Payment Hub Standard Edition

Service Description

Contents

Introducing the Payment Standard Service

The centralization of payments processing has long been a costly, complex, and resource-intensive effort – and treasurers with many international business operations and banking partners can struggle to establish standardized, secure connectivity channels.

FIS introduced its “Payment Hub - Standard Edition” to address such requirements out-of-the-box. The solution offers a **fully managed payments platform** that centralizes all aspects of global payments processing. It acts as a bank connectivity hub, connecting your treasury and finance technology infrastructure to your banking partners in a scalable and secure manner, while a centralized team maintains a pre-built library of bank connection protocols and formats to simplify the bank communication set-up process.

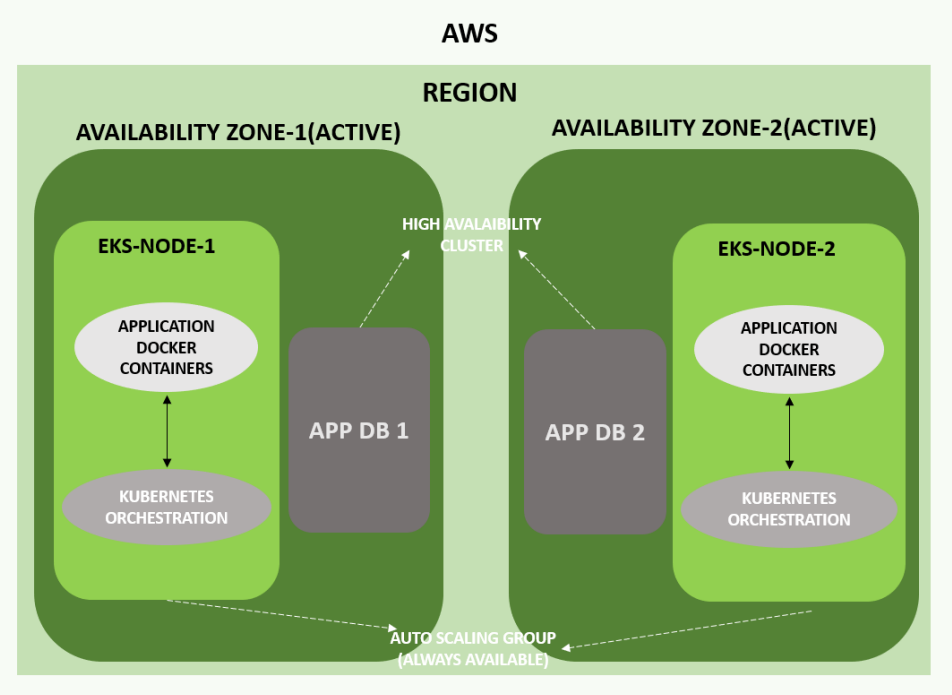
This new multi-tenant global platform for payments and statements processing currently is operated on two SaaS instances (“cells”), US and EU, to align with data protection regimes our client base.

Architecture and Infrastructure for the Standard Edition platform

The platform is a true SaaS, which enables cost efficiency, scalability, resiliency, reliability, availability, and consistency for the payment services.

The FIS Solution is a multi-tenant environment with data segregated using a pool of dedicated isolated database instances for each tenant deployment. At no point will client data be intermingled with any other client data to ensure absolute segregation.

Clients receive one or more tenant accounts on the application within the production and test environments with access to their own data, secured through a Single-Sign-On authentication.



The solution is fully operated by FIS and runs under FIS' subscription on AWS (Amazon Web Services). The platform's availability is guaranteed through several mechanisms:

- Local fail-over capabilities of the production environment: the solution is spread over multiple Public Cloud Availability Zones to remove any single point of failure.
- The solution is designed to failover to an additional Availability Zone in the event of a disaster recovery ("DR") invocation. DR plans are tested annually.

Upon subscription, each client is offered one production tenant, and one default test tenant. The default test tenant is used:

- By FIS, to test its software updates, which are made available in the test environment before the update is pushed to production.
- By FIS consultants, to test client configuration (during the initial implementation)
- By clients, to test new configuration *
- By clients, to validate the absence of impact of the software updates.

a. Maintenance & Application Updates

Maintenance of the FIS Solution, infrastructure, security, and operating system are performed on a scheduled basis by FIS technical resources. Maintenance tasks will occur sometime within the scheduled maintenance period; each scheduled maintenance period begins at 4:00 PM on Saturday and runs until 9:00 AM on Sunday in the time zone where the SaaS service is located. Maintenance tasks will occur sometime within the scheduled maintenance period. Each scheduled maintenance period begins at 4:00 p.m. on Saturday and runs until 9:00 a.m. on Sunday in the time zone where the SaaS service is located.

Application updates are taken care of by FIS as part of the service. All clients receive regular platform updates at the same time. Clients using custom interfaces and reports should retest them post these updates.

There are two types of updates:

Quarterly Releases

- These happen according to a fixed frequency: currently new releases are applied each quarter.
- FIS utilizes a Blue/Green upgrade model, clients subscribed to the platform will be informed of the times when the production environment will be switched from Blue to Green, clients will be notified when the outages will be planned for, as there will be a small outage when the environment is switched from Blue to Green
- The new releases may contain bug fixes, enhancements, and minor functional additions.
- All changes that impact client usage will be documented and shared with key point of contacts from the client's team as soon as the new release is available in the Test environment.
- New functionality (except. Bank/ERP connection and preference changes) are added centrally for all clients. Clients get access to Aha! Portal to propose new items to be added to product roadmap.
- Are available in the Test environment four weeks before being applied in Production, so clients may get a preview.

Hot fixes

- Occur exceptionally.
- Are used to fix urgent and severe issues, impacting clients without workaround, or having security implications.
- Are restricted to a single-issue code change.
- For the sake of urgency, a hot fix may be deployed at the same time in the client test and production environment.

The smooth deployment of application updates is the responsibility of FIS. The client impact of releases is the following:

	Clients may	Clients are expected to
Quarterly Releases	• Preview some functionality in advance by activating features on their Test environment. • Leverage their Test environment to proactively retest some key processes or complex customizations	• Learn about the release content. • Do an impact analysis of the changes introduced. • If there is an impact, plan the appropriate project resources (e.g., to activate features, change or extend configuration, or amend some custom reports or interfaces) during the change window.
Hot fix	• N/A	• N/A

b. Capacity Management

Managing the platform's capacity is key to maintaining performance levels stable as the number of clients on the platform grows. FIS uses the following tools to manage capacity:

- **Scalable architecture**. All application layers will determine their capacity and as needed can be extended by adding more computing resources.
- **Scalable model**. As the platform is operated on AWS Cloud, FIS can add additional regions if the need arises. Capacity will be managed based on organic growth of existing clients and expected capacity requirements of new clients being on-boarded onto the Standard Edition platform.
- **Monitoring**. The production system's performance is monitored, both at the infrastructure and at the application level.
- **Performance testing**. Before releasing an updated version, FIS verifies that there is no performance degradation.

c. Availability Management

The Payment Hub - Standard Edition platform offers an SLA of 99,9% availability with 4hr RTO (Recovery Time Objective) and 1hr RPO (Recovery Point Objective), within the Service Period. Service Credits may apply when the SLA is breached. The service period is 24*7 excluding planned maintenance.

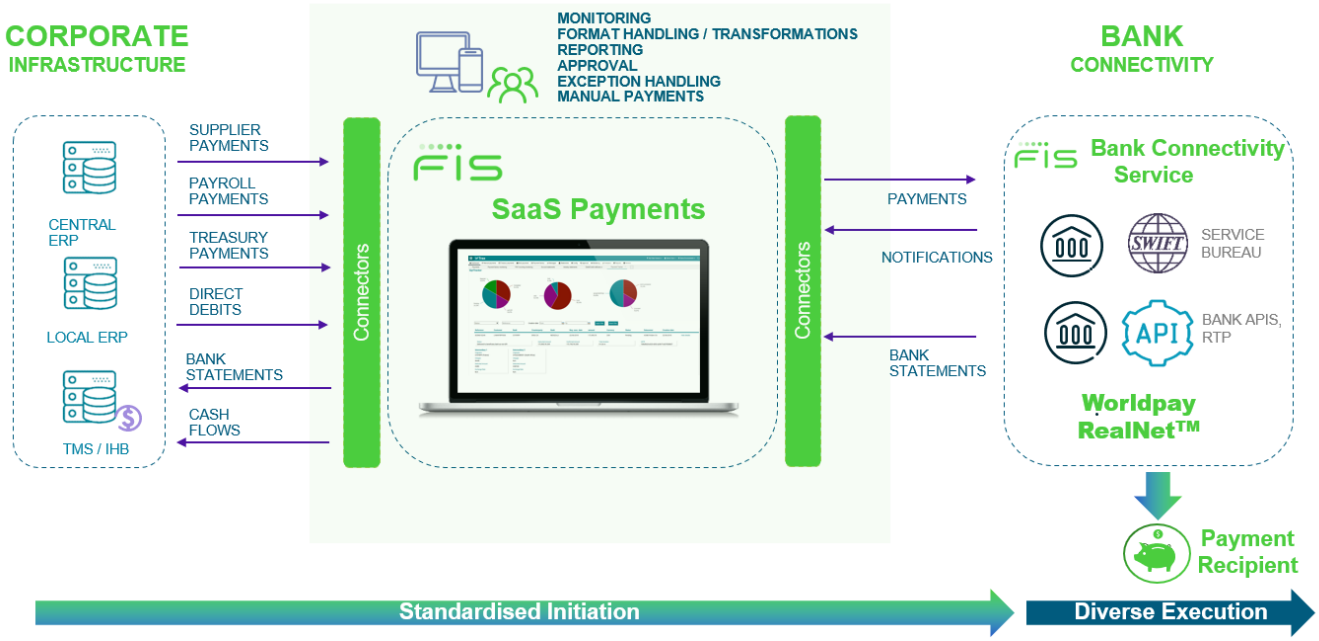
FIS uses the following techniques to guarantee availability:

- Planned downtime outside of the Service Period: all interventions are scheduled typically on Saturdays (Aligned with SWIFT downtime).
- Local redundancy: the production site uses server clusters and load-balancers to offer high availability.
- The Standard Edition platform is deployed in AWS regions having two Availability Zones ("AZ"), these can be considered as data centers:
    - When one of the AZ is not functional, there will always be another AZ up and running as AZs are in ACTIVE-ACTIVE mode.
    - The AZ which is not functional can then be further investigated, troubleshooted or recreated to have it up and running.
    - This entire process is non-disruptive as the routing of traffic to the application is managed by Application Load Balancer (ALB).
- Disaster Recovery: DR will be rehearsed annually. Please note that DR is invoked at cell-level, also for rehearsals (not per client).

Payment processing and Treasury Management

The Payment Hub Standard Edition platform offers fully automated processing of payments and bank statements, integrating into several source systems (ERP, Payroll, TMS and other back-end applications) via bank agnostic connectivity channels. Standardized pre-defined workflows have been designed to validate, enrich, repair, and authorize payments to support corporate treasury business requirements and processes related to payments and account statements.

Seamless integration can be established with the FIS Treasury and Risk Manager – Integrity Edition or Quantum Edition, which enhances automation and efficiency in cash management and cash position monitoring. Additionally, the Payment Hub solution can connect to other FIS treasury solutions as well as third party TMS and client ERPs, FX, cash management or other applications.



1. User setup and Role based access control.

The service is available over the Internet, via the HTTPS protocol. Access requires a modern HTML5-compliant browser on the user's platform.

User ID's will be provisioned via the FIS IdP or Client selected IdP. There is no limitation on the number of users that can be created in the system. However, the number of users will impact the pricing of the service.

The platform has predefined user roles configured based on frequently observed business functions. These roles can be assigned to users based on their tasks. Please see the appendix for a complete list of available profiles.

No.	Entity	Managed by	Supported by
1	Single Sign On setup	Client selected IdP	-
2	Role definition	FIS	-
3	Role assignment to the user	Client	FIS

2. Static data management

Payment Hub Standard Edition is equipped with the capability to synchronize static data from FIS Treasury Management Systems (Quantum, and Integrity), ensuring consistent and up-to-date information across platforms

To kickstart the client onboarding process, the platform will be loaded with client specific reference data.

Following table summarizes the static data and the responsibilities of maintaining it thereof:

Sr. No.	Entity	Managed by	Supported by
1	Bank	FIS	-
2	Country	FIS	-
3	Currency	FIS	-
4	Accounts	Client	FIS
5	Holders	Client	FIS
6	Calendar	FIS	
7	Templates	Client	FIS

Change management for accounts or holders will be done via the templated workbook attached below. A change approval via 4 eye review is enabled on the platform.

3. Connectivity support

a. Source System Connectivity

The Payment Hub - Standard Edition platform supports receiving payment instructions electronically from source systems such as an ERP, Treasury applications and manually via file uploads or manual entry in the webapp.

For the exchange of files with clients' ERP applications, a single SFTP account with pre-defined folders & SSH-key authentication is provisioned for each client. It is each client's responsibility to secure their key and request a re-issue by FIS when applicable.

The platform can consume encrypted and compressed files from these folders. The encryption method supported is PGP and compression methods supported are zip and gzip.

The platform handles SWIFT and ISO20022 formats and accepts frequently used local banking formats. All native text-based formats (flat-file, xml, JSON, …) can be processed by the application; support for a specific format can be provided on request. Binary files such as PDFs are not parsed in the application.

The platform will also use SFTP for publishing notifications and bank account statements back to source/internal systems that need it for tracking or reporting purposes.

Protocol	Initiator of transfer	Data direction	Data type example
SFTP	Client applications	Standard Edition Platform	Payment files
SFTP	Standard Edition Platform	To client applications	Account statements, cashflow, notifications, payment status reports.

b. Bank Connectivity

The Standard Edition Platform is “SWIFT Certified for corporates” and integrates seamlessly with the FIS SWIFT Services through standard SWIFT protocols SWIFT FIN, FINPlus & FileAct. Additionally, the platform can connect to Banks via EBICs and Host to Host (H2H) via SFTP.

Formats sent to the Banks are either SWIFT standard or ISO20022. The format conversion of incoming non-standard formats to Industry standard ones is readily available in the application and will be managed by FIS. Our platform is committed to providing comprehensive banking support. While we strive to adhere to universal standards like ISO20022, we understand that not all banks may be able to support this. In such cases, we will proactively choose an alternative format that ensures seamless integration.

Files being sent to Banks can also be compressed and encrypted. Compression methods supported in the platform are zip or gzip and encryption methods supported are PGP or CMS.

Channel	Initiator of transfer	Data direction	Data type example
SWIFT (FIN & FILEACT)	Standard Edition Platform	To Bank	Payments
SWIFT (FIN & FILEACT)	Bank	From Bank	Account Statements
EBICS	Standard Edition Platform	To Bank	Payments
EBICS	Bank	From Bank	Account Statements
H2H via SFTP	Standard Edition Platform	To Bank	Payments
H2H via SFTP	Bank	From Bank	Account Statements

4. Payment type support

The Payment Hub - Standard Edition is equipped with payment workflows that are designed to handle the specific needs of different transaction types and reflect best practices to manage payment types such as supplier payments, salary payments, treasury payments, collections, or even generic financial messages.

Payment types currently supported include the following (see the appendix for the complete list):

- Credit Transfers
  - Supplier/Vendor/Account Payables/Intercompany/PINO
  - Payroll/Salary payments - Ability to shield confidential and personal information in payroll payments.
- Direct Debits
- Cheques

In addition to the above, the platform is designed to pass through a wide range of financial message types, ensuring comprehensive support for your banking needs.

5. Bank Country coverage

The Payment Hub - Standard Edition is equipped with pre-configured formats for more than 1,200 combinations of banks and countries, and it accommodates all types of payments that a specific bank can support. This comprehensive library has been developed over several years, drawing from the diverse implementations carried out with this product.

6. Payment process

The following key functions are embedded in the workflow:

a. Validations

- Duplicate check at File and Transaction level
- Requested Execution Date (RED) validation & optional auto-recalculation in scenarios where:
  - Date is empty.
  - Date is a Non-Business Day
  - Date is in the past or “x” number of days future.
  - Payment is received late / misses bank cutoff time.

- Account Validation based on
  - Account Structure (IBAN, BBAN…).
  - BIC (Bank Identifier Code) details.
  - SWIFT Ref - BIC IBAN consistency.
  - National Clearing Code structure.
  - Address Country Code (of both account holder and bank).

- Instructed Amount Validation such as:

  - Nonzero amount.
  - Currency is valid.
- Payment Warehousing – Future dated payments will be warehoused and will be released for further processing as soon as the Requested Execution Date is within the configured number of business days (As per the client's selection in preferences document).

b. Approval and Signature

Payment approval is an important feature for a payment processing hub and the Standard Edition platform can enforce 4-eyes approval. Payment approval filters can include:

- Amount Thresholds.
- Amount range based.
- Or exempt from approvals.

Additionally, payments can be digitally signed using digital signatures such as SWIFT_3SKEY on request.

c. Embedded Sanction and Fraud screening

The Payment Hub - Standard Edition platform offers the following mechanisms for payment screening:

- Blacklisting
- Whitelisting
- Fraud prevention
- External payment screening (Optional, at a cost)

Blacklisting, whitelisting, and fraud prevention are internal screening mechanisms as the payments are checked against various lists and patterns that are managed internally in the platform.

Payments can be prevented from processing to completion being made to an EU or US OFAC listed beneficiary using officially available Blacklists that are imported on the platform weekly.

Our fraud prevention supports three options:

- Frequency: Each payment value date is assessed against the frequency of historical payments which is set by the client at preferences gathering stage (subject to data retention policy) & is stored in the database. When the requested value date of a payment deviates from the expected pattern, the check fails, and the payment is flagged as a screening suspect.
- Amount: Each payment amount is assessed against historical payment records as compared to a median amount of previously processed and matching payments. When the amount is smaller or bigger than the median of the matching payments, the check fails, and the payment goes to screening suspect.
- Invoice: Can be used in three different use cases:
  - Detect invoice fraud.

- Detect new beneficiaries.
- Detect payments with new general criteria.

7. Account Statements

End of Day and Intraday Statements flowing from banks are captured and processed by the Account Statement workflows which includes monitoring of timely balance and transaction reception. The statements can be exported in the formats required by the target systems.

The platform can perform the following functions on statements:

- Receive statements from the Bank.
- Enrich bank statement line entries on request.
  - Normalize Bank Transaction codes.
  - Data as required from accounting systems.
- Publish it to internal systems.
  - To ERP systems for reconciliation purposes
  - To TMS for cash management purposes
  - To Ledger applications for accounting purposes
- Search for specific account statements and entries.
- Export or print (as PDF).

8. Cash flow notifications and status reports

The platform can generate cash flow messages to Treasury Management Systems. When the payment file has been sent to the bank, an actual cash position update message is created and can be sent to the TMS. If the bank rejects a payment and notifies the client via a Pain002 message, the platform can send a reversal cashflow to the TMs for each rejected payment.

Cash flow details along with Account statements enable treasury management systems to reflect real-time cash positions.

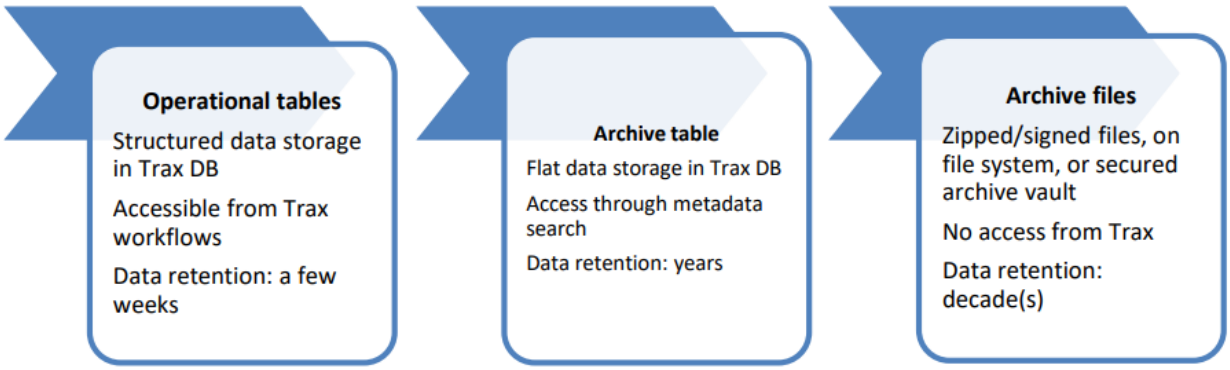
9. Reporting, Archiving and Data Retention

FIS Payment Hub – Standard Edition platform offers standard reporting capability that provides customized ad hoc report generation.

In addition, the platform includes archiving capabilities. Archiving the operational data (transactions) on a regular basis has several benefits:

- Keep the workflows clean, so that only the most recent payment instructions, account statements and messages are displayed in the active workflows.
- Provide a searchable archive that contains all the payment instructions (sent to the bank), account statements (received by the bank) and messages.

By transferring transactions from the workflows to the archive, the performance of the workflows is maintained while the payment, account statement and message information can still be accessed.



After a set time, data will be cleaned up ("purged") from the archive. Optionally, archived data can be exported to files; this enables the platform to store the business data and bank communications in a suitable 3rd party vault for an unlimited time for regulatory compliance.

The following table provides an overview of archive and purge settings:

Transaction type	Operational Data	Archive	Exported Archive Files (additional cost if stored by FIS)
Payment files	6months	7years	No limit
Account Statements	3months	7years	No limit
Intraday Statements	1 week	Not archived	N/A
Messages (any other file)	3months	7years	No limit

Onboarding the Standard Edition Platform

This section explains the implementation model for a typical Payment Hub - Standard Edition set-up project.

The Payment Hub - Standard Edition platform is designed for fast onboarding and go-live. It can be set up with minimal effort by FIS once data is provided by the client. This results in a short and standard implementation that requires a lean implementation cycle.

Typical onboarding onto the Payment Hub - Standard Edition platform consists of 2 distinct phases: Initiation and Testing/Go Live.

The Standard Edition platform is set up through simple configuration of the solution's features based on the features selected by the client.

a. Initiation

The project starts with a kick-off call which will be conducted together with the client to review the agreed scope of items and develop an implementation plan. During this phase, FIS will gather information about the client's payment landscape, perform comprehensive analysis of the chosen preferences and validate provided data.

b. Testing and Go Live

Once configured and unit tested by FIS, the application is then ready for hand over to the client. FIS follows the train the trainer approach and will provide demo-based training to the key users of the application. Ideally this will mark the beginning of the client testing phase.

This phase will consist of Acceptance Tests (on the Test environment) and Penny Testing (on Product environment).

- **Acceptance Tests**: these tests are aimed at checking the conformity of the service with the initial agreement and of the integration of the service into the client's overall payment and statement processes. The client is responsible for organizing, preparing, and performing any form of validation deemed suitable.

- **Penny Testing:** the client ensures payment flows have been validated in Production environments through penny test (small amounts, individual payments) until they were successfully processed by the banks.
  The client takes the Business Go/No-Go decision after the Penny Tests.

Due to the SaaS nature of PHSE, typical IT project management is not deemed mandatory for every client onboarded to the platform. The client chooses from the list of features and banks that they would like to subscribe to. This input is then utilized to create a platform tenant for them and delivered ready for UAT (User Acceptance Test). In other words, this would be a ready to use/pre-defined solution with some expanded functionalities that are based on client preference without involving complicated configurations.

Therefore, the client onboarding is not meant to result in a full-fledged project. However, due to certain complexity like a large scope of bank connections, if a client wishes to engage in an extensive project management model, FIS can support this request with its extensive tailor made in executing large complex projects in this domain. For more information, contact your sales representative.

Also attached is a draft implementation plan template for each client onboarding. This will be further detailed as part of the kickoff discussions with the client.

Client support model

10. Application support teams

a. FIS Payment Hub Standard Edition Tenant Onboarding team

This team will be responsible for the initial tenant onboarding on the platform, with the goal of bringing the client live in a timely manner. This includes tasks like, but is not limited to:

- Account and Holder data loads.
- User authentication and authorization setup
- Source system and Banks setup.
- Unit and End to End tests.
- UAT, Go Live and Hypercare support.

They will also continuously enhance the platform with new features, bank format library, defect fixes and improvements.

b. FIS Standard Edition Operations team

This team will be responsible for Production support via ticketing systems and Standard Operating Procedures. This team will work in close cooperation with FIS Standard Edition Product team, and is responsible for:

- Maintaining client portfolios and documentation on each client's setup
- User management and modifications, as requested by the client.
- Scheduler Service monitoring
- Payment exception monitoring and alerting
- Infrastructure monitoring and alerting

Operations support services for Standard Edition Platform will be managed via tickets created on SNOW (Service NOW). Alternatively, a client support email distribution list will be provided to log in incidents/contact Operations team via emails.

c. Production support SLAs (Service Level Agreements)

Support SLAs are defined in the FIS Support Services website: Support Services - Legal | FIS (fisglobal.com)

Production Database Incident Severity Level and Description	Target Response Time during Support Times	Response and Escalation
Severity 1: Critical. An Incident which results in one or more of the following: • Material negative impact to time-sensitive critical Client service level or key output from the Solution is imminent, within the next 12 hours or has already occurred. • The solution is completely down for all users – not operational or accessible. • Causes the Solution to fail to make use of the Solution seriously impractical and greatly interrupts production by Client. • Data corruption is occurring through the use of the Solution.	1 hour (or such time as set out in the Agreement)	The Incident will be promptly assigned to the FIS personnel. The team will promptly start work on resolving the Incident. Members of the team will be primarily dedicated during Support Times (or at such other times as stated in the Agreement) to resolving the incident until a reasonable work-around or correction is implemented. An FIS representative will keep Client regularly informed of the Incident status and be available during Support Times (or at such other times as stated in the Agreement) until a work-around or correction has been implemented. Client may escalate to the key personnel management contacts, such contacts to be promptly provided by FIS upon Client's request.
Severity 2: Major. An Incident which results in one or more of the following: • Impact to time-sensitive critical Client service level or output from the Solution is imminent, within the next 24 hours. • Key users are experiencing a severe degradation of service • A portion of the Solution is inoperable or compromised,	2 hours (or such time as set out in the Agreement)	FIS personnel will promptly begin work on the Incident. Items that cannot be solved by a first line support consultant will be escalated to senior support staff. Support staff will continue to work on the Incident, during Support Times, until a workaround or correction has been implemented. Such correction may be implemented through a new Release made available to Client.

putting key outputs from the Solution at risk.		
Severity 3: Moderate. An Incident which results in one or more of the following: • Impact to Client is yet to be determined, but no known service levels or Client outputs from the Solution are in danger of being missed within the next 72 hours. • The solution is highly operational, although anomalies have been noted. • A portion of the application is inoperable or compromised, however key deliverables are not at risk.	2 business days (or such time as set out in the Agreement)	FIS personnel will address the Incident as promptly as possible during Support Times. Correction of the Incident may be made through a new Release implemented for Client.
Severity 4: Nominal. An Incident which results in one or more of the following: • Low to no risk of Client missing service levels or any major output from the Solution. • Solution users may have a single Client Incident or one for which there is a work around. Client requests for information or general use of the Solution (but, for the avoidance of any doubt, not training on the use of the Solution)	5 business days (or such time as set out in the Agreement)	FIS personnel will address the Incident as promptly as possible during Support Times. Correction of the Incident may be made through a new Release implemented for Client.

d. Ongoing support - post Go Live

The client will be provided with training videos that they can refer to at any time during their journey on the platform. These videos are brief and provide a summary of various features such as user access control, manual payment creation, static data management etc. These have proven extremely helpful for our early adopters in training their users when being onboarded on the application.

Change requests will adhere to the following:

Change Type	Example	Response time	Notes
Minor Change	Create/Update Profile	2 Business Days	Resolution time will depend on Business impact.
Medium/Large Change	Connect New Bank / Implement New Format	5 Business Days	resolution time will depend on several factors such as: 1. Business impact. 2. Size of Change/update. 3. FIS and client resource requirements and alignment 4. Timely receipt of information needed from client.

Furthermore, if there are changes in the Banking relationship or adding new entities / users to the application, here is how this will be managed:

Scenario	Process	FIS	Client
New business unit; existing Bank connection	Templates / Manual upload (4 eye enabled)	CI	RA
New accounts for existing entities/Banks	Templates / Manual upload (4 eye enabled)	CI	RA
Close/Deactivate existing accounts	Manual configuration	CI	RA
Change format / connectivity protocol for existing banks	Via Snow Tickets – templatized requests	RA	CI
New Bank onboarding, connectivity, and routings	Via Snow Tickets – templatized requests	RA	CI
New user onboarding	Templates / Manual upload (4 eye enabled)	CI	RA
Existing user change of access	Manual configuration	CI	RA
Deactivate users	Manual configuration	CI	RA

At any point in time post Go Live, if the client requires assistance from FIS for any of these changes, they can make a request for Professional Service Consultancy via Snow platform.

Depending on the type and complexity of the request, the client may incur additional costs for the consultancy availed.

11. Security Management

At FIS, our priority is to protect our clients' data and financial interactions. We realize cybersecurity has no end state and are constantly improving our services and security to stay in front of the ever-changing industry threats. FIS employs a defense-in-depth strategy by putting multiple compensating controls into place to protect our clients' data from malicious activity. These combined efforts, sorted by their purpose to prevent, detect, and respond, demonstrate our approach to threat mitigation. These activities are monitored and governed by our Risk, Information Security and Compliance (RISC) organization:

- **Deployment:** The multi-tenant Standard Edition is deployed to an FIS managed subscription account on the AWS Public Cloud. The solution is deployed using Kubernetes containers. There are two instances, one in the EU, and another in US, no client data is passed between instances.
- **Network**: Managed WAF firewalls and network intrusion detection services, encryption for all connections (TLS, SSH), multi-factor authentication of users
- **24/7 Security Monitoring**: Our 24x7 global security team instantly respond to any security incidents (real-time log capture and analysis, digital forensics analysis, denial of service response and mitigation, malware, virus and data loss incidents, botnet identification and counteraction)
- **Patching and Releases**: quarterly server patching, synchronized with the application updates, antivirus on all devices, all unused services de-activated.
- **Application roles**: Fine-grained user authorization possibilities, dual approval & segregation of duties - Application code: Daily static source code scans, quarterly Dynamic application scans, yearly 3rd Party Penetration testing and ethical hacking
- **Data at rest**: All individual client/tenant databases are fully encrypted using Transparent Database Encryption (TDE).
- **Certification:** The FIS Information Security Management System is globally ISO27001 certified. The FIS operational controls are audited externally against SSAE18 SOC 1 Type and SSAE18 SOC 2 Type 2. The annual audit period is from 1 January until 30 September, with the audit reports being published by our external audit in December of each year.

APPENDIX

12. User roles

Code	Usage	Sample End Users
Create Manual Payments	Manually create credit transfers in PHSE without using a payment template.	Account Payables Team with Manual Payment Creation Access
Create Payments from Template	Manually create credit transfers in PHSE using a prefilled payment template.	
Create Payment Template	Create a credit transfer template for payments that recur.	
Create Manual Payroll Payments	Manually create payroll transfers in PHSE without using a payment template.	HR/Payroll Team with Manual Payroll Creation Access
Create Payroll Payments from Template	Manually create payroll transfers in PHSE using a prefilled payment template.	
Create Payroll Payment Template	Create a payroll transfer template for payments that recur.	
Approve Payment Templates	4-eye approval of credit transfer or payroll templates that were created or edited	HR/Account Payable Team
Create Manual Direct Debits	Manually create direct debit transfers in PHSE without using a payment template.	Account Receivables Team with Manual Payment Creation Access
Create Direct Debits from Template	Manually create direct debit transfers in PHSE using a prefilled payment template.	
Create Direct Debit Template	Create a direct debit transfer template for payments that recur.	
Approve Direct Debit Templates	4-eye approval of a direct debit template that was created or edited	
Sign Payment Files Level 1	Access to level-1 approval of credit transfers, payrolls, and direct debits	Business or Treasury Approvers for Credit transfers, Payrolls and Direct Debits
Sign Payment Files Level 2	Access to level-2 approval of credit transfers, payrolls, and direct debits	
Sign Payment Files Level 3	Access to level-3 approval of credit transfers, payrolls, and direct debits	

Sign Payment Files Level 4	Access to level-4 approval of credit transfers, payrolls, and direct debits	
Payment Factory Monitoring	End to End Payment monitoring, from payment creation to being sent to the bank	Account Payables/Account Receivables/Payroll Team
Payment Factory Release Monitoring	View payment processing after it is approved.	Payment Approvers to monitor rest of the payment workflow
Warehouse Administrator	Accept or reject payments in warehousing	Account Payables/Account Receivables/Payroll Team Heads who can cancel a payment
Warehouse Monitoring	View payments in warehousing.	Account Payables/Account Receivables/Payroll Team
Internal Screening Admin	Accept or reject payments identified as fraudulent or risky.	AML Screening Tean
Internal Screening View	View payments held as suspected fraud or risk payments.	Account Payables/Account Receivables/Payroll Team
Cashflow Monitoring	View cash flow files sent to Treasury systems.	Treasury Team
Archive	View the archival repository	Account Payables/Account Receivables/Payroll Team
Account Statements Monitoring	View and print end-of-day and intraday statements.	Account Payables/Account Receivables/Payroll Team
Debit/Credit Notification Monitoring	View Debit and Credit Notifications (Advice)	Account Payables/Account Receivables
Reporting	Generating and viewing standard reports offered by PHSE	Account Payables/Account Receivables/Treasury
Incoming File Management	Accept or cancel incoming payment files that are identified as duplicates and view files that failed in PHSE.	Account Payables/Account Receivables/Payroll Team Heads who can cancel a payment file
Static Data Administrator	Manage bank accounts (add or edit) and business units (edit).	Admin Users
Static Data Approval	4-eye approval for changes made to bank accounts and business units	
Static Data Monitoring	View bank accounts, business units, and exchange rates in PHSE.	Account Payables/Account Receivables/Payroll Team
User Administrator	Manage user access (Add/Edit) in PHSE	Admin Users
User Approval	4-eye approval for changes made to user access	
User Monitoring	View users and their accesses in PHSE.	Admin Users/ BU Heads

Communication Monitoring	View incoming payment files that are duplicates or failed.	Account Payables/Account Receivables/Payroll Team Heads who view all files
Inbound Message Monitoring	View incoming files, like pdfs and texts, that are not supported in the standard workflow or do not have a standard format.	Account Payables/Account Receivables/Payroll Team Heads who view all files
Outbound Message Monitoring	View outgoing files like pdfs and texts that are not supported in the standard workflow or do not have a standard format.	Account Payables/Account Receivables/Payroll Team Heads who view all files