IFS Information Security – IFS Cloud Services Controls

IFS Global ISMS

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-focused 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 improved 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:

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.

High Availability Solution for IFS Products

High Availability (HA) in IFS environments ensures continuous operation, eliminates a single point of failure, and maintains service levels even during component failures. IFS delivers HA capabilities across its Cloud, on-premises, and hybrid deployments by combining redundant infrastructure, load balancing, and tier separation. The overarching objectives are to mitigate unplanned downtime, support seamless failover, and enable predictable performance underload. (Starting from version 25R1 this solution is made available to the clients)

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

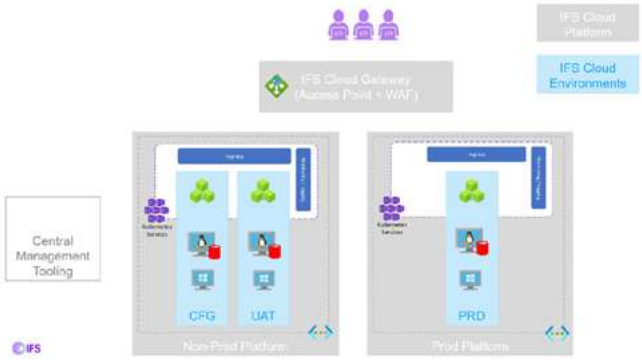
The IFS Cloud solution is deployed in a single-tenant Microsoft Azure subscription. The IFS Cloud Architecture Diagram below shows the default installations of the IFS Cloud software for the customer environment.

Environments provided by default:

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

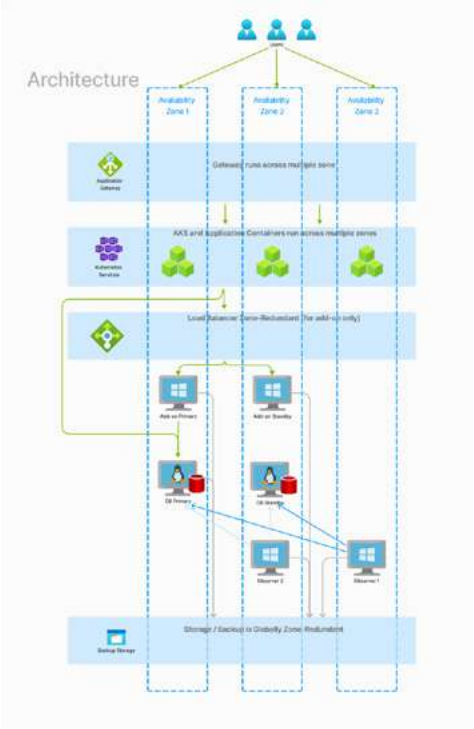
2.1.1. IFS Cloud version 25R1 and prior

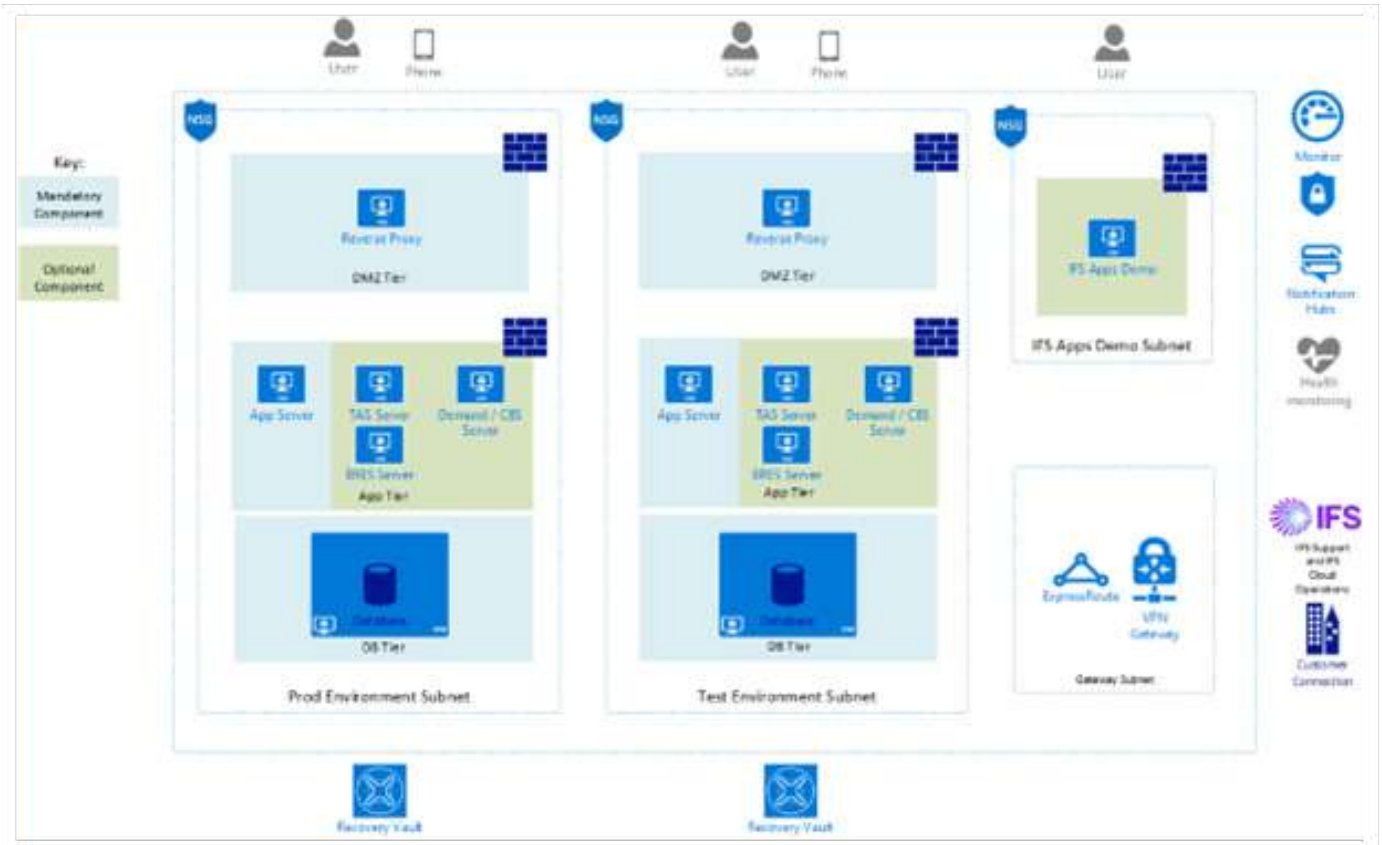
The solution comprises separate two, Non-Production environment and a Production environment, each environment comprising a database, application tier that is containerized and running in an AKS Cluster as shown in the architecture diagram below.



2.1.2. IFS Cloud version 25R1 and above

IFS Cloud version 25R2 and above introduces a robust suite of AI-driven capabilities designed to enhance operational resilience, scalability, and high availability across enterprise functions. With the integration of IFS.ai, organizations benefit from predictive analytics, autonomous workflows, and intelligent copilots and optimize resource utilization. The platform's shift away from legacy reporting tools toward modern, cloud-native dashboards like Power BI and Lobbies supports real-time insights and continuous service delivery. IFS Cloud ensures systems remain agile, secure, and consistently available to meet evolving business demands.



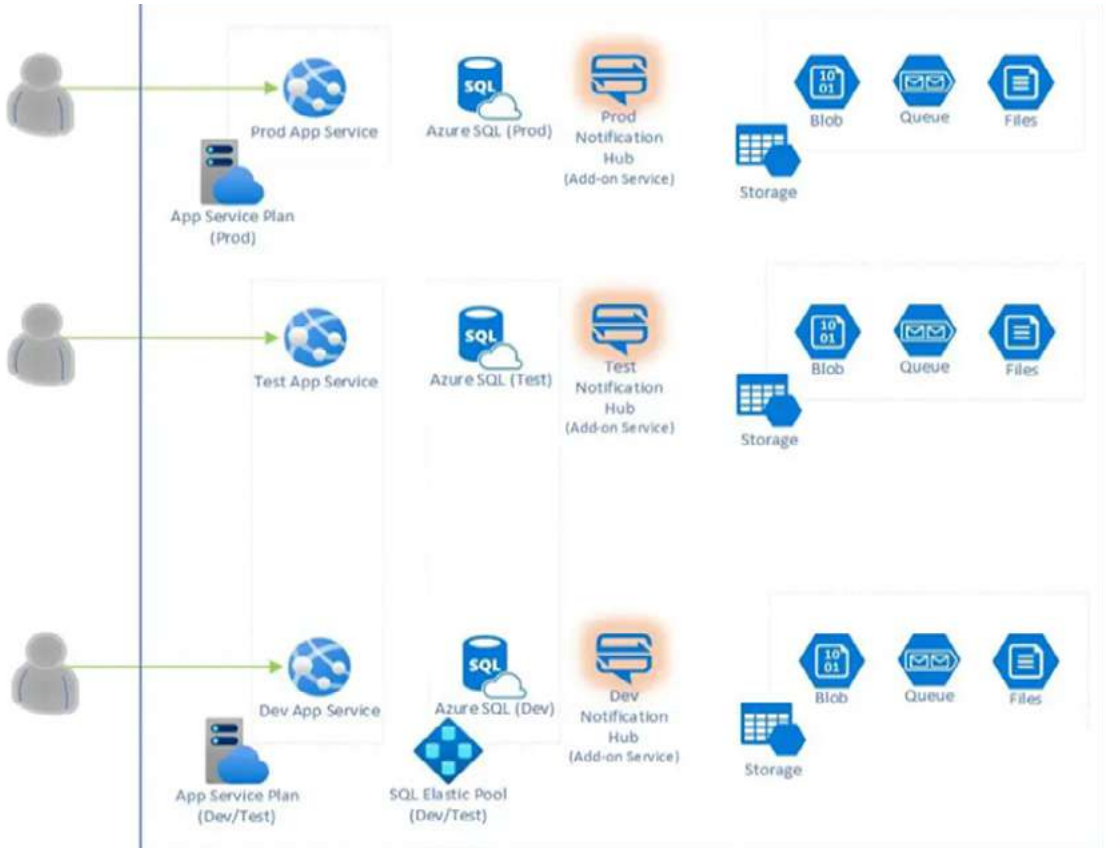


2.2. IFS Applications

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).

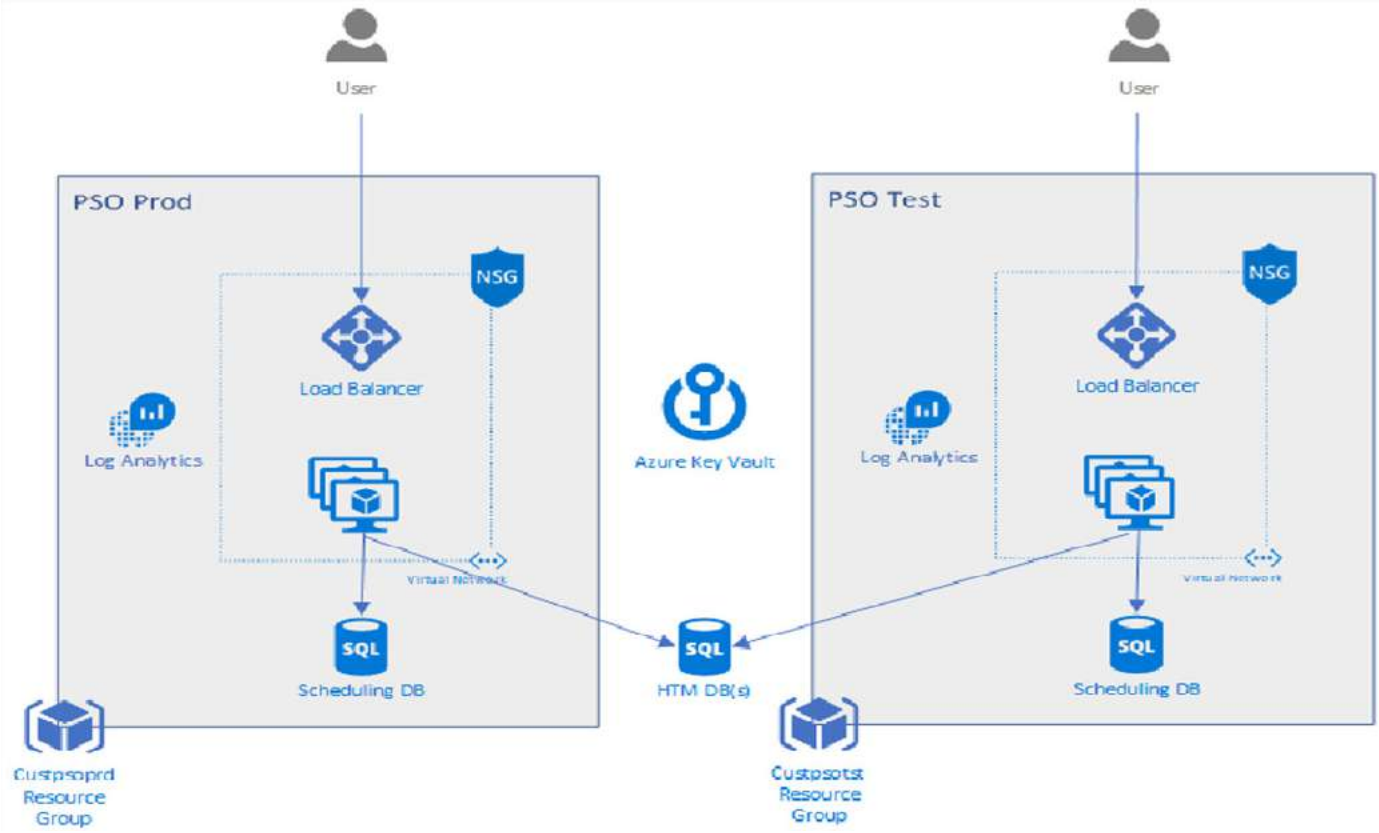
IFS Applications 10 (Apps10) reached the end of standard support on March 27, 2025, with extended support available until March 27, 2028. During this phase, users can access critical fixes and limited assistance, but no new features or fully regulatory updates.



2.3. 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 dedicated Azure App Service and 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.

IFS FSM version 6 is entering its end-of-life phase, with Extended Support commencing in January 2026 and transitioning to Restricted Support in January 2029. During Extended Support, customers will receive limited assistance and critical fixes, while new features and full regulatory updates will no longer be provided. As support phases out, organizations may face increased risks related to security, compliance, and system integration.



2.4. Scheduling (PSO)

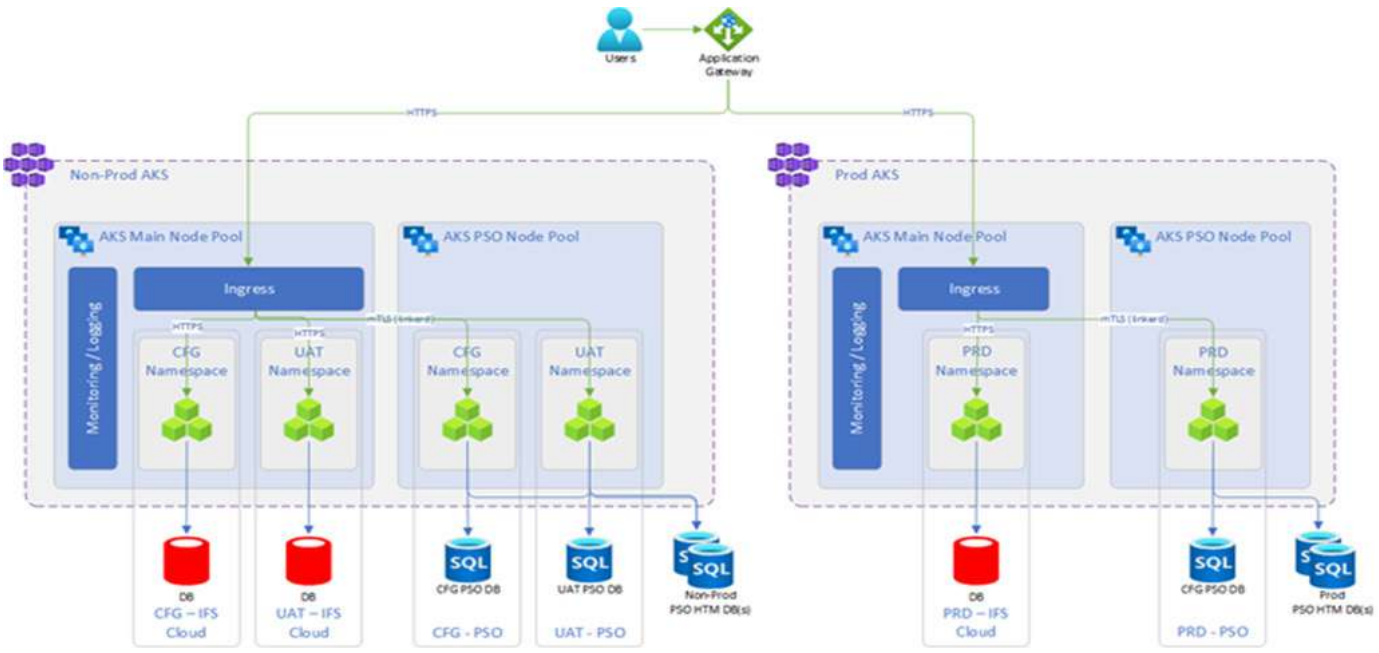
The IFS Scheduling solution "PSO" (Planning & Scheduling Optimization) is offered standalone or connected to other IFS products utilizing a default, but configurable connector as follows:

- IFS Applications
- Field Service Management
- IFS Cloud
- Existing Architecture for customer deployments pre Q4 2025

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 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 utilization of solution features such as single sign-on and establishment of a single integrated cloud/ on-premises virtual domain being dependent upon customer requirements and customer IT landscape constraints.



2.4.1 New Architecture for customer deployments post Q4 2025 (Core 25R2 Release)

The PSO deployment has been re-engineered to leverage the same Kubernetes containerized infrastructure and methodologies used for the IFS Cloud product, leveraging the latest technology to enhance service scalability, service availability, overall performance and streamlined management benefits of automated pipeline deployments.

Both deployment methods meet the same high standard of processors and sub processors outlined within the scope of this document in the context of the PSO (Planning Scheduling Optimization) product.

Deployment Offerings

1. IFS Cloud product + PSO within the same azure subscription.
2. IFS Cloud product + PSO + 'High Availability' within the same azure subscription.
3. PSO Product (standalone) deployed in a dedicated Azure subscription, integrated with a data master solution of choice via https.

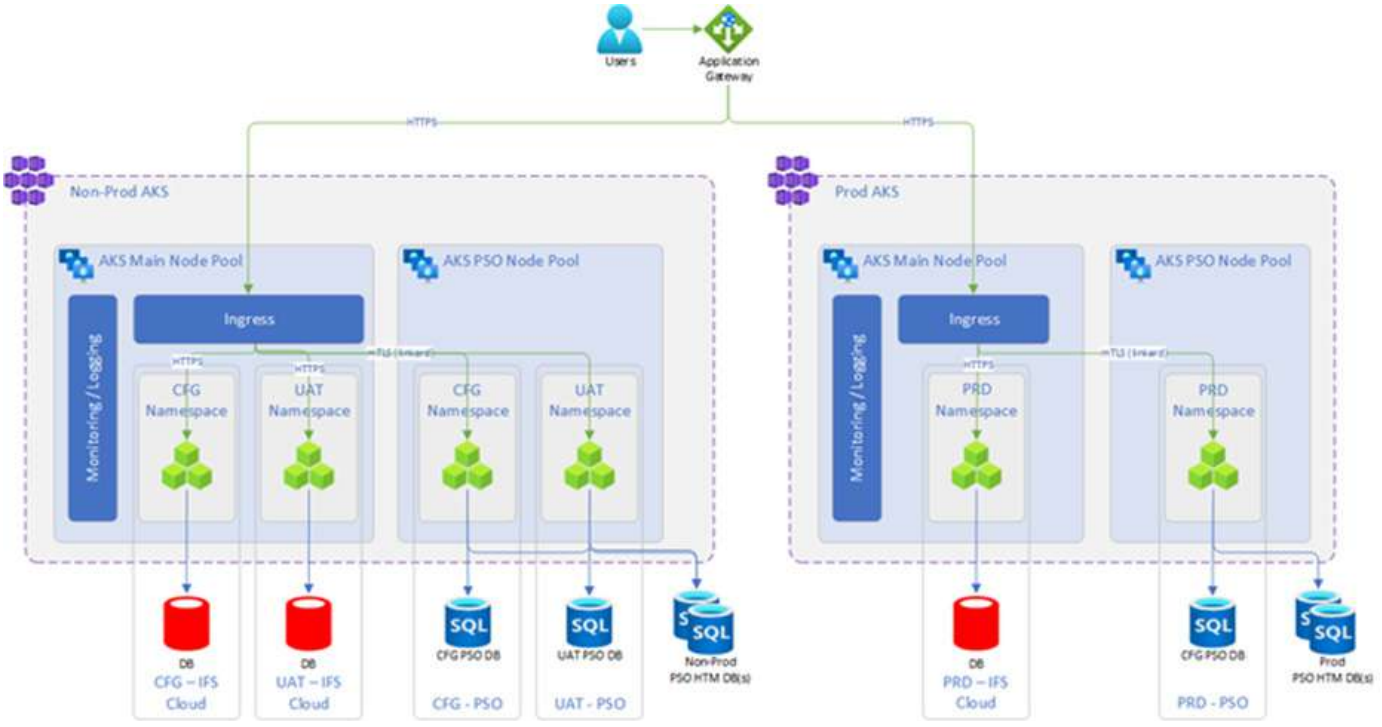
2.4.2. PSO and IFS Cloud integrated Product (25R2 Release)

The PSO product we previously implemented will serve as a scalable solution, primarily because it leverages Azure Kubernetes Service (AKS) with automation through deployment pipelines. This integration enables dynamic scaling based on workload requirements, streamlining operations and improving resource efficiency.

It can also be connected with other services or modules to support broader business needs, including monitoring, logging, and performance optimization.

The key distinction lies in its shift from manual resource provisioning to a fully automated, containerized infrastructure. By utilizing AKS, the system benefits from high availability, rapid deployment capabilities, and simplified management all driven through continuous integration and delivery pipelines.

The high-level architecture diagram of PSO and IFS Cloud integrated Product is outlined below.



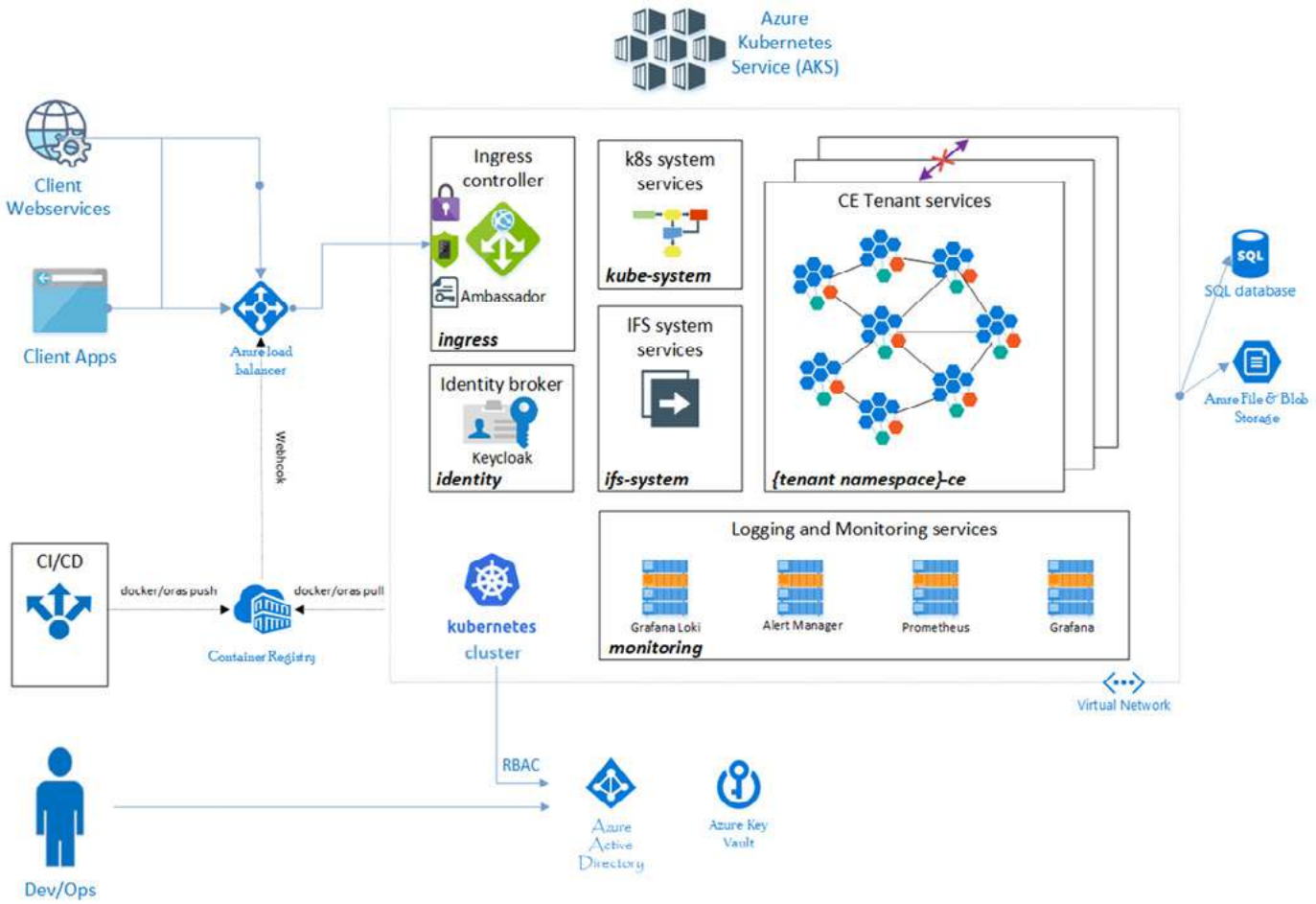
2.5 Customer Engagement (CE6)

Customer Engagement (CE6) is a modern, omnichannel contact center solution built to handle real-time customer interactions through a skill-based Automatic Call Distribution (ACD) engine. It enables intelligent routing of calls, messages, and tasks based on agent skills, availability, and business rules. The platform is designed to ingest data from multiple sources, either through automated queue progression or rule-based workflows, and deliver actionable, prioritized information to the most suitable agents, improving operational efficiency and customer experience.

The following diagram provides a high-level view of the CE6 system architecture:

CE6 adopts a multi-tenant, cloud-native, and distributed architecture to support scalability, isolation, and high availability. It runs on Azure Kubernetes Service (AKS), where each tenant is deployed in a dedicated Kubernetes namespace (example: tenant namespace}-ce) to ensure logical isolation and security. While the AKS cluster handles core platform services, media services for production (PRD) and preproduction (PPR) deployments are distributed across Google Cloud Platform (GCP) and AWS, allowing for regional optimization and redundancy.

This falls under the IFS standard support structure.



2.6 IFS.ai Platform

The IFS.ai Platform is the result of extensive operational experience with IFS Cloud and a strategic evolution beyond single-tenant architectures. It enables all IFS application teams to deliver cloud-native services with enhanced agility and scalability.

The IFS.ai Platform is architected as a multi-tenant environment. This design allows multiple customers to operate on shared infrastructure while maintaining strict logical and physical data isolation. This approach not only optimizes resource utilization but also significantly enhances security, monitoring, and compliance capabilities, ensuring robust protection of customer data across all services.

IFS.ai Platform deployment is based on Kubernetes clusters (AKS), with tenants distributed across multiple deployment stamps for scalability and resilience. Data is managed via sharded MongoDB clusters, and Kafka is used for data streaming. The architecture supports different application types (tenant, regional, global) and is designed to a large number of tenants and applications, with careful partitioning and automation to ensure performance, isolation, and operational efficiency.

Data Residency & Sovereignty

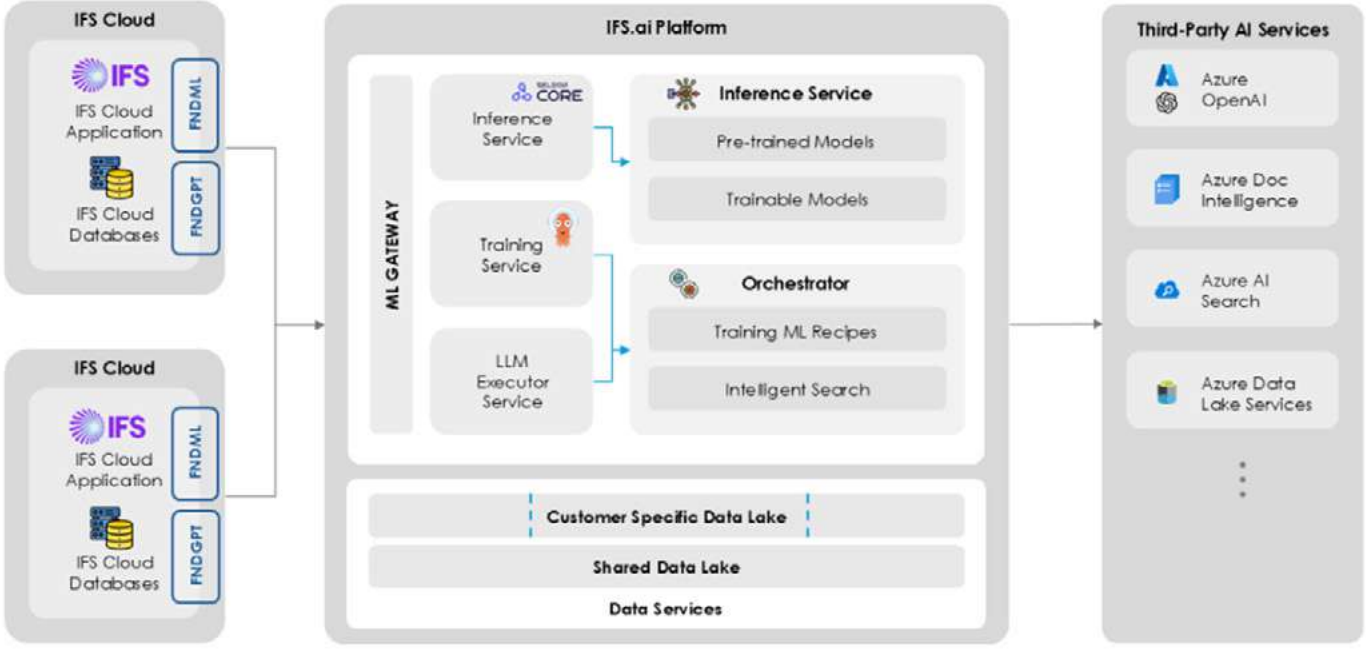
IFS.ai ensures compliance with data residency requirements through a combination of architectural design, deployment controls, and governance policies:

Regional Deployment Options: The platform supports both SaaS and connected on-premises deployments. This flexibility allows customers to choose where their data is processed and stored, ensuring alignment with regional data residency laws such as GDPR.

Tenant-Specific Isolation: Each customer's data and models are isolated at the tenant level. This includes training data, model artifacts, and inference outputs, which are never shared across tenants.

Zero Trust and Token-Based Access: Access to AI services is gated by customer-specific tokens, ensuring that only authorized users and services can access data within the permitted region.

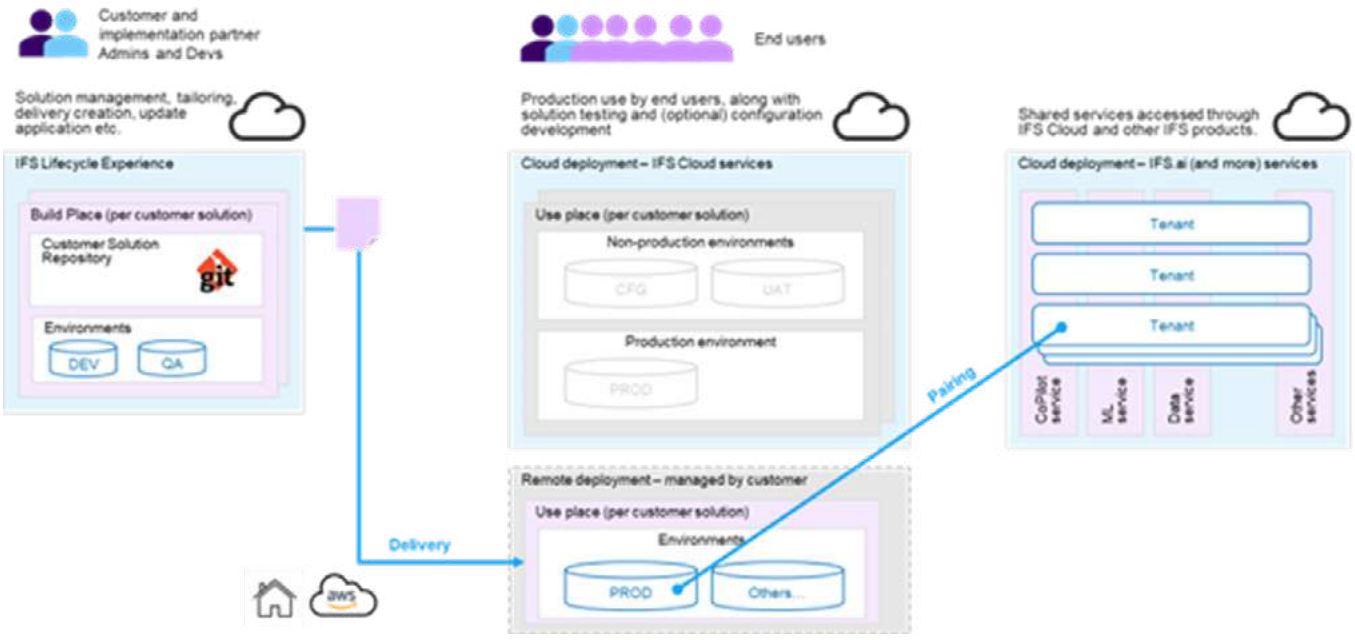
In addition, a formal governance model is in place to ensure that AI services are used responsibly and in compliance with legal requirements. This includes oversight of data residency, privacy, and ethical use.



2.7 Hybrid Model

The Hybrid Model (Remote customers) is designed to extend IFS.ai services to customers using the IFS Cloud Service, as well as those with existing remote deployments. This deployment approach enables access to all IFS.ai services, delivered via the IFS Cloud Service for remote environments. These services are cloud-hosted and managed by IFS yet remain accessible and usable within the remote deployment application layer.

The Hybrid Model can be deployed similarly to the traditional remote model, whether on-premises or in a customer or partner hosted cloud. The key distinction lies in the consumption of services; while the deployment remains remote, the services themselves reside in the IFS Cloud on Microsoft Azure and are fully managed by IFS.



3. Asset Management

3.1. IT Assets

The Azure Management Services 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 Azure Management Services team themselves have no direct interaction with Azure services themselves.

Microsoft Service management and service teams 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 the end of life.

Customer onboarding comprises the establishment of the Azure services that host the specific IFS Cloud Services solution. This is followed by the installation of software assets onto the Azure services then followed by the establishment of a 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 utilizing IFS' IT Service Management tools.

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

3.2. Information Assets

IFS Cloud Information assets fall into the categories below:

- Customer data
- IFS Cloud Service operations data
- Data Classification in AI Services
- Managing Data and Model Lifecycles in AI Services

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. 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 supports 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.

3.2.3. Data Classification in AI Services

Training data is handled with strict data governance principles, especially when it includes sensitive information such as PII. Training data used in the ML Service is stored in customer-specific environments. Access is controlled via unique access tokens that embed a customer ID, ensuring that no customer can access another's data.

Customers have complete discretion over the handling of training data. Data is discarded after use unless the customer explicitly requests its retention. Machine Learning employs the concept of Recipes that define how data is transformed and used, including preprocessing steps that could include anonymization or filtering of sensitive fields.

Inference operations are treated with the same rigor as training:

- Inference Endpoints: These are customer-specific and tied to the same access token mechanism, ensuring that inference requests are isolated and secure.
- No Raw Data Retention: Inference processes do not store raw input data. Instead, models operate on the data and discard it after processing.
- Auditability and Monitoring: The ML Service supports continuous monitoring and retraining workflows, which are essential for maintaining model integrity and compliance

3.2.4. Managing Data and Model Lifecycles in AI Services

AI services at IFS implement structured retention policies that balance operational needs with compliance and privacy. Training datasets are versioned and retained only as long as necessary for model development. As described previously, training data is discarded after use unless the customer explicitly requests its retention.

Models transition through states such as POSTED, TRAINING, TRAINED, and ACTIVE. Each state is logged and versioned, allowing customers to track changes and roll back if needed.

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 categorized with a sensitivity level that defines their access to Azure hosted services and data utilized 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 requires the use of administrative level accounts which provide access to the Azure services and platforms that underpin 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.

IFS access management model is based on Role-Based Access Control (RBAC) to ensure the least privileged access and is further strengthened by Privileged Identity Management (PIM) to enforce just-in-time and approval-based elevation of administrative roles.

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. the 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 recognized that disabling accounts allocated to IFS may prevent delivery of the contracted services or fulfilling any applicable service level agreements.

Platform-Level Access Controls for IFS.ai

Access to AI models, training data, and APIs are controlled through a centralized identity system. All AI service requests are routed through a centralized gateway. As part of the CPL, this gateway serves as the first line of defense against unauthorized access.

Key security measures include:

- Centralized identity system with role-based access control (RBAC)
- Authentication and authorization for every AI service request
- Rate limiting to prevent abuse or overuse

4.4. Security 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 utilizes Microsoft Azure native 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.

The IFS Cloud Security Operations Center (SOC) team utilizes Microsoft Azure native monitoring and detection tools as part of its 24/7 monitoring services, supplemented by additional security and health monitoring tools at the application level. Alerts and incidents are integrated with IFS Service Management and Incident Management toolsets to enable fast and efficient responses to events requiring immediate action. Monitoring and detection form an integral part of IFS's incident management processes (see Section 11 below for further details).

4.5. Data Segregation

IFS Cloud Services solutions can, dependent 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.

Tenant Isolation in AI Services

Each tenant is issued a unique access token that includes a customer-specific identifier. This token is required to access any trainable ML model, ensuring that only the owning tenant can invoke or manage their models. Even when models are trained on customer data, they do not retain or expose raw data. Instead, they encode learned patterns into parameters, ensuring that the original data cannot be reconstructed from the model.

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 Management is used to safeguard cryptographic keys and secrets that cloud applications and services use. Permissions to access keys are restricted to authorized 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 utilizes 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 utilized 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

IFS Cloud Services are hosted on Microsoft Azure, leveraging data centers that are designed, built, and operated by Microsoft with strict physical access controls. These facilities are purpose-built to safeguard customer data and infrastructure, ensuring that only authorized personnel can access sensitive areas where IFS Cloud customer data is stored.

Microsoft employs a layered approach to physical security, significantly reducing the risk of unauthorized access to data center resources. Azure data centers feature multiple tiers of protection, including:

- Access approval at the facility perimeter
- Controlled entry at the building perimeter
- Internal building access restrictions
- Secure access protocols on the data center floor

These measures are complemented by:

- 24/7 surveillance and monitoring systems
- Biometric authentication and multi-factor access controls
- Strict visitor management procedures and audit trails
- Environmental controls and redundancy systems to ensure operational continuity

Microsoft's physical security protocols align with internationally recognized standards, including ISO/IEC 27001, SOC 1/2/3, and other compliance frameworks. These controls are continuously reviewed and enhanced by Microsoft's dedicated security teams to maintain the highest level of protection.

For further transparency and assurance, stakeholders are encouraged to review Microsoft's official documentation:

- **Microsoft Trust Center:** Overview of Microsoft's security, privacy, and compliance commitments
- **Azure Physical Security Overview:** Detailed explanation of Azure's datacenter security architecture
- **Datacenter Physical Access Security:** Specifics on access provisioning, monitoring, and enforcement

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 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. Observability

Our Observability capability provides end-to-end visibility into applications, infrastructure, and user experiences through industry-grade solutions. Leveraging leading platforms, we deliver unified monitoring, log management, metrics, and tracing capabilities. This enables proactive issue detection, accelerated root cause analysis, performance optimization, and compliance reporting. The observability framework reduces downtime, and improved customer experience while aligning service operations with business outcomes. These platforms are fully owned and managed by IFS, details of which are described below.

IFS Cloud

The IFS Cloud application and its underlying infrastructure are continuously monitored using enterprise-grade platforms designed for event detection, metric collection, and real-time alerting. These platforms capture telemetry data in a time-series database, enabling flexible querying and dynamic alert generation based on predefined thresholds.

Each customer environment includes a dedicated monitoring instance deployed within the Kubernetes cluster hosting the IFS Cloud application. This instance polls a defined set of data sources at regular intervals, aggregates the collected metrics, and stores them centrally for analysis. Regardless of origin, all incoming data is processed according to established alerting rules and surfaced through an analytics application used by support teams for proactive issue resolution.

Data transmission between endpoints occurs exclusively over private network links, ensuring secure and isolated communication. The only publicly accessible component of the monitoring platform is the user interface (UI), which serves as the visualization layer. This UI allows authorized users to view dashboards and based on their roles and permissions, perform direct queries.

Access to the UI is strictly controlled via Azure Active Directory. Only registered IFS users with explicitly granted permissions can authenticate and interact with the monitoring environment.

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 the 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 are deployed via automated processes.

7.2. Automation and Templates

Automation tooling is used to automate frequently repeated tasks to reduce the 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 includes 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 computer, 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 the best practice 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.

Offline Database Backup Service (Production only)

For customers that have compliance or regulatory requirements and need to store their production data at their premises or require a long-term data storage of their production data and database, this service will provide a weekly copy of the customers' production database.

The service will securely store the copy of the backup in an Azure Secure Vault (blob storage) where the customer can download the database backup every week to the desired location or 3rd party vault.

7.4. Disaster Recovery

Disaster recovery plans are in place for 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 utilize 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 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 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 monitors 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 action as part of IFS Cloud Service management.

In addition 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 utilize these as part of their own internal governance processes. Configurable by appropriate, authorized 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 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 Microsoft cloud native security tools. The state-of-the-art advance security features and recommended advisories are followed as per industry's best practices. These features are embedded in the Microsoft cloud native security tools that are in place.

7.6. Malware Protection and Patching

The IFS Cloud Services incorporates a modern, extended threat detection and response capability designed to safeguard service components from evolving cyber threats. This advanced security infrastructure continuously monitors malicious activity and is routinely updated with the latest threat intelligence, ensuring robust protection across the cloud environment.

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 with Microsoft and IFS according to defined patching and maintenance responsibilities.

Patching 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 Connection
- Hybrid Data Transfer Security for AI Services

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.

Integration is 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 the internet, and it is important that the customer's internet connection is reliable.

VPN Connections

A VPN establishes an encrypted tunnel between cloud servers and the customer's on-premises network, enabling secure, network-level access to those servers as if they were part of the internal network. This secure tunnel also ensures that integration of traffic is encrypted, mitigating the risks associated with transmitting data over unsecure channels.

For IFS Applications 9 and 10, we provide a full VPN solution that allows secure private access to both the Application and Database servers. However, for IFS Cloud, VPN access is limited to Database and Addon servers only.

For IFS Cloud, we provide Site-to-Site VPN connectivity for UP customers and Point-to-Site VPN for BP customers.

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-premises 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 endpoint 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.

Hybrid Data Transfer Security for AI Services

IFS.ai supports hybrid deployments where data originates in OnPrem environments and is securely transferred to the cloud for training, inference, or storage.

The key mechanisms include:

- Azure Data Lake Integration: data from OnPrem systems is captured and staged in Azure Data Lake before being used in AI workflows. This staging area is secured with Azure-native encryption and access controls.
- Token-Based Access Control: Transfers are authenticated using scoped access tokens that embed tenant-specific identifiers. These tokens ensure that only authorized services can initiate or receive data transfers.

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 connects to the customer's IFS Cloud Services using SupportNet. IFS SupportNet is a secure point of termination for all LAN to LAN based customer connections and is used for both on premises and IFS Cloud Services customers. It utilizes 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 using TLS encryption. In most cases, the X.509 certificates are self-signed. Exceptions include certificates for connections accessible from outside the Azure network and for the Azure Fabric Controllers (FCs). FCs have certificates issued by a Microsoft Certificate Authority (CA), backed by a trusted root CA, which allows public keys to be rolled over easily.

Azure implements host-based Secure Network Gateways inside the production network. Several core security and gateway features reside within the Azure environment, reflecting a defense-in-depth strategy. Customer data in Azure is safeguarded by the following Secure Network Gateways:

Hypervisor Secure Network Gateway (packet filter): Implemented in the hypervisor and configured by the Fabric Controller (FC) agent. This gateway protects the customer's tenant running inside the Virtual Machine (VM) from unauthorized access. By default, when a VM is created to host IFS Cloud Services, all traffic is blocked until the FC agent applies the required rules and exceptions to enable authorized communication.

Native host Secure Network Gateway: Azure Service Fabric and Azure Storage run on a native operating system without a hypervisor. In this case, Windows Secure Network Gateway rules are configured appropriately to manage and control traffic.

Host Secure Network Gateway: Protects the host partition running the hypervisor that manages Azure services consumed by IFS Cloud Services. Access rules allow only Fabric Controllers and jump boxes to communicate with the host partition on designated ports.

Secure Network Gateways implemented on all internal Azure nodes aligned with three primary security architecture considerations:

Placement behind load balancers – Gateways accept packets corresponding to exposed ports, similar to a traditional perimeter firewall, while ensuring layered protection.

Restricted address sets – Gateways accept packets only from specific, limited address ranges as part of a defense-in-depth approach against DDoS attacks. Such traffic is cryptographically authenticated.

Controlled internal access – Gateways accept packets only from an enumerated list of trusted internal nodes and source IPs, further strengthening isolation and security.

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 the industry's best practice security frameworks.

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 an accredited service provider. 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 encouraged 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 utilized 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 analyzed and security bulletins published on the IFS customer's Service Portal.

10. IFS Secure Product Development Lifecycle

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

IFS operates 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 implementing and supporting the customer solution preserve the information security throughout. This is achieved using IFS' trusted lifecycle management tools, formal change management processes and coordination with customer activity.

Some customer solutions may involve the use of products developed by IFS partners. In such cases, the 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 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-premises 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-premises customers depending upon the nature of the specific vulnerability.

11. Information Security & Third Parties

IFS operates formal supplier management policies and processes 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.

IFS practices comply with ISO/IEC 27001 and SOC 2 audit requirements by incorporating third-party diversification and alternative delivery channels to minimize dependency and resilience risks. Additionally, we implement robust supply chain security controls to safeguard against counterfeit, tampered, or unauthorized components, ensuring operational integrity and compliance.

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 as external consultants and accredited organizations. The IFS Cloud Integrated Management System (IMS), comprising both the Information Security Management System (ISMS) and the Quality Management System (QMS), is certified to ISO 27001 and ISO 9001. These certifications are subject to annual external audits by accredited specialist agencies. This features as part of IFS' commitment to continuous improvement in the areas of information security and quality management of its products and services, and the assessments are conducted in accordance with industry best-practice frameworks including ISO 27001, ISO 9001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the 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 organization performs an examination of IFS' system and suitability of the design and operation effectiveness of controls. IFS Cloud reporting periods are assessed every 6 months, whereas other IFS cloud-based services and solutions are assessed every 12 months, with customer-facing reports being issued at those intervals. Reports are available to customers upon request to support their financial and security annual audit requirements.

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 they are maintained, which frequently includes validation of compliance by an accredited organization 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.

Data Ownership and Responsibility in AI Services

Training datasets are typically owned by the customer or the data originator:

- Segregated Customer-Provided Data: When customers upload datasets for training, they retain ownership of that data. The AI Services processes this data under strict access controls and does not use it to train shared models.
- Internal or Public Datasets: For pre-built models, IFS uses internally curated or publicly available datasets. These are governed by licensing agreements and are not customer specific.

Ownership of AI models depends on the model type and training context:

- Pre-Built Models: These are developed and maintained by IFS and are shared across tenants. They are trained on generic datasets and are not influenced by customer-specific data.
- Trainable Models: When a customer trains a model using their data, the resulting model is considered tenant specific. While IFS retains operational control (e.g., hosting, monitoring), the customer effectively owns the model logic and outputs.

IFS has implemented several safeguards to ensure data protection:

- No LLM Training on Customer Data: Customer data is never used to train, fine-tune, or re-train third-party large language models (LLMs). This is a strict policy applied across all LLM-powered use cases.
- Data Minimization and Redaction: For AI use cases involving personal data, IFS applies redaction and anonymization techniques to minimize exposure. This is especially relevant when customers are data controllers.
- GDPR Compliance by Design: The IFS ML Service is architected to operate without storing data, making it inherently GDPR-compliant. Regular AI audits are conducted to ensure ongoing alignment with legal and ethical standards.

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 in the EEA

Entity name	Reg no	Service description	Data Processing (see Section 4)	Control Measures	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
IFS Poland Branch	REGON: 017186081	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	Poland
Industrial and Financial Systems India LLP	AAO-2621	Marketing, Sales, distribution, delivery & support of IFS SW products via channel partner or otherwise	Marketing, Sales, distribution, delivery & support of IFS SW products via channel partner or otherwise	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS Private network	India
IFS World Operations India Pvt. Ltd	CIN-U72900WB-2022PTC255849	IFS Corporate IT, Cloud Services, R&D, Global Support, Sales & Presales Support, Marketing support	Product Implementation, Product Support, IFS Cloud Services, R&D, Global IT Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS Private network	India

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
Tech Mahindra	Consulting services	IFS Cloud Service Support	IFS Partner DPA Management in accordance with IFS ISMS IFS Monitoring & Detection Containerized 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

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 follows a standard implementation process using standardized implementation toolsets comprising the following activities:

- Discussion of business processes and practices.
- Design of system customizations.
- 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 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 IFS support agreement, IFS regional support teams and the IFS Global Support Organization 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 datacenters. For European customers, these data centers will be located within the EEA to limit the extent of any transfers of personal data outside of the EEA. Selection of the datacenters that form the solution is made with the agreement of the IFS customer.

The Managed Services Team assesses the customer environment in Azure 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's solution.
- Configuration of the solution including the establishment of system performance monitoring.
- Monitoring the system to ensure that it is compliance with its agreed service levels.
- Execution of backups to a secondary data center, 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 systems, 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 because of an agreed change with the customer.
- Service decommissioning in accordance with a process agreed with the customer.
- We do not offer customers the option to use their own encryption keys. We rely on Azure platform-managed encryption keys for data at rest, and TLS encryption over HTTPS for data in transit. The SSL certificates used for this purpose are managed by IFS through a standardized and centralized process.

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.

Restricted Cloud Services

IFS offers a Unified Support Service tailored for organizations subject to International Traffic in Arms Regulations (ITAR), enabling compliant use of its software and cloud services. The service includes operational and physical isolation, infrastructure managed by ITAR-trained US persons, and strict access controls to ensure only authorized personnel handle ITAR-controlled data. Deployments are hosted on Microsoft Azure Government Cloud to maintain data sovereignty and meet regulatory obligations.

For European customers, IFS provides the European Restricted Access (EURA) Service, designed to meet specific data residency and privacy requirements. This service ensures that customer environments are accessed only from EU, EFTA, and UK locations, with data hosted exclusively in regional data centers. EURA is available to IFS Cloud and IFS Platinum customers and involves an additional charge beyond standard maintenance and cloud subscriptions.

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 perform 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

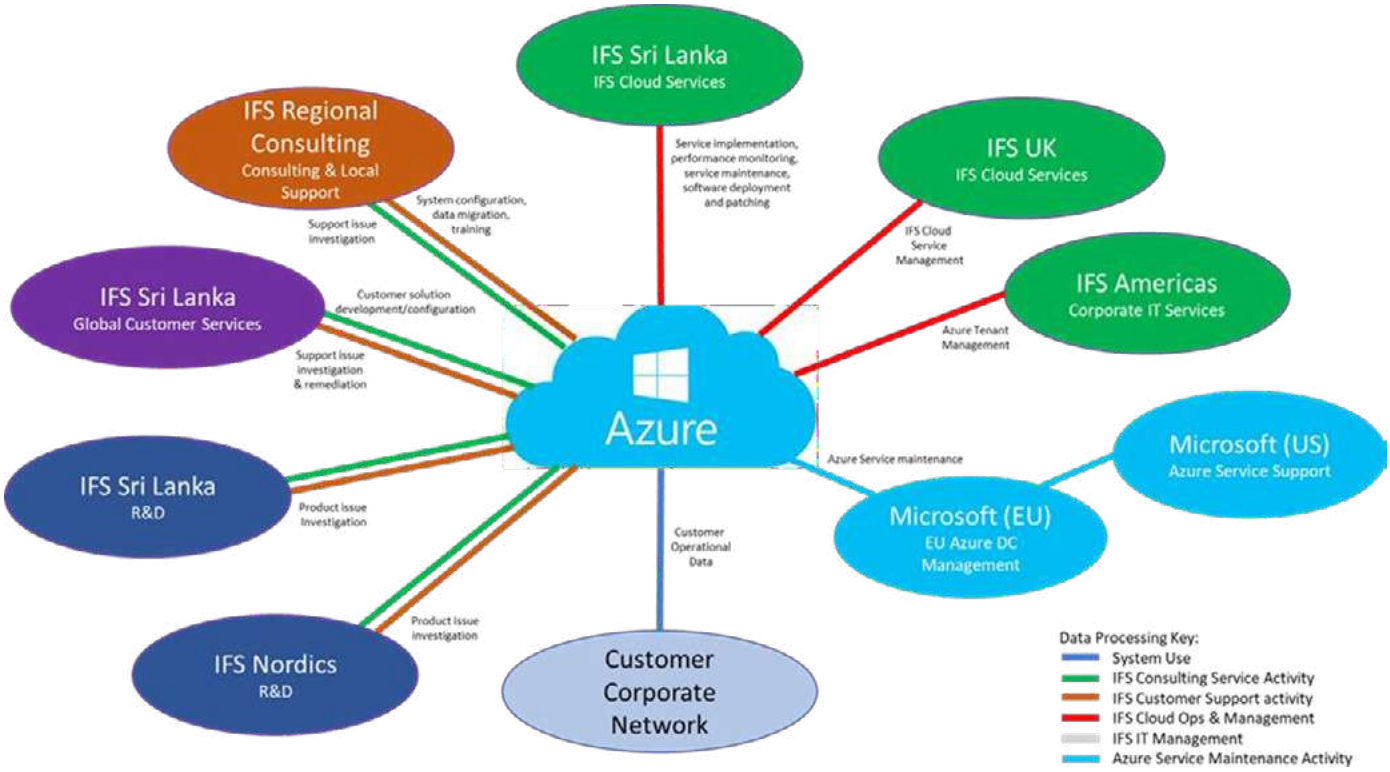
Microsoft does not have access to applications within the virtualized environments within which the IFS products that make up our customer solutions run. They therefore do not have access to customer production data held within IFS Cloud solutions. However, since Microsoft staff have elevated permission 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 to investigate performance issues). Microsoft's processes for managing 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:



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
8	30/09/2025	Shakir Khan	Updated with latest control descriptions and processes.

Distribution & Document Handling

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

Authorization & 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 is the world's leading provider of Industrial AI and enterprise software for hardcore businesses that make, service, and power our planet. Our technology enables businesses which manufacture goods, maintain complex assets, and manage service-focused operations to unlock the transformative power of Industrial AI™ to enhance productivity, efficiency, and sustainability.

IFS Cloud is a fully composable AI-powered platform, designed for ultimate flexibility and adaptability to our customers' specific requirements and business evolution. It spans the needs of Enterprise Resource Planning (ERP), Enterprise Asset Management (EAM), Supply Chain Management (SCM), and Field Service Management (FSM). IFS technology leverages AI, machine learning, real-time data and analytics to empower our customers to make informed strategic decisions and excel at their Moment of Service™.

IFS was founded in 1983 by five university friends who pitched a tent outside our first customer's site to ensure they would be available 24/7 and the needs of the customer would come first. Since then, IFS has grown into a global leader with over 7,000 employees in 80 countries. Driven by those foundational values of agility, customer-centricity, and trust, IFS is recognized worldwide for delivering value and supporting strategic transformations. We are the most recommended supplier in our sector. Visit ifs.com to learn why.

Production: IFS, November 2025.