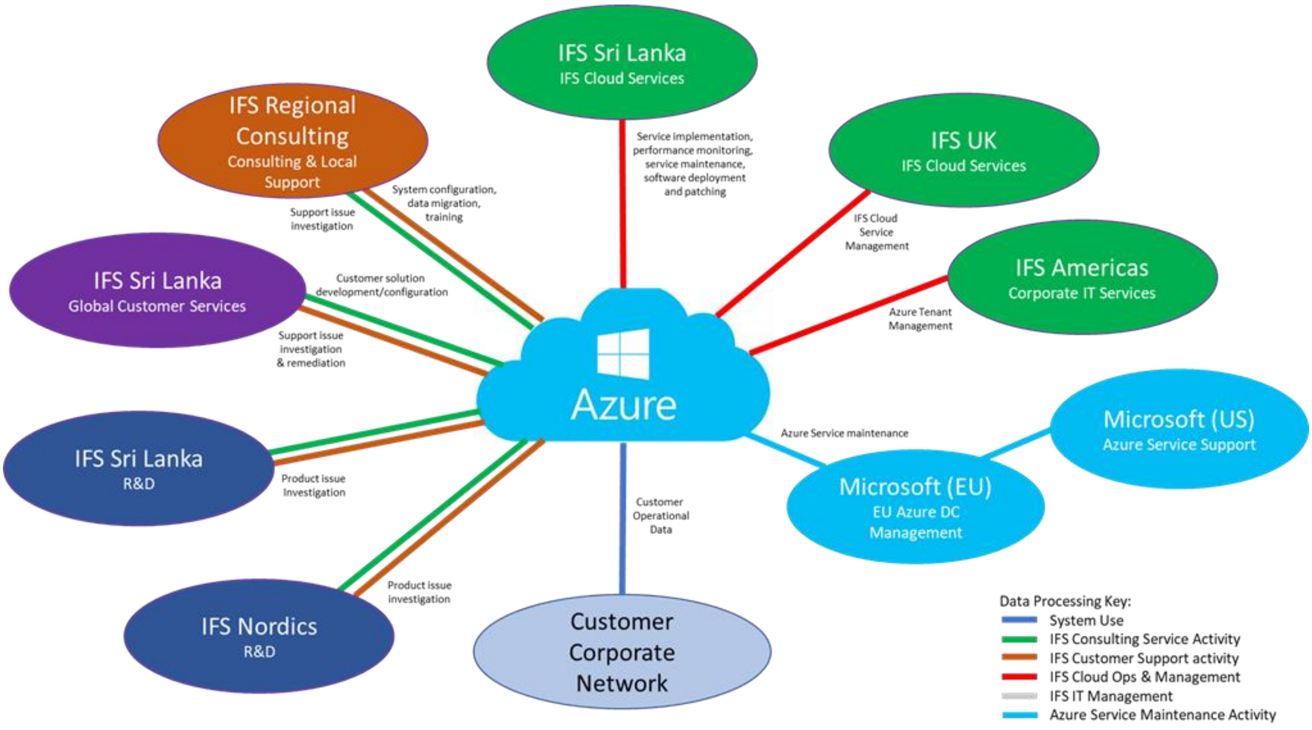
Microsoft do not have access to applications within the virtualized environments within which the IFS products that make up our customer solutions run. They therefore do not have access to customer production data held within IFS Cloud solutions. However, since Microsoft staff have elevated permission 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.

14.5. Data Flows

The following diagram shows the data flows between each entity associated with the implementation and support of the IFS Cloud SaaS solution:


IFS Sri Lanka
IFS Cloud Services
IFS Regional Consulting
Consulting & Local Support
Service implementation, performance monitoring, service maintenance, software deployment and patching
IFS UK
IFS Cloud Services
System configuration, data migration, training
Support issue investigation
IFS Cloud Service Management
IFS Sri Lanka
Global Customer Services
Customer solution development/configuration
IFS Americas
Corporate IT Services
Azure Tenant Management
Support issue investigation & remediation
Azure
Microsoft (US)
Azure Service Support
Azure Service maintenance
IFS Sri Lanka
R&D
Product issue Investigation
Microsoft (EU)
EU Azure DC Management
Customer Operational Data
Product issue investigation
IFS Nordics
R&D
Customer Corporate Network
Data Processing Key:
System Use
IFS Consulting Service Activity
IFS Customer Support activity
IFS Cloud Ops & Management
IFS IT Management
Azure Service Maintenance Activity

Document Revision History

Rev.	Date	Owner	Remarks
1	28/7/2020	Todd Williams	Initial release including Cloud Security
2	1/3/2021	Richard Rogers	Annual Review
3	21/5/2021	Todd Williams	Updated to reflect IFS current certification status
4	30/6/2022	Shakir Khan	Updated with latest control descriptions
5	12/1/2023	Richard Rogers	Correction of typographical errors
6	27/6/2023	Richard Rogers	Updated Sub-processor list to change TCS to TechMahindra
7	30/08/2023	Richard Rogers	Clarification regarding service connections methods for various service versions

Distribution & Document Handling

This document is intended for use by IFS customers and partners and is shared openly on the IFS website.

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