PUBLIC

IFS Information Security - IFS ESM Assyst Service Controls

IFS Global ISMS

Date:	04/08/2022
Revision:	2
Owner:	Shakir Khan
Approved By:	Richard Rogers

Contents

1. IFS ESM Assyst 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.

2. IFS ESM Assyst Security Architecture

The IFS ESM Assyst environment is hosted on an Azure Public Cloud data centre(s) located in the customer's operational region, with off-site backups and GRS Storage accounts paired and replicated to a second Azure datacentre in the same region. IFS will not replicate nor move the data out of region without the customer's formal consent.

The only entry point to IFS ESM Assyst is via a Silverline F5 WAF that mandates HTTPS, TLS 1.2, and 2. Additionally, files can be uploaded to Azure dedicated storage using Microsoft secure transport utilities. The IFS ESM infrastructure support team may connect to a Bastion server secured by encrypted key access and locked to an IFS ESM source address. VPNs are not supported in any scenario.

The IFS ESM Assyst environment servers are dedicated to each installation in dedicated subnets, with vNet and NSG/RSG separation and internal firewalling at every level. The dedicated IFS ESM Assyst server(s) are provisioned n+1 to ensure maximum loading for the licence count during normal maintenance. There is no multi-tenancy for your data as each customer has their own dedicated servers, databases and dedicated URLs that are protected by customer provided SSL certificates.

All storage accounts and drives are encrypted, as are the databases and backups (TDE), with the keys stored in Microsoft Key Management Service (KMS). End user authentication is via SAML to the customer's own IdP services, with Azure AD, Microsoft ADFS, F5, Shibboleth and other implementations supported.

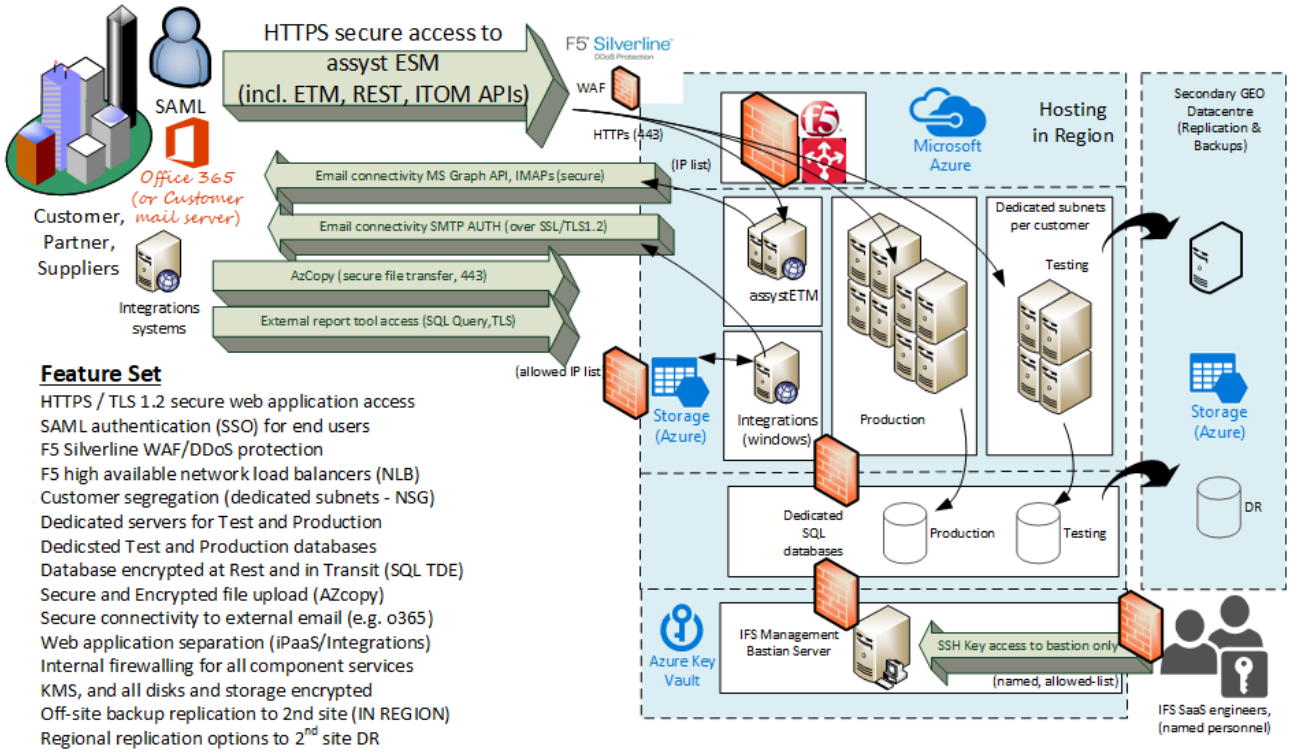


Figure 1: Typical customer implementation.

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 ESM Assyst Services are managed by the IFS ESM 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 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 ESM solution. This is followed by the configuration of authentication security and the involvement of Professional Services to complete the build-out of the system. All access is over the internet via https as defined above.

During the life of the IFS ESM Assyst solution, the IFS ESM 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 ESM Assyst solution, 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 ESM Assyst Information assets fall into one of two categories:

- Customer data;
- IFS Assyst 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 the production system is owned and are the responsibility of the IFS ESM Assyst customer. In execution of the IFS ESM Assyst Services agreement, it may be necessary for IFS to process information within this environment, for example when investigating a reported software issue that only manifests itself within the customer's data. IFS has implemented procedures designed to ensure that customer data is processed only as instructed by the customer. This carries 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 list of sub-processors involved with the delivery of the IFS ESM Assyst service.

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 ESM Assyst Services agreement, customers may request either the deletion or offboarding and deletion of its data as is defined in their contract. In this IFS typically will 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 ESM Assyst Service due to commercial, legal and technical factors.

At the point of termination of the IFS ESM Assyst 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 ESM Assyst Service Operations Data
IFS ESM Assyst Service operations data comprises the information associated with the management and operational delivery of the services themselves 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 ESM Assyst 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 ESM Assyst Service 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 ESM Assyst solutions.

4.1. Microsoft Access to IFS ESM Assyst 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 ESM Assyst Services. These role-based access permissions 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 ESM Assyst 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 services and are allocated on an "as required" basis in accordance with the user's job function, much like the principles applied by Microsoft RBAC (Role Based Access Control). These accounts comprise both Microsoft Azure accounts as well as non-data facing administration accounts for the various infrastructure components that make up the IFS ESM Assyst Service. These accounts are multi-factor authenticated to serve as an additional identity validation measure.

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

4.3. Customer Controlled Application Access

Access to IFS ESM Assyst Services requires authentication via one of the supported SAML mechanisms described in the IFS Assyst 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 ESM Assyst Service. The IFS customer has complete control of access in that they can enable and disable such accounts using application administrator accounts provided to them as part of the IFS ESM Assyst Service. Mechanisms should exist under the IFS customers control for granting access to the application where IFS is required to carry out support actions, otherwise this may prevent delivery of the contracted services or fulfilling any applicable service level agreements.

4.4. Monitoring and Threat Detection

IFS ESM Assyst Services are monitored for unauthorized intrusions attempts using a combination of network and WAF intrusion detection mechanisms. IFS utilises Azure Security Centre which provides threat protection using facilities including continuous discovery and monitoring of Azure

deployed resources and an assessment of their security status and any applicable security vulnerabilities that need remediation.

Microsoft Azure services perform their own active monitoring in accordance with defined SLA requirements. These tools are configured to provide alerts to Azure security personnel in situations that require immediate remediation.

The IFS team utilise Azure monitoring and detection tools as part of IFS' own service monitoring 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' security incident management processes.

4.5. Data Segregation

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 ESM Assyst Services to help protect information both in transit and at rest.

5.1. Encryption in Transit

All connectivity to the IFS ESM Assyst Services over the public internet, used for the establishment of the services by the IFS ESM team, includes the use of RSA 2048-bit key encryption using TLS at a minimum version of 1.2 over HTPS. TLS 1.2 provides strong authentication, message privacy and integrity (enabling detection of message tampering, interception, and forgery), interoperability and ease of deployment and use.

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 ESM Assyst Service, server-side Transparent Data Encryption (SQL 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. Encryption of the database file is performed at the database level.

6. Physical & Environmental Security

For IFS internal physical and environmental security please refer to the "IFS Information Security – Internal Controls" document which applies to IFS's own sites. Azure data center design and operational management is compliant with a broad range of international and industry standards

including ISO 27001, FedRAMP, SOC 1, and SOC 2. Information on standards and certifications can be found at Azure Trust Centre. They also are compliant with country or region-specific standards including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls which these standards mandate.

6.1. Physical Security Access Controls

Azure data centers used by IFS to provide IFS Assyst Services are designed, built and operated by Microsoft in a way that strictly controls physical access to the areas where IFS ESM Assyst 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 data center 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 the Azure Trust Centre.

6.2. Physical Security Reviews

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

6.3. Physical Disposal of Devices holding Data

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

7. Operations

7.1. Monitoring Platforms

Multiple monitoring platforms are used to support IFS ESM Assyst Services operations.

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

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

7.2. Automation and Templates

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

7.3. Backup and Recovery

IFS ESM Assyst 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 ESM Assyst Services customers can 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 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 to ensure that an IFS Assyst Services can be restored following a major system failure.

The standard retention period for backups is 12 months.

7.4. Disaster Recovery

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

7.6. Malware Protection and Patching

The IFS ESM Assyst Services includes the deployment of anti-virus and malware protection services to protect the service components held within the IFS ESM Assyst 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 ESM Assyst Services customer 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 Assyst Services, is a customer responsibility and is not performed by IFS.

8. Communications

8.1. Customer connections to an IFS ESM Assyst Service

IFS ESM Assyst Services connect over the public internet with or without IP whitelisting.

It is important that a reliable secure connection with adequate bandwidth and acceptable latency is available through the customers ISP. Not all IFS products support all connection speeds, and selection of the appropriate method is agreed between IFS and the IFS ESM Assyst Services customer either during the procurement or service implementation phase.

Public Internet Connections
IFS ESM Assyst Services are made available over the public internet and are secured using TLS 1.2, or above, encryption (HTTPS). This enables users to access the client from anywhere with an internet connection. IFS strongly recommended that IP whitelisting is implemented. This blocks access from any location except the customer's nominated IP addresses, providing an important additional layer of security. IP whitelisting is implemented and managed as part of the service but may not be viable in certain situations - in particular if the customer's internet connection has a dynamic IP address or if users need to access the system from many unpredictable locations.

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

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

8.2. IFS Connection to Customer IFS Assyst Services

The IFS ESM team need to connect to the customer's IFS ESM Assyst Services in order to implement, monitor, manage and maintain the service. In this regard, IFS connects to the customer's IFS ESM Assyst Services using HTTPS or via a Bastian server.

8.3. Internal Azure Communications

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

Hypervisor firewall (packet filter): This firewall is implemented in the hypervisor and configured by the fabric controller (FC) agent. This firewall protects the customer's tenant that runs inside the Virtual Machine (VM) from unauthorized access. By default, when a VM is created to host the customer's IFS Assyst 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 ESM Assyst 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 ESM Assyst Service Development & Maintenance

9.1. Security Testing

IFS Product Development Testing
Security testing is performed at multiple stages within the development of an IFS ESM Assyst Service. 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 Assyst Penetration Testing
In addition, IFS Assyst 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 ESM Assyst 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 are 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 supported by IFS.

IFS ESM Assyst 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 Assyst Services solution. The report will be provided under an appropriate non-disclosure agreement only and will be for the customer's information only. IFS reserves the right to redact an element of the penetration test report if the release of that element would compromise security, but the redaction would not be done to a level that would obfuscate any critical report messaging.

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 ESM Assyst Services. As described above, known vulnerabilities in Azure infrastructure and platform services and IFS product infrastructure components are patched automatically as part of IFS Assyst Services management. Security vulnerabilities when identified will be notified to the affected customers and authorities where appropriate.

10. IFS Secure Product Development Lifecycle

Product development at IFS is conducted by IFS ESM' 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.

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.

The IFS ESM Assyst Service is dependent upon very few suppliers for service delivery, the main supplier being Microsoft with the provision of the Azure service upon which IFS ESM Assyst 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 Security 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 ESM Assyst 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 taking account of industry best practice security frameworks. This includes ISO 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, SANS 20 Critical Security Controls amongst others.

As part of the planned ISO 27001 certification scope of the IFS ESM Assyst Service, there are a number 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.

13.2. Microsoft Azure Compliance and Certifications

Various audits and certifications apply to the Microsoft Azure Platform details of which can be found at the Azure Trusted Cloud Compliance site. 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 ESM Assyst 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 ESM Assyst 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 associated DCs	Data Centre location will be specified in the contract with customer

F5	Silverline WAF	Firewall Malicious entity detection	F5 Privacy Statement 801 5th Ave Seattle, WA 98104	Global

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

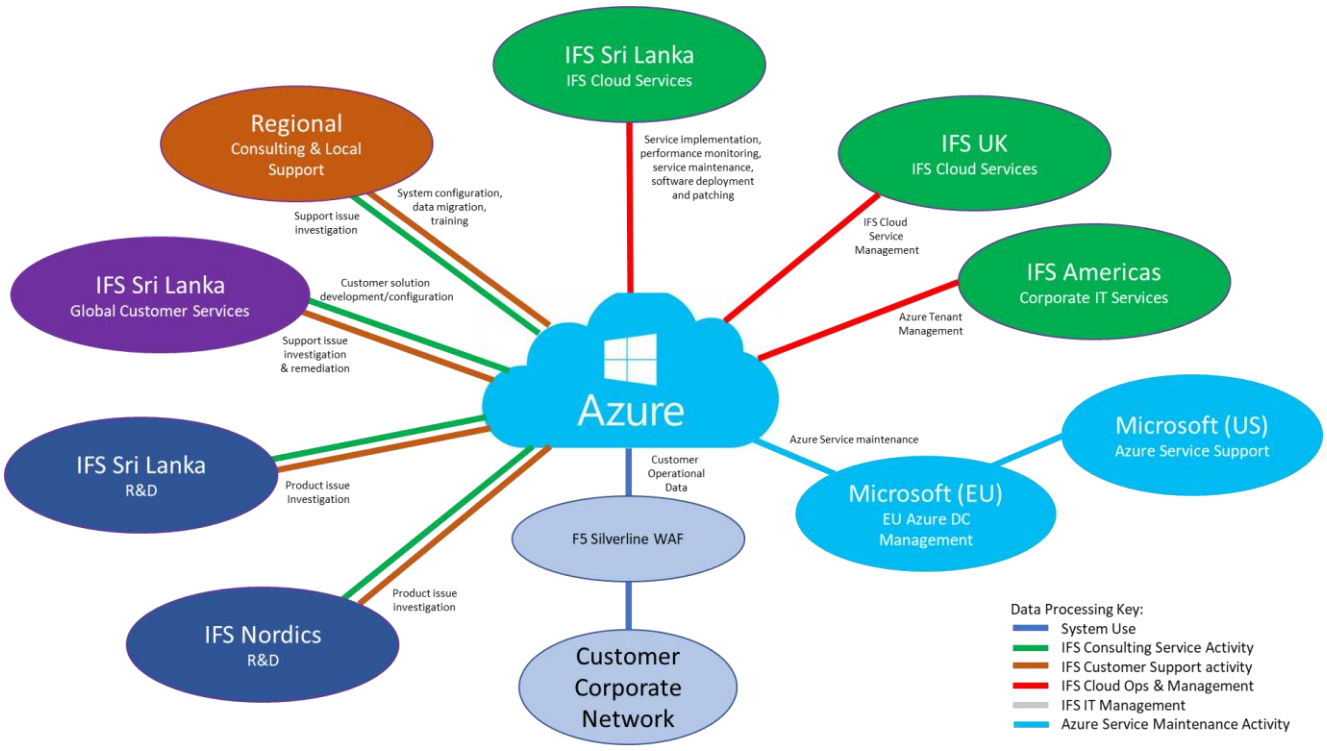
Microsoft do not have access to applications within the virtualized environments within which the IFS products that make up our customer solutions run. They therefore do not have access to customer production data held within IFS Cloud solutions. However, since Microsoft staff have elevated permission 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 tbhan 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	18/03/2022	Shakir Khan	Initial version covering IFS ESM Assyst
2	04/08/2022	Richard Rogers	Minor edits to as part of periodic review.

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