INTESA SANPAOLO

Group Technology & Services

SERVICE LEVEL AGREEMENT
INTERNATIONAL NETWORK IMI CIB

Declaration

TO WHOM IT MAY CONCERN

1 Introduction

1.0 Generality

The “Group Technology & Services (from now on GTS) of INTESA SANPAOLO” oversees the implementation and the management of all technological infrastructures and procedures serving the Domestic and the International Networks of INTESA SANPAOLO Group.

The “GTS of INTESANPAOLO” is a wide organization, consisting of several departments/offices/processes, each one carrying out specific tasks. IT Services provided to each branch of International Network can therefore be regarded to as the final output of a process involving the whole “INTESA SANPAOLO GTS” structure.

The “GTS of INTESANPAOLO” is a part of the INTESA SANPAOLO Group specifically mandated for providing IT services to the Group’s Operational Units.

1.1 Aim of this declaration

The aim of this service level declaration is to define the engagements undertaken by “GTS” as the INTESA SANPAOLO Group internal IT services provider to allow International Department (**from now on “DCO – International Network”)** perform all specified functions that are necessary to carry out their business.

“DCO – International Network” includes the “Foreign Branches” which outsourced their IT environment to “INTESA SANPAOLO” (from now on: “The Supplier” or “GTS”). the above specified Operational Units may already accept to centralize their IT environment (this SLA is already operational), or they may decide afterwards (this SLA will be operational from the date of the acceptance).

The International Network Operational Units covered by this declaration are HUB Foreign Branches, Foreign Branches, Representative Offices and the relative local Disaster Recovery Sites. The content refers to the services provided and delivered at t -1 where “t” is the current year.

Here follow the entities list:

- ISP New York, hub branch for North American Area
- European HUB Area with the following branches:
    - ISP Madrid
    - ISP Paris
    - ISP Frankfurt
    - ISP Warsaw
    - ISP Amsterdam
- UK and Middle East Area with the following branches:
    - ISP London
    - ISP Dubai
    - ISP Istanbul
    - ISP Abu Dhabi
    - ISP Doha
- Asia Pacific (APAC) with the following branches:
    - ISP Hong Kong

- ISP Shanghai
- ISP Tokyo
- ISP Singapore
- ISP Sydney

- All ISP Representative Offices

1.2 Principles governing the SLA

1.2.1 Accountability

The management of any Foreign Branch having accepted the outsourced services of "GTS" and this Service Level Agreement, will remain fully and directly responsible of any activity covered by the outsourcing agreement except for the technical activities, outsourced to GTS. For the latter, the management will retain the ultimate responsibility of the activities by:
- controlling the quality of the services provided by the outsourcer (Quality Report)
- having evidence of the incidents (KPI report – Incident discussion)
- maintaining the absolute right to input/modify/delete the Branch data
- assuring to the Branch staff unlimited grants for inquiring the databases (the full extent of the grants is reserved to the Senior Management) [1]

1.2.2 Regulatory Authority Audit access rights

"GTS" recognizes to any Regulatory Authority supervising the Operational Unit as well as any Internal and External Auditors a full access to the databases, to the operational procedures, to the programs and to the logs belonging to the said Operational Unit under the governing law of that country and with the same limits in force in that country.

[1] NY HUB – Abiliweb – availability 8.00 a.m. – 6.00 p.m. NY time

1.2.3 Access by Italian Authorities to the Customer's data managed by GTS

Subject to some conditions determined by the Italian laws, the Fiscal, Administrative and Criminal Italian Authorities have the power to obtain in Italy all the data existing in Italy. "GTS", by executing the outsourcing contract, manages in Italy the Foreign Branches Customer's data. "GTS" declares that its internal procedures provide for an immediate notification to the Business Owner "DI" which is in charge to notify, in turn, the involved Operational Unit(s) of any request concerning the Customer Data. The involved Operational Unit(s) will then be entrusted to report the event to the local Regulatory Authority when required.

1.2.4 Compliance with external requirements

Each Operational Unit is responsible to forward to Head Office relevant Department the guidelines pertaining IT Outsourcing or circular and documentation on the matter received by the local Regulators and that may affect this Service Level Agreement, with the aim to ensure promptly compliance with the external requirements.

1.2.5 Intellectual and industrial property rights

All the intellectual and industrial property rights in general (including those related to the software and the know-how) owned by GTS, or licensed, used in connection with the supply of the services, shall remain in the ownership of GTS (or its licensor). GTS (and/or its licensor, as the case may be) keeps the exclusive ownership of the software and any other intellectual property, process or invention covered by intellectual or industrial property in general (hereinafter the "IP Rights") created directly or through third parties - by GTS in performing this Service Level Agreement. Intesa Sanpaolo S.p.A. shall therefore not acquire any right over the IP Rights, except for those granted pursuant to specific written license agreements entered with GTS.

1.2.6 Customer data (only for ISP Hong-Kong)

In the event of a termination of outsourcing document, for whatever reason, ISP should ensure that all customer data managed by GTS is either retrieved from the service provider or destroyed.

1.3 Object and Governing Law of this declaration – Revision

This declaration is applicable to all services provided by "INTESA SANPAOLO" (from now on: "GTS") **only**. In each Foreign Branch, in fact, there are some IT services acquired and/or produced locally under the control and the responsibility of the Foreign Branch management, even if the "GTS" provides a remote support at least by approving (from a technical point of view) any development/enhancement. for such services, the responsibility of the "GTS" cannot be invoked.

Services must be provided by GTS also in compliance with the laws governing the activity of each Operational Unit, provided that such Operational Unit shall be responsible to identify, update and timely communicate to GTS the relevant requirements set forth by local laws and regulations with reference to the outsourced activities (included Data protection and Banking laws and regulations of such Operational Unit).

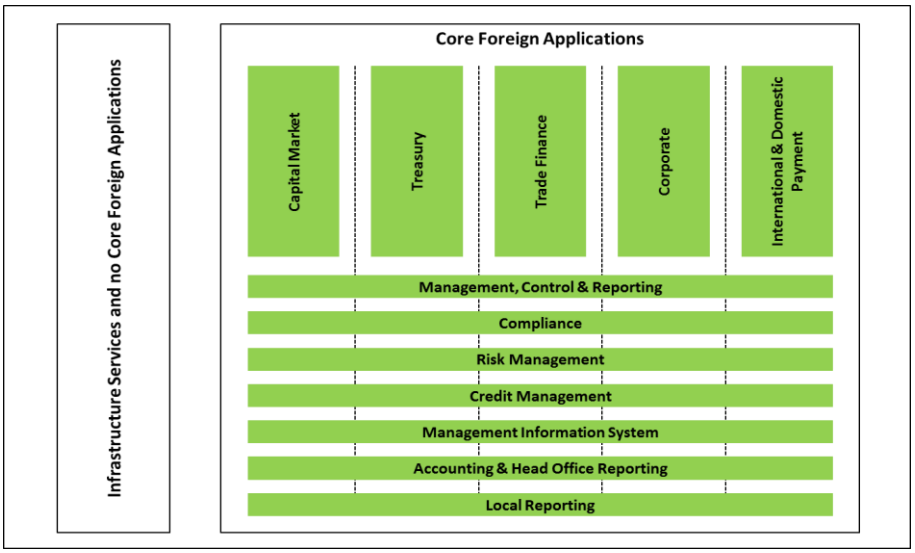
Save for the above, the contract signed the SLA between **Intesa Sanpaolo S.p.A.** and **GTS is governed by Italian law.**

For the avoidance of any doubt, it is understood that reference to Italian law included in this Service Level Agreement may not be construed or intended as to limit the above obligation to comply, in the delivery of the service, with the current regulatory provision of the country in which the Operational Unit beneficiary is based.

1.4 Services provided by "GTS" – General Overview

Foreign Branches having accepted the outsourced services of "GTS" and this Service Level Agreement are no more involved in the following processes, with the exception of the "local" IT services, approved on a case-by-case basis to optimize the cost/benefit ratios.
The list of main Services/Materials/Applications/Tools covered by this agreement is provided here below. Without contrary agreement (to be discussed and approved on a case-by-case basis), acquisition and maintenance costs are invoiced to "Intesa Sanpaolo S.p.A."

SERVICES / MATERIALS / APPLICATIONS COVERED BY THE SLA



- **Communication MPLS Line** needed for connection to the centralized servers/applications in Italy and the workstations/users in the Foreign Branch
- **Routers and Proxy-Firewalls** linked to these communication lines and installed in the Foreign Branch/premises
- **LAN and switches**, even when materials are provided and installed locally
- **Servers** in Italy dedicated to run the applications/tools, and the infrastructural server (domain controller) located in each foreign branch
- **Payment messages and related services**: BOX, Group Payment Hub (GPH) project underway, with a multi-year project and progressive definition of the release perimeter
- **AML platform** (SafeWatch and Worldcheck tools) [2]
- **Core Applications** (middle and back-office) and mainly the **SI-RE platform** [3]
- **Logical Security infrastructure** (being the Physical Security managed by the Local Responsible). It includes server patching and desktop patching. "GTS" should guarantee the upgrade of the OS Windows patches periodically, following Cyber-Security policies and indications

[2] except for New York HUB where AML is still managed by Local IT Dpt.

[3] For Istanbul Branch the local core banking system is WinBank. Please refer to chapter. 4.

- **Management of the Workstations** (the so-called Desktop Management) and distributed technologies
- **Disaster Recovery Plan** and the infrastructure necessary to provide it [4]
- **Reporting to the local Regulators** [5] - The local IT is the general entry point for the I.T. solutions for local regulators reporting
- **Local Core Banking System** [6]
- **NAS live and DR**
- **Telephone Services** (Traditional, VOIP, Trading, Soft phone)

Entity	Core TLC [7] Infrastructure	Distribution TLC Infrastructure	IPC TRADER PHONE SOLUTION	IP Phone, Webex, Cisco CUCM Infrastructure managed by TLC
London Branch	x	x	x	x
New York	x	x	x	x
European HUB	x	x	x	x
Hong Kong	x	x	x	x
Mea Area	x	x		x
Spokes	x	x		x

SERVICES/MATERIALS/APPLICATIONS LOCALLY MANAGED not covered by SLA and under responsibility of each foreign branch management

- **Physical security**
- **Business Continuity Plan** (even if under the control of the Head Office - Business Continuity Dept and the support of the "DCO – International Network with the technical support of "GTS")
- **Human Resources Area management tools** (incl. salaries/taxes and so on), including, if any, the "local" servers. Global Core HR project underway, with a multi-year project and progressive definition of the release perimeter for the adoption of "People" application
- **Market Data Services** and related Infrastructure not explicitly mentioned in the above list
- **Local Services Infrastructure** (i.e., E-GIFTS, Voice Recorder)
- **Local Network Infrastructure and Connectivity to Hot site** (Extranet connections and third-party connections)
- **Internet and Phone Services**
- **Other Applications locally relevant**, if any

"GTS" will review the SLA based on the request of the Business Owner DCO – International Network or on its own initiative. It is understood that eventual changes or integrations will be evaluated in accordance with the feasibility of the proposals. Integrations, updates and changes

[4] Disaster Recovery only pertains to those Services/ Materials/ Applications that are centralized

[5] were the local target solution must be implemented

[6] For Istanbul Branch only

[7] "TLC" refers to Networking & Collaboration team

will be shared and agreed among the counterparties and mediated by the Digital Business Partner.

1.4.1 Acquisition of hardware and services

Except for the hardware, software and services locally acquired (even if under the control and with the support of "GTS"), "GTS" will deal with the acquisition of technological resources according to the annual authorized budget or upon specific request from "DCO – International Network" in the framework of the Intesa Sanpaolo Spa budget workflow, acting on behalf (and upon request) of the Foreign Branch.
All IT initiatives requested by foreign branches will be discussed at Head Office level. According to the relevance of the request, a project will be activated. Before introducing new systems or major systems change, an analysis, including a technological risk assessment, will be performed by the relevant Head Office Departments. Afterwards, "pilot" branches will be chosen for a deeper analysis. Once the pilot is completed, a roll out phase is done in all the other foreign branches. For major project, local needs will be evaluated, and local support will be provided before the go live phase.
Functional tests (UAT – User Acceptance Tests) will be performed by "DCO – International Network" or by the Foreign Branches (or some of them, working as "Pilot Sites"), to ensure compliance of the acquired software and hardware with the Group's standards and the specified business requirements.
Similar UAT tests are performed for any development/enhancement of the tools in use, as per the Group's policies.

1.4.2 Technical and operating management of data processing systems/networks

For an easier exposure, these services are analysed here below as the sum of the following items, each one non-independent from the others. In the following paragraphs the main features are listed, together with a list of the relevant measures, objectives and related reporting, when available.

- Geographic network management and access to data processing systems, pertaining to TLC - Telecommunications Dept within "GTS".
- Real Time & Batch Procedures development and monitoring, pertaining to Financial & Foreign Applications Dept within "GTS".
- Management and monitoring of the OS Windows Foreign Branches servers, domain controllers and NAS (including management of the OS Windows updates on all branch servers and technical monitoring)
- Management of the Payments platform (Box tool) and AML platform, pertaining to Payments Dept within "GTS" [8].

1.4.3 Geographical network and access to data processing systems

❑ ***Data processing systems availability during standard working hours***

The Foreign Branch staff is enabled to continuously access to its front & back-office systems, both for input and enquiry, during the working hours in which they are used to work: from

[8] except for New York HUB where AML is still managed by Local IT Dpt

Monday to Friday, from 08:00 a.m. to 07:00 p.m. – **Local Time of each Foreign Branch/Bank.**[9] [10] [11]

The Foreign Branch may ask for an extended service whenever is possible, any request must be forwarded 2 weeks in advance (or as soon as the necessity is known by the local Management) to "DCO – International Network", which is in charge to validate the request and to forward it to the relevant Operational Unit of "GTS". The latter will confirm back to the Foreign Branch the temporary extension of the system availability or the reasons preventing "GTS" from satisfying the request.

Measured quantity: time and duration of the systems unavailability, measured either through automatic system tools (when available) or manually.

Objective: a monthly average of 97% of the working time.

Report: monthly table and histogram of the time of availability, for each calendar day of the last month, with the average values of the last and previous months.

- ***Data integrity and consistency***

All the file update performed by the night batch processing must be completed before the time the Foreign Branch staff starts working the following day. The integrity of the data against accidental corruption must be granted.

Measured quantity: time of end of the daily End of Day procedure. Time necessary to restore the whole database of the Branch.

Objective: end of the End of Day before 07:00 a.m. - Foreign Branch Local Time. 4 hours as maximum time to restore the whole Foreign Branch database (each) at the DR site.

Report: table of End of Day times (start, end and duration) for each working day of the last month (at request). annual report (at request: the report is provided on a regular basis to Business Continuity & DR Service of ISP).

- ***Data confidentiality and protection***

"GTS" jointly with Cyber-Security Department, through the structure in place (Logical Security), ensures the confidentiality of the Foreign Branch data and protection against any unauthorized access. The access to the servers is dependent on personal user profiles and passwords as per the industry standards. Data transmitted using communication lines outside the Foreign Branch and Head Office are encrypted. If an unauthorised access is proved, reaction measures will be immediately taken to identify and close the security breach.

Measured quantity: number of rejected attempts of access to the Foreign Branch environment, obtained through the auditing tool "Rapport Audit Master".

Objective: no unauthorized access to each Foreign Branch environment.

---

[9] For Dubai and Abu Dhabi Branch Monday to Friday, for Doha Branch Sunday to Thursday

[10] whenever a Saturday or Sunday is declared as "business day" by the local Authorities, "GTS" is engaged to provide the service, provided that the Foreign Branch requires it with a reasonable pre-advice

[11] NY HUB – the availability of the AS400 environment is 7*24 with the exclusion of the timeframe of the EOD/SOD procedures

Report: number of access attempts rejected (on monthly basis). The report is not published

- ***Efficiency***

The response time of the system during online operations must be optimized.

Measured quantity: average response time of the front / back-office system during online operations, obtained by automatic data collection.

Objective: response time ≤ 5 sec. in 90% of transactions.

Report: average response time of interactive processes (on monthly basis). The report is available at request.

- ***Geographic communication network***

Communications between the Foreign Branch and the Head Office hosting servers, applications and data are active and available for continuously accessing to front/back-office systems, **7 days x 24 hour**.

That availability level comes out from the redundant architecture supporting the Foreign Branch/Head Office communications: proxy-firewalls/routers/switches are duplicated in the Foreign Branch environment, as well as in the main sites (in Italy – Moncalieri & Parma). The MPLS line is redundant on geographical basis, in case of failure on one link, dynamic routing converges traffic to the secondary links under the control of the "GTS – TLC" team without any direct intervention from the "GTS" team.
Moreover, each Foreign Branch user, can access most of the centralized applications through a Citrix METAFRAME/Internet encrypted link available, under the control and with the assistance of "DCO – International Network", in the Main & Business Continuity Sites of the Foreign Branch (as well as in the Main Site), as per the Branch Business Continuity Plan.

Measured quantity: time in which the communication is active.

Objective: the proposed SLA for yearly availability of Geographical Link is 99,9%

Report: connection availability (on monthly basis) as per the KPI report

1.4.4 Real Time & Batch Procedures development and monitoring

- ***Batch procedures processing results***

Batch processes (including the End of Day of all front & back office outsourced applications and the copy to the Disaster Recovery site) must be terminated before the next day opening of the Foreign Branch.

Measured quantity: time of end of the daily End of Day procedures.

Objective: end of the End of Day before 07:00 a.m. Foreign Branch time.

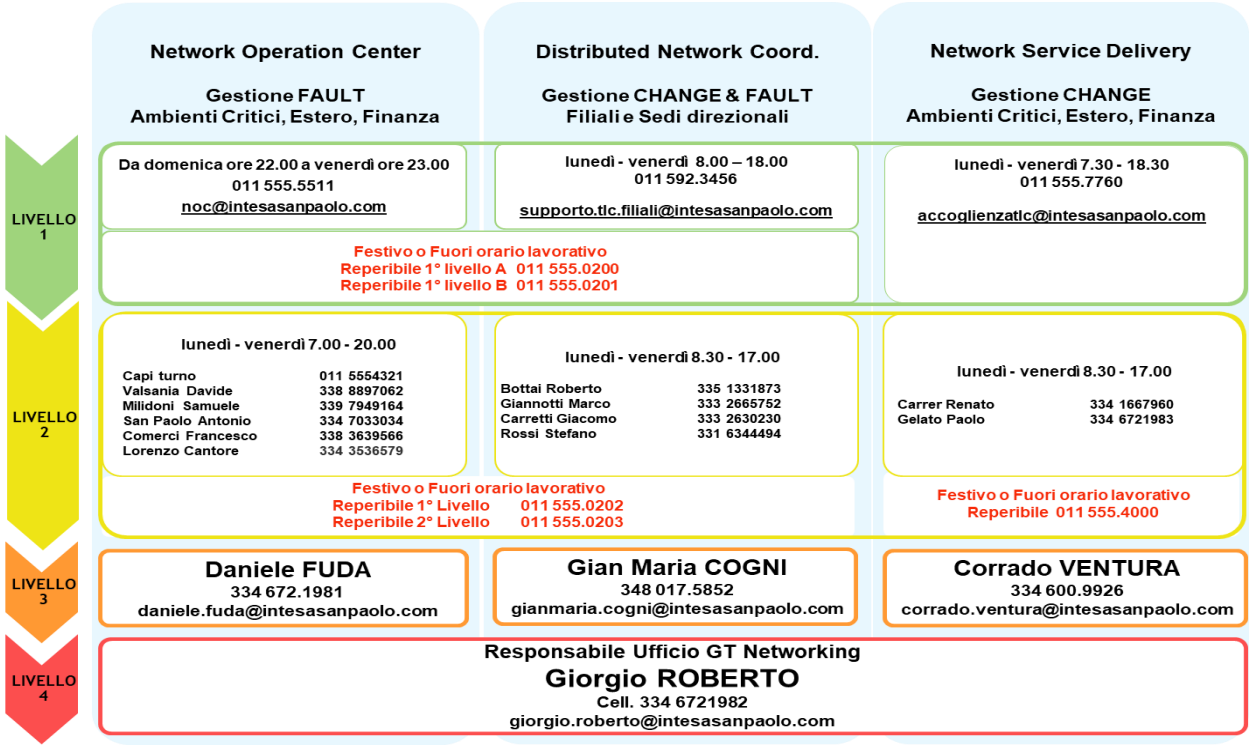
Report: table of End of Day times (start, end and duration) for each working day of the last month, available at request

1.4.5 Management of the Foreign Branch servers

The OS Windows central server dedicated to the Foreign Branches are shared, usually with the Operational Units of the relevant Region (Asia – America – Europe). This service consists of the following activities, in charge to Infrastructural & Distributed Systems Dept of "GTS":

- technical and operating management of OS Windows server.
- user profiles management (except the profiling activities within the tools for which the Business Owner of the tool is responsible).
- components, systems, and computer products installation and start.

Contact references for TLC



Summary details of service:

SERVICE	Foreign Branches Hub	Foreign Branches Spoke
International Link	Severity 1: 7 hours	Severity 1: 7 working hours
MPLS connectivity	Severity 2: 9 hours	Severity 2: 9 working hours
Local network Devices (Switch)	7 hours	7 working hours
Firewalls (Perimetral Network Devices)	5 hours	5 working hours
Cisco Phone Service	Major Failure: 9 hours	Major Failure: 9 hours
(Cisco CUCM, VoIP Phone, ecc.)	Minor Failure: 9 working hours	Minor Failure: 9 working hours
	Single Phone: 22 working hours	Single Phone: 21 working hours
IPC Trader Service	Major Failure 3 hours* (During Business Day)	ND
Voice Recording IPC SW	Major Failure 3 hours*	ND

*take in charge time

The service trading phone with the new NICE/IPC system is available on the following Site: NY, London, Hong Kong, Dubai, and their relative spokes.

1.4.6 The Core Applications and mainly the SI-RE platform

- SIRE
- Corporate Banking - INBIZ
- AML Safewatch, AML NetReveal
- KONDOR+
- Back End Trade Finance System - Eximbills
- LoanIQ (LoanIQ/SIRE interface is active on Europe, NY and Asia)
- RICORA
- BOX
- IRION-DQ
- MUREX

1.5 Services provided by "GTS" through outsourcers

"GTS" has the right to outsource at any time, partially or totally, a service by confirming to "DCO – International Network" its intention. "DCO – International Network" must check with the Foreign Branches management any legal or procedural impact deriving from the outsourcing proposal in view to assure that any Regulatory or Legal rules and the Local Country's Industry standards are observed.

Specifically, "DCO – International Network" is in charge to verify that the BIA – Business Impact Analysis is reviewed, and the Business Continuity Plan updated, under the control of Business Continuity and Disaster Recovery Dept.

Then, the Outsourced service is treated as it is provided internally to the Group by "GTS" resources.

1.6 KPI

General Principles

"GTS" will guarantee:

- Efficiency and quality of provided services.
- Flexibility to protect interests of both parties.
- Reliability and safety of performances.

"GTS" has an organizational unit, independent from the units that provide the service, dedicated to operative and quality controls. This unit uses technological instruments (system logs, measurement instruments, problem detection and problem management) to guarantee adequacy and validity of measurements.
Level of service detection is made measuring KPI (Key Performance Indicators) associated to the services provided.
The technological infrastructure is subject to the same management and control processes used for Intesa Sanpaolo systems.
The SLA's represented will be monitored, confirmed/revised and agreed between DCO – International Network and the Supplier.

KPI REPORT

It's agreed that the KPI Report is available after the first 10th of each month on the web Portal of Intesa Sanpaolo - Corporate and Investment Banking Division – ATLANTE 2.0

2 Infrastructure – Main Services and no core Foreign Application provided by "GTS"

2.0 ISP HO Datacenters

The "Facility Management" Services consist in providing the International Network Units with the technological infrastructures, basic system software and personnel to run Data Centres on which the "Internal Customers" can perform on-line and batch elaborations of the applications of its own Information System, managed by the "Application Management" structures of "GTS".
Services are provided through technological components in one or more Data Centres of "GTS" on which basic services are assured (i.e., high availability power supply including fault management service of power generators, cooling, guard with active physical presence h24, 365 days per year, etc.).
In detail, access to protected data rooms is controlled by guards using appropriate security policies (e.g., issuing of access cards for a temporary period or definitively).

The "Facility Management" Service includes activities described below, grouped by type:

- Technological platforms maintenance
- Virtual Farm maintenance
- Backup management
- Operation management
- Operation support
- High Availability and Disaster Recovery
- Basic System SW Licenses (Operating Systems SW, Infrastructure System SW - for example Virtualization SW - and Data Base Management SW)

2.0.1 Common Technological Infrastructure service and maintenance

"GTS" provides main services to its "Internal Customers" through a common infrastructural layer. The services involved in this layer are:

- Physical space
- Physical security
- Fire prevention system
- Redundant Power and Cooling
- Backup Infrastructure and Tape Area Network
- Storage space and Storage Area Network with redundancy according to HA needs
- LAN connectivity with full redundant appliances

2.0.2 Dedicated Technological platforms service and maintenance

On the technological infrastructure dedicated to the "Internal Customers" and within the limits of Facility Management Service, "GTS" performs the following tasks:

- it guarantees correct dimensioning of technological components, with availability and throughputs agreed with Intesa Sanpaolo Spa "DCO – International Network".
- it provides the service in line with Intesa Sanpaolo Group Security Policies.
- it decides how to update products in use, to enable the proper integration with its application services.
- it defines the system monitoring procedures used by the operation management to ensure adequate service levels.

- it provides the amount of storage and CPU processing capacity.
- it offers resource increase.
- it provides a dedicated environment for virtual machine.
- it manages the provisioning of new physical servers.

"GTS" guarantees the Internal Customer's Home Country Regulatory Authorities access rights to the dedicated physical machines, in the server farm at any time, provided the minimal pre-advice for assuring the Security continuous monitoring.

2.0.3 Management of the Workstations (alias Desktop Management) and distributed technologies

- HO manages the distribution and production of the OS layer windows Masterkit for desktop, laptop, and workstations. The customization of the machines is delegated to the local IT structures with respect to the particularities of the HW used
- The Deployment infrastructure has been implemented to allow self-taught autonomous semi-automatic installation for each foreign Branches. The Database and architecture are totally managed by GTS HO.
- MDM: Mobile Device Management (MDM). Used to distribute and manage devices following the CBCM rules, with the possibility for the branch to configure devices and App Blacklist/Whitelist. Support is granted for certified Samsung and iPhone models. The SW architecture is managed by UTD GTS HO while the MDM policy and branch configuration are owned by the local IT.
- Server Printers queue Management (add/remove): HO UTD manages the Printers queue drivers update.
- Additional Software distribution.

2.0.4 Virtual Farm maintenance

"GTS" is responsible for the maintenance of the virtual farm (including Virtual Hosting Foreign Network), ensuring Internal Customer the adequacy of CPU resources available and their levels of redundancy. Supplier defines on behalf of the Internal Customer:

- Quantity, kind, and redundancy methodology of physical servers.
- Type and version of virtualization software.
- Configuration of network used by the virtual infrastructure.
- Provisioning of new virtual servers

The Supplier guarantees *the Internal* Customer*'s Home Country Regulatory Authorities* access *rights to the* dedicated virtual machines, in the virtual server farm *at any time, provided the minimal pre-advice for assuring the Security continuous monitoring.*

2.0.5 Back-up management

"GTS" provides basic backup infrastructure and services like backup software, Tape Area Network, backup LAN and data cartridges, tape maintenance and physical or electronic vaulting. "GTS" acts as a back-up manager to ensure continuity of service in case of malfunctions.
Under the Backup Management service, "GTS" sets criteria related to Backup policies & Data retention, following the specific Home Country Rules of each Internal Customer.

"GTS" main responsibilities are:

- to set-up the Backup Policy, once the available resources and the requested policy have been evaluated.
- to execute the Backup's and restores. data restore activity is in charge to the outsourced Application Management Teams of the Supplier "GTS". that activity is covered by this document, too.
- to offer visibility of the Backup log to the Internal Customer and to the Supplier's Application Management Teams
- Standard backup tool GTS. Previous operations and limits will be ruled with specific user profiles.

2.0.6 Operation Management

As part of the services provided by operation management, the following activities are identified:

- Hardware management: "GTS" manages the hardware components part of the technological infrastructure used for providing services pursuing optimization of performances and consumptions.
- Virtual Farm infrastructure administration: "GTS" is the owner of "server administration", to manage administration processes including monitoring of processes, system performances, disk space and thresholds.
- Monthly reports on monitored servers will be prepared by the supplier and shared with the customer.

2.0.7 Operational Support

As part of the services provided by the operational support the following activities are identified:

- Trouble ticketing management (provisioning standard trouble ticketing tool).
- Incident Management (analysis and fixing of incidents).
- Execution on target site of any manual activities (i.e., reboot a server, insert media in server).
- Handling of magnetic or optical medias.
- Physical server system monitoring.

Supplier uses standard tools feature tracking system to monitor alarms and then reports any HW anomalies or malfunctions.
First level problem determination, unless related to HW malfunctioning, is usually performed by the Internal Customer, supported by the Help Desk.
Recurring activities (i.e., annual capacity planning, extraordinary maintenance, etc..), are defined by the Supplier.
Hardware and software acquiring, and the related maintenance contracts are managed by the Supplier according to the internal policies, following whenever possible, global enterprise contracts.
Application Management (for core/critical tools) and related Change Management are included.

2.0.8 High Availability

"GTS" provides two different systems to guarantee the continuity of those services identified as critical.

The High Availability Solution allows to guarantee continuity of provided critical services in case of faults of a single technical part or in case of unavailability of an entire building, thanks to a specific solution for duplication of data and elaborative resources.
In this solution, all the storage and network devices and servers are redundant in two different buildings of two different sites with a third site still available as Disaster Recovery.
For less critical tools and services, when some or all resources in one building are unavailable, the affected services are moved to the other building (DR) in a short period of time.

2.0.9 Disaster Recovery

The Disaster Recovery solution allows to restore services on a different site from the production ones.
This solution could be activated only in case of complete unavailability of both buildings in production sites.
The decision of DR site activation will be managed according to Intesa Sanpaolo Group Disaster Recovery Policy.
RPO and RTO, as defined below, will be analogous to those of Intesa Sanpaolo Group:

- **RPO (Recovery Point Objective):** shows the time-limit which exists between last available saving of data and applications to be usable after the crash moment. It is therefore the time of data loss that is acceptable.
- **RTO (Recovery Time Objective):** is the duration of time and a service level within which the critical business processes (coming from business impact analysis – BIA) must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity.

RTOs and RPOs are defined at Head Office level for the whole Intesa Sanpaolo Group and agreed with Italian Local Authority, Bank of Italy. Therefore, those parameters are not included in the SLA between Head Office and Foreign Branches since they are defined at Group Level.
The "hot DR" solution activates the system on backup centre restoring the active application environments at the moment immediately preceding the one in which the service block was verified.
The Supplier is available to perform an expected test crash, once a year, which allows to evaluate the described efficiency and the effectiveness of the DR procedures. Procedures to be followed are documented step by step by the Supplier and verified and accepted by the Business Continuity & Disaster Recovery Dept of Intesa Sanpaolo SpA.
In a disaster scenario:

- the Supplier is responsible for the reactivation of infrastructural and technological components.
- the Supplier is responsible for critical application reactivation and organizational aspects related to the handling of the disaster.

2.0.10 Business Continuity Management

The Business Continuity Management is locally managed even if under control of the Head Office – Business Continuity Dept. and the support of the “DCO – International Network”, with the technical support of “GTS”.

Specifically, regarding IT services provided to support foreign branches, GTS declares to adopts the Intesa Sanpaolo Group Business Continuity Management (BCM) model that meets Bank of Italy requirements on BCM topics.

BCM Agreement

GTS is obliged since the very beginning of the deal to have and maintain updated and efficient business continuity plans and tools to guarantee business services supply even if an exceptional emergency event should occur.

Plans shall include and specify all the technological, organisational, and infrastructural measures necessary to guarantee the continuity of services delivered by GTS in case of events that cause:

- Large-scale (metropolitan or greater dimension) physical destruction of the infrastructures essential for the services provided or of third parties.
- Sever crisis situations not connected with physical destruction events (i.e., pandemic flues, biological attacks, etc.).
- Interruption of the functioning of essential infrastructures (including electricity, telecommunication networks, etc.).
- Unavailability of the personnel staffed on the most critical IT processes.
- Destruction or inaccessibility of the facilities in which the operational units or critical equipment are stored.
- Damage to key technological and financial infrastructures caused by a disaster.
- Unavailability or destruction of essential documents.
- Severe damages caused by unfaithful employees.

Specifically:

- as mentioned above, a Disaster Recovery Plan (DRP) is available and back up facilities, systems and infrastructures must be located outside the metropolitan area in which the main business site is located. A Recovery Time Objective (RTO) compatible with the RTO identified in the BIA of the processes in scope and a Recovery Point Objective (RPO) must be as close as possible to zero.
- a Business Continuity Plan (BCP) is available defining logistic and organisational solutions to be applied in case of emergency. Specifically, operational back up sites must be available if normal business premises should be unavailable, and backup personnel and/or capabilities have to be identified in the event that ordinary GTS's personnel should not be available.
- GTS guarantees the operational availability of any essential ICT Centres and facilities that host critical business processes by High Reliability systems solutions (power supply, cooling systems, telecommunications, etc.), to be activated in the event of unavailability of infrastructural services (i.e., a blackout).
- If the SUPPLIER has defined agreements with other contractors or sub-contractors for the delivery of the service, the SUPPLIER shall ensure that those contractors or sub-contractors fulfil the same obligations binding on the SUPPLIER under the service agreement.
- The SUPPLIER undertakes to introduce and regularly update procedures and methods (including suitable controls and data backup) that guarantee, within the scope of its responsibilities, the integrity of the data managed within the scope of Services. to this end, SUPPLIER shall implement techniques at the state-of-the-art for preventing and/or reducing the effects of adverse external events on the operational environment. Where the need for measures not falling within the scope of its responsibility is identified, SUPPLIER shall promptly notify BANK thereof in writing.
- The SUPPLIER undertakes to guarantee the availability of a management-level crisis representative officer (and a substitute) on a permanent basis, responsible for promptly informing the BANK once informed of any event or situation that may represent a

potential critical situation or that may impede the expected delivery of services. If a disaster should hit the Bank, SUPPLIER's crisis representative officer may call upon and involve by the BANK in the management of the crisis and the implementation of business continuity measures in order to prevent any single point of failure.

- The SUPPLIER shall test the DRP and BCP at least once a year. When the BANK runs its own annual tests, SUPPLIER shall ensure its availability to participate in said tests, within the scope of its responsibilities, upon request.
- The SUPPLIER shall be obliged to ensure that service levels do not deteriorate or that the service becomes unavailable in the event that SUPPLIER has committed the same resources to the delivery of similar services to other companies, especially companies located in the same territorial area.
- In the event the BANK activates its own BCP and DRP, the SUPPLIER shall guarantee the continuity of services during emergency operations performed at Bank's back-up sites, as required by the solutions implemented.

2.0.11 Service Provisioning

Operation Management outside service timeframes specified in Chapter 1 will be provided but must be agreed in advance with the Intesa Sanpaolo' supplier.
All planned activities that may stop any production services will be performed in agreed time and, if it is possible, they will be grouped to reduce number of services stop.
All malfunctions must be reported (incident management) using standard tools defined by Intesa Sanpaolo' supplier.
Only problems reported with the above tools are managed. For very urgent problems, Customer could also contact Help Desks by phone/mail/fax, but the problem must be furthered and reported using the above-mentioned tools.
Scheduled stops of service, inside the service timeframes, will be agreed between Supplier and DCO – International Network. Stops of service, inside the service timeframes, must be agreed between Supplier and DCO – International Network in terms of schedule (at least five working days in advance) and duration.
For the measurement of SLA scheduled stops and stops outside timeframes will not be considered.

2.0.12 Middleware IXP/Spazio and IBM MQ

IBM MQ

MQ provides application designers with a mechanism to achieve non-time-dependent architecture. Messages can be sent from one application to another, regardless of whether the applications are running at the same time. If a message receiver application is not running when a sender sends it a message, the queue manager will hold the message until the receiver asks for it. Ordering of all messages is preserved, by default this is in FIFO order of receipt at the local queue within priority of the message.

Interactive Cross Platform (IXP)

IXP (Interactive Cross Platform) architecture is to provide access to common application services, residing on different technological platforms, to "requesting" applications, removing any need to know their physical location and/or the technology of how they communicate.

The IXP infrastructure in the Application Server environment provides an execution environment, where requesting application services, or services called by other applications that use the IXP architecture, can reside.
The solution uses Java classes and is consistent with the J2EE architectural model, and therefore it is open to the various Application Servers that conform to this architecture.
The IXP architecture is made up of three components:

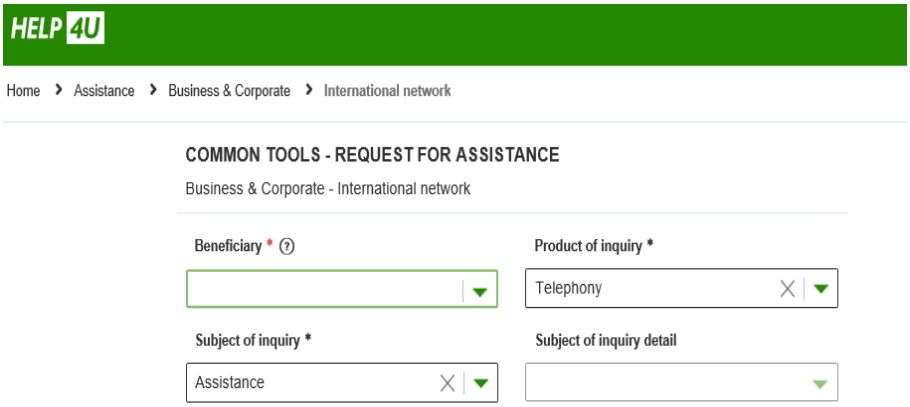
- A requesting component, or IXP-Requester.
- A format conversion support component (ASCII/EBCDIC and vice-versa), IXP-Encoding.
- A receiving component or IXP-Server.

The IXP services supported can be divided into synchronous and asynchronous services. IXP Use the following layer protocols for exchange asynchronous messages: WebSphere MQ and SPAZIO File Transfer

2.0.13 IPC Voice recording

The service is fully localized and managed through the NICE/IPC system dedicated to traders. It is available on NY, London, Hong Kong.

To open a ticket, the User's Branch should open a ticket using the standard ISP portal "Help4U" - Service Now.



2.0.14 Availability of the service - KPI

a) Facility Management Open - Availability and time to re-start: Datacenter Infrastructure - Air conditioning

KPI	Measurement Metrics	SLA	Tolerance	Indicator
Availability and time to re-start: Datacenter Infrastructure - Air conditioning	Air conditioning availability 24x7	99,9%	0	Av

b) Facility Management Open - Availability and time to re-start: Datacenter Infrastructure - UPS

KPI	Measurement Metrics	SLA	Tolerance	Indicator
Availability and time to re-start: Datacenter Infrastructure - Air conditioning	UPS availability 24x7 (fully redundant rotating generator unit)	99,99%	0	Av

2.1 NAS PRODUCTION

GTS Intesa Sanpaolo states that it is not the owner of the data on the NAS, therefore it cannot be held responsible for it. It is also recalled that the ACLs of each individual NAS are managed by the local IT (or reference HUB).

2.1.1 NAS HUB

We define NAS HUB those branches that have both NAS production and DR site locally.

- London
- Hong Kong
- Dubai
- New York
- Istanbul

2.1.2 NAS SPOKE

We define NAS Spoke those branches that have NAS production locally and DR site in Italy.

- Paris
- Frankfurt
- Madrid
- Singapore
- Tokyo
- Abu Dhabi
- Warsaw
- Shangai

2.1.3 CENTRALIZED NAS

We define Centralized NAS Spoke those branches that have both NAS production and DR site in Italy.

- Sydney
- Doha
- Amsterdam

2.2 NAS DR

2.2.1 Content of the service

The scope of the service is to provide a DR service for the NAS of the Foreign Branches.
This service does not cover the HUB Branches as they already have a DR service in place.

2.2.2 NAS DR Recovery times and data retention – Foreign Branches (HK, NY, London)

The Disaster Recovery solution allows to restore service on a different site from the production ones.
RPO and RTO, as defined below, will be analogous to those of Intesa Sanpaolo Group:

- **RPO (Recovery Point Objective):** shows the time-limit which exists between last available saving of data and applications to be usable after the crash moment. It is therefore the time of data loss that is acceptable. In this case the RPO is 12 hours. Please note that, in case of data changes more than 5%, we cannot guarantee this RPO if this causes band saturation or in case of a TLC anomaly which degrades the replication in DR.
- **RTO (Recovery Time Objective):** is the duration of time and a service level within which the critical business processes (coming from business impact analysis – BIA) must be

restored after a disaster to avoid unacceptable consequences associated with a break in continuity. In this case the RTO is 4 hours from DR declaration.
- **Local Internal Copy to the same NAS (internal disk)**
- **Data restore and ACL:** in case of losses the restore of the data is performed autonomously by the IT of each Hub.

The Supplier will create new KPI in according with business priorities.

2.2.3 NAS DR Recovery times and data retention – Foreign Branches with DR site (Dubai, Istanbul)

The Disaster Recovery solution allows to restore service on a different site from the production ones.
RPO and RTO, as defined below, will be analogous to those of Intesa Sanpaolo Group:

- **RPO (Recovery Point Objective):** shows the time-limit which exists between last available saving of data and applications to be usable after the crash moment. It is therefore the time of data loss that is acceptable. In this case the RPO is 24 hours. Please note that, in case of data changes more than 5%, we cannot guarantee this RPO if this causes band saturation or in case of a TLC anomaly which degrades the replication in DR.
- **RTO (Recovery Time Objective):** is the duration of time and a service level within which the critical business processes (coming from business impact analysis – BIA) must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity. In this case the RTO is 4 hours from DR declaration.
- **Local Internal Copy to the same NAS (internal disk)**
- **Data restore and ACL:** in case of losses the restore of the data is performed autonomously by the IT of each Hub.

The Supplier will create new KPI in according with business priorities.

2.2.4 NAS DR Recovery times and data retention - Spoke branches + Sydney, Doha and Amsterdam branches

The Disaster Recovery solution allows to restore service on a different site from the production ones.
RPO and RTO, as defined below, will be analogous to those of Intesa Sanpaolo Group:

- **RPO (Recovery Point Objective):** shows the time-limit which exists between last available saving of data and applications to be usable after the crash moment. It is therefore the time of data loss that is acceptable. In this case the RPO is 24 (Twenty-four) hours for data at previous day (T -1). Please note that, in case of data changes more than 5%, we cannot guarantee this RPO if this causes band saturation or in case of a TLC anomaly which degrades the replication in DR.
- **RTO (Recovery Time Objective):** is the duration of time and a service level within which the critical business processes (coming from business impact analysis – BIA) must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity. In this case the RTO is 8 (eight) hours from DR declaration.
- **Data Retention:** The data retention of the files on the NAS, that is to say the number of years' data is kept online, is 10 (ten) years.
- **Local Internal Copy to the same NAS (internal disk)**
- **Remote copy from local NAS to Italy is scheduled after local business hours every day**
- **Complete replication of local NAS to Italy during the night (Branch local time)**

- **DR tests (or True DR) are fully guaranteed at maximum for two branches at the same time** according to the current setting of the machines.
- **Data restore e ACL**: in case of losses, each spoke can refer to the competent Hub for the restore of the data.

2.2.5 Availability of the service - KPI

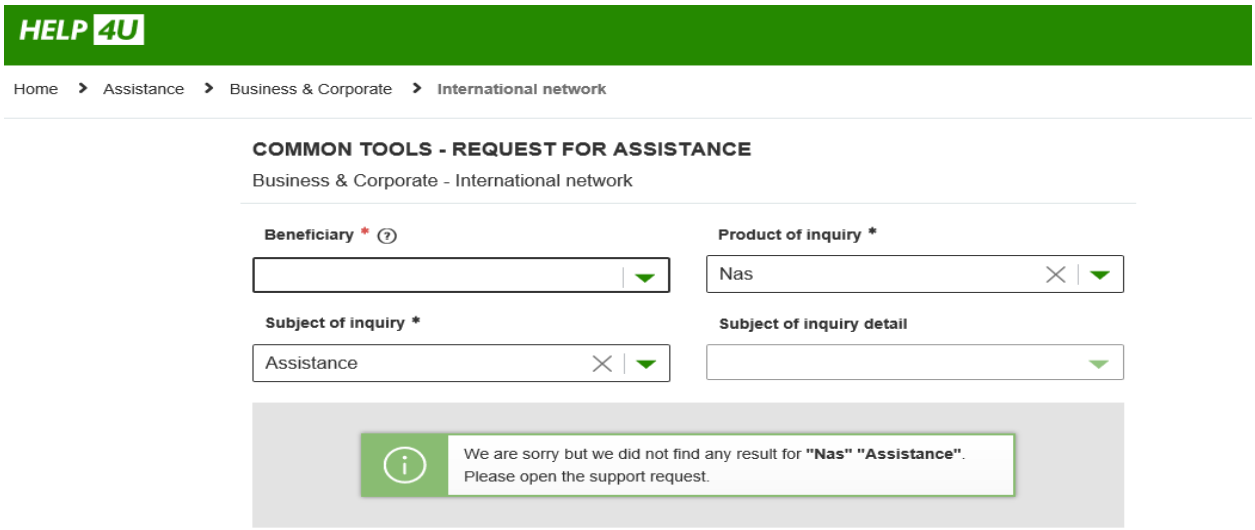
There are three levels of support:

1. The First Support Level: local help desk (as is).
2. The Second Level: Head Office (HO First Level).
3. The Third Level (HO Second Level): take in charge of the ticket forwarded by the Help Desk HO First Level.

The issues must be categorized as follow:

- Service Request (CR)
  - Is a not blocking issue that will be managed only during the direct support period. If HO First Level will receive a CR during the on-demand support period, it will be taken in charge at the beginning of the direct support period.
- Incident Request (IR)
  - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Common Tools – Request for Assistance – NAS".



The Supplier will create new KPI in according with business priorities.

2.3 NETWORKING and Internet Services

2.3.1 Service Description

The service consists in realization, evolution and tuning of connectivity services, respecting the Internal Customer needs, from the Internal Customer main and BC/DR site (if any) to Italian Data Centres (primary/secondary/DR) where the services described in previous chapters will be active.

The service is based on two main components:

• **International connectivity** between the Internal Customer site(s) and Italian Data Centres.
• **Telecommunication technological infrastructure** arranged in primary/secondary data centre (production sites) and the Disaster Recovery site.

2.3.2 International Connectivity

High speed and High Availability connectivity services will be delivered between the Internal Customer site(s) and Italian Data Centres. Service is based on virtual private networking connection on a private network infrastructure with Multiprotocol Label Switching (MPLS) technology.
The connection is realized differing both nodes and connection devices on provider side (POP geographically diversified). Incoming traffic from the Internal Customer site(s) will be directed on one of the two Italian Data Centres using dynamic routing (BGP).
The Internal Customer site(s) and Italian Data Centres will be provided with completely redundant configuration both for connectivity to private network and connection appliances. Diversification on node and connection devices on provider site will be available (POP geographically diversified) and the path of local loop from PE to CE installed at the Internal Customer site(s) will be diversified. On the functional point of view, data transmission between the Internal Customer site(s) and both Italian Data Centres will be encrypted. The whole infrastructure realization can guarantee to Internal Customer and Supplier the possibility to use distinct logical layers.
On quantitative side, the access to service speed will be guaranteed to the 50% of available throughput.
At the internal Customer site(s), TLC provider will install router appliance CE (Custom Edge). These routers will define the boundary between the TLC carrier ambit (chosen by the Supplier) and the Supplier responsibility.
CE Router will identify the area in which the TLC Carrier operates. CE Routers will be provided, maintained and managed by the Carrier.
CPE (Customer Premise Equipment) Routers represent the routing component managed by the Supplier at the internal Customer site(s). These Routers define the boundary of the internal Customer site(s) network on which local users and services remain connected.

2.3.3 Telecommunication Infrastructure in the Italian Data Centers

The telecommunication technological infrastructure for services described in previous paragraph will be realized in Italian Data Centers according to architectural choice and quantity identified in design phase. The TLC infrastructure will enable the connection to reach applicative and technological environment involved in Facility Management service.
The internal Customer IP addressing plan is part of the common Intesa Sanpaolo SpA plan, even if separately managed, both in the case of public or private RFC1918 address range is in use.

2.3.4 Service provisioning

Services belonging to previous classification include:

- supply of geographical international network connectivity.
- supply of local network connectivity in primary / secondary and DR Data centres.
- supply and configuration of telecommunication devices (routing, switching, firewalling and Wi-Fi).
- under specific request from Cyber Security or/and Audit, where devices are already capable, it is possible to enable authentication protocol 802.1x on ports of the switches dedicated to the users (specific vlans) that enable connection on basis of a machine

certificate is issued by the corporate CA, in order to let local Cyber Security ensure a Network Access Control. authentication still reside on corporate DC and specific policies can be enable on centralized control cluster (ISE) following HQ Cyber Security best practices.

- maintenance of all components (HW and SW) of described telecommunication infrastructure.
- connection operative management:
- Network surveillance and Fault management: real-time infrastructure monitoring, 2nd level help desk, analysis and solution (remote or on-site) of troubles, maintenance of routing, switching, Wi-Fi and firewalling devices.
- About on-site intervention, it is in charge to the Internal Customer to indicate the procedures to follow in order to enable access to devices to Supplier or identified maintenance third parties' people.
- Performance management: measurement and reporting on service's performance.

2.3.5 Network Management

Network connection in this agreement will be proactively monitored by the Intesa Sanpaolo Supplier through a real-time network management platform.

2.3.6 Vulnerability Assessment test

A Network Vulnerability Assessments (NVA), on year based, is conducted by an independent third-party team, using independent security assessment tools from the internal network coordinated by GTS Security Department, on the most critical infrastructures in terms of sensitive data stored.
A periodic update of the corrective action plan is distributed to each foreign branch, until fully resolution of the detected issues.

2.3.7 Availability of the service – KPI

SLA computation will be based on following parameters:

- **Network availability**
- **Time to Repair**
- **Quality of Network for geographical link**

Scheduled stops of service, inside the service timeframes, will be agreed between Supplier and the Internal Customer.
Stops of service, inside the service timeframes, must be agreed between Supplier and Internal Customer in terms of schedule (at least five days in advance) and duration.
For the measurement of SLA scheduled stops and stops outside timeframes will not be considered.
The technological infrastructure is subject to the same management and control processes used for Intesa Sanpaolo systems.
The SLA's represented will be monitored, confirmed/revised and agreed between DCO – International Network and Supplier.

2.3.8 Network Availability

a) Geographical Link

Geographical link is considered available if from Intesa Sanpaolo network equipment installed in the Internal customer site(s) (CPE) at least one of the two TLC equipment present in Italy is reachable (ping).
Formula: **100 * (1 - (total time of unavailability in observation time)/observation time))**.
Observation time = 1 year, 24 hours for day

The proposed SLA is 99,9%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
TLC Network Availability: Geographical Link (Yearly measurement)	Geographical link is considered available if from Intesa Sanpaolo network equipment installed in the Internal customer site(s) (CPE) at least one of the two TLC equipment present in Italy is reachable (ping). Formula: 100 * (1 - (total time of unavailability in observation time)/observation time)). Observation time = 1 year, 24 hours for day	99,9%	0	Av

b) Geographical Connection

Service recovery time will be measured based on time interval passing from the first report of the problem to the resolution report done by Supplier and its formal confirmation by the Internal Customer. Above service recovery times are dependent on Service Level provided by local third parties to the Supplier.

Service recovery time: Defined as the time between the first appearance of the problem and the recovery of availability of the service.

Service recovery time is classified using following categories:

• **High level fault.** A fault is called 'high level' when it is the cause of a stop in communication from switches in the Internal Customer site(s) to Italy or vice versa.

The proposed SLA for high level faults, service recovery time won't be longer than: 7 hours

KPI	Measurement Metrics	SLA	Tolerance	Indicator
TLC Geographical Connection (CE to CE) - Service recovery time High level fault	Service recovery time: Defined as the time between the first appearance of the problem and the recovery of availability of the service. High level fault: A fault is called 'high level' when it is the cause of a stop in communication from switches in the Internal Customer site(s) to Italy or vice versa.	420	0	P

• **Medium level fault:** A fault is called 'medium level' when only one international channel is available and the communication between the Internal Customer site(s) with CE in Italy is possible through that channel.

The proposed SLA for medium level faults, service recovery time won't be longer than: 9 hours

KPI	Measurement Metrics	SLA	Tolerance	Indicator
TLC Geographical Connection (CE to CE) - Service recovery time Medium level fault	Service recovery time: Defined as the time between the first appearance of the problem and the recovery of availability of the service. Medium level fault: A fault is called 'medium level' when only one International channel is available and the	540	0	P

	communication between the Internal Customer site(s) with CE in Italy is possible through that channel.			

c) Geographical Link Appliances (CPE's)
For these appliances the proposed KPI is the time to repair in case of fault causing stop in communication of a single appliance with correspondent appliance in Italy and vice versa.
Time for intervention: Defined as the time between the first appearance of the problem and the intervention (physical or remote access to equipment) to solve problems.
The proposed SLA for time for intervention won't be longer than: 7 hours

All the Geographical Link TLC Appliances are configured in High Availability to reduce service stop.

KPI	Measurement Metrics	SLA	Tolerance	Indicator
TLC Geographical Link Appliances (CPE's) - Time for intervention	Time for intervention: Defined as the time between the first appearance of the problem and the intervention (physical or remote access to equipment) to solve problems.	420	0	P

d) TLC Server Farm Switches - Service recovery time
Service recovery time: Defined as the time between the first appearance of the problem and the recovery of availability of the service. For these appliances the proposed KPI is the time to repair in case of fault.

The proposed SLA for time for intervention won't be longer than: 7 hours

KPI	Measurement Metrics	SLA	Tolerance	Indicator
TLC Server Farm Switches - Service recovery time	Service recovery time: Defined as the time between the first appearance of the problem and the recovery of availability of the service. For these appliances the proposed KPI is the time to repair in case of fault.	420	0	P

Local network devices
To ensure the maintenance of all network components installed at the foreign branches (HW, SW), GTS Telecommunications department subscribed support agreements with worldwide coverage partners. Recovery times are divided into two categories, depending on the service type (data or voice service-related device), and are subject to the following reference recovery values:

1. ***Data network devices.***

- Seven hours for HUB head offices, regardless of the business or non-business time window.
- Seven working hours for spoke foreign branches, referred to branch local time zone.
- Next Business Day for local VPN gateway

2. ***Voice network devices (Subscribers, voice gateways, phones)***

Defined as blocking a fault when it impacts more than 50% of users in the single branch (hub or spoke), non-blocking when it impacts up to 50% of users or is related to non-business critical features:

- Nine hours for blocking faults (regardless of the business or non-business time window).
- Nine working hours for non-blocking faults.
- Twenty-two working hours for a fault on the single phone.

3. Cisco Identity Services Engine (ISE) for protocol 802.1x where enables

- For blocking faults (regardless of the business or non-business time window) an authentication bypass is enabled in order to ensure business continuity in case of fault or unreachability of the Central Infrastructure.
- Next business day for non-blocking faults.

4.3.2. Provisioning

Geographical Connection Improvements: exclusion

Every update of bandwidth of the geographical connection or any other change in configurations will be managed with dedicated analysis and as specific projects, so it won't be included in present agreement.

2.4 Help desk

2.4.1 Content of the service

Since "GTS" shall assure to each Foreign Branch the capability to work remotely, it is very important to have an efficient way to monitor any problem concerning every single step of the monitored processes.

The help desk support activities are in charge:

a) to Infrastructural & Distributed Systems Dept:
The Foreign Branch / Bank staff must immediately communicate any kind of problem or malfunctioning occurred to a centralized hardware/process or service and to any locally installed hardware under the control of "GTS". The service is available 24/24 hours and 7 days per week [1].
Alerts/enquiries must be sent to the Help Desk Group by using the specifically designed web tool (Help 4U). The Help Desk Group must dispatch it within the following 15 minutes to the relevant Maintenance Team, confirming the execution to the Foreign Branch as soon as the Problem Determination Task has been terminated.

Alternatively, the TLC support can be reached via phone (0115555511).
On request, the Help Desk Group will keep the Foreign Branch staff updated about progresses on reported problems.

For non-critical problems, errors or questions the Help Desk Group may postpone the intervention of the relevant Maintenance Team till the day-after (from 08:25 a.m. to 04:55 p.m. CET time).

b) to Financial & Foreign Applications Dept:
The Foreign Branch staff must immediately report any kind of problem or malfunctioning occurred to the core SIRE application by using the specifically designed web tool (Help 4U). the team is available at any time to fix errors. for support activities, the SIRE Support Group is available during standard Italian working hours (from 08:25 a.m. to 04:55 p.m. CET time).

Non-critical actions can be performed the day-after or later on: "evolutive" maintenance requests has to be reported to "DCO – International Network" too, and the intervention plans will be decided in agreement with the Foreign Branch management.

2.4.2 Availability of the service – KPI

Even outside the perimeter of the Business Continuity Plan, the Foreign Branch staff is supported during its working hours by the "GTS" structure in view to smoothly perform its daily operations.

Any breach to the Help Desk service availability is immediately reported by the Foreign Branch staff to "DCO – International Network" which is in charge to decide with "GTS" Service Manager on-duty the consequent actions.

On 2024 The Supplier will create new KPI in according with business priorities.

2.5 Centralized E-mail service

2.5.1 Content of the service

"GTS" provides Foreign Branches, having accepted an outsourced service and this Service Level Agreement, with a centralized e-mail service, based on a hybrid Microsoft Exchange Server platform (on-premises) and Office365 cloud infrastructure.

The list of the main services provided is:
• Personal email accounts
• Group email accounts
• Integrated Fax Server
• Exposure of Application SMTP services
• Exposure of EWS services – Exchange Web Services
• Self-service management tools – Web Delegation
• Integration with company mobile devices
• Access to mailboxes both from the internet and from intranet through OWA or specific mail client

Standard configuration architecture provides for routing e-mail service over an Internet connection (the bandwidth is decided by each Operational Unit, which is in charge for supplying the connectivity: as large as economically sustainable). In case of troubles, service can be switched over MPLS connection (by using webmail service over Intranet). Wherever it's technically possible, the primary Internet connection fiber link is doubled by a satellite Internet link, supplied by the Operational Unit.

Being the service qualified as "critical" in respect of the Group's daily operations, "GTS" guarantees that the service:

a. is based on a High Availability Infrastructural Solution which allows the continuity in case of faults of a single technical part or in case of unavailability of an entire building.
b. the technical infrastructure is hosted in 3 different sites (aimed to support the Production, Business Continuity and Disaster Recovery environments), according with the certified Business Continuity Model.

c. is supplied as a non-interrupted service 365 days per year / 7 days / 24 hours.
d. is supported by the same Help Desk infrastructure operating as a common entry point for all the services provided by GTS (SIRE service excluded). Help Desk support is available 24/24 hours and 6 days per week (Sunday night to Saturday morning, CET[12]).

Any Operational Unit User is provided with a personal mailbox, by default. Group mailboxes and Group Distribution lists are provided on request. In conformity with the Intesa Sanpaolo Group policies, "GTS" provides the following functionalities to each group & personal mailbox:

a. transmission
b. archiving
c. journaling

2.5.2 Transmission

Incoming & outgoing messages are processed provided that:

a. size is no more than 30 MB (attachments included).
b. messages don't contain any attachment contrary to the ISP Group policy (e.g. .exe files).
c. messages don't infringe the security rules.

2.5.3 Journaling

The functionality allows the Operational Units of the Intesa Sanpaolo Group to cope with the Legal Archiving rules. Journaling will archive (independently from the Archiving function) all inbound and outbound message traffic for legal and compliance purposes. In fact, the Journaling function is set-up for:

- Archiving all inbound and outbound message traffic automatically in a protected database
- Storing and indexing all messages for legal purposes
- Allowing the access to the protected database to specific Governance bodies (Users cannot have access to it)
- Retain all messages (default configuration) for 10 Years
- Allowing the Users to delete their messages without infringing the Best Practice rules

2.5.4 Availability of the service – KPI

SLA computation will be based on following parameters:

- **E-mail service availability**
- **Quality of the ticket management**

No scheduled stops of service, inside the service timeframes, are admitted.

a) <u>E-mail service availability</u>

E-mail service is considered as "available" if from an Intesa Sanpaolo Operational Unit workstation at least one out of the servers present in Italy is reachable (ping).
Formula used to calculate the availability is the following.
100 * (1 - (total time of unavailability in observation time)/observation time))
observation time = 1 year, 24 hours per day

[12] From Sunday h 23.58 to Saturday 07.00 CET time; during the uncovered time, service is assured by people on-duty of-site by calling +39-3357421121

The SLA for yearly availability of e-mail service is 98,00%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
MAIL-D-availability of email service	Percentage of system availability than the theoretical time defined	98	2	Av

b) Quality ticket management

Number of tickets opened for Application anomalies compared to the number of users of the Service and compared with its average index.

The SLA for yearly availability of e-mail service is 92,00%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
ELECTRONIC MAIL-A-Number of tickets	Number of tickets opened for Application anomalies compared to the number of users of the Service and compared with its average index Percentage	92	2	A

To open a ticket, the User's Branch should open a ticket using the standard ISP portal "Help4U" - Service Now. (Home > Assistance > Sharing and Comunication >…)

2.6 Multimedia services

2.6.1 Service description

The Supplier shall ensure the provisioning of the following macro-service (hereinafter the service):

2.6.2 Video conference

This service enables the audio and video communications through dedicated videoconference equipment that can connect each other via the corporate LAN or the public ISDN network.
The base services guaranteed under this Service Agreement are mentioned below:

- Video communications between 2 videoconference rooms.
- Multiple video communications

- Possibility to connect in the same session videoconference equipment, telephones and PC laptops with appropriate dedicated real time communication tools.
- Possibility to display to remote sites images from a PC.
- Audio conference
- Integration with real time collaboration tools in point-to-point and multipoint calls

The main technical definitions describing the service are reported below:

- **Audio Conference** represents a call conference that connects more than 3 users simultaneously, managed centrally from the Control Room VDC.
- **Video conference** represents a video communication session that connects 2 videoconference rooms. The management of these calls is handled independently by the user who has to book the rooms, has to access and arrange to make the call (with the possible support of the Control Room VDC).
- **Multi Video Conference** represents a multi video conference session that normally connects 3 or more videoconference rooms, centrally managed by the Control Room VDC of Moncalieri. Also, the video conference sessions between two rooms ("point - point" connection), that are not centrally managed, are included in the statistics.

The supply of the services described above is completed by the delivery and the management of the video conference and includes the following activities:

- management of requests for the new assignment of equipment.
- management of requests of transfer of equipment.
- maintenance of functional defects and accidental failures of equipment.
- first support service provided by Control Room VDC.
- V.I.P. support for Country and General Manager Board Room VDC (real time response for malfunctioning intervention)

The typologies of videoconference rooms are:

- **Standard Video conference**
  Solution with desk equipment
  Standard solution single monitor.
- **Video conference for the board meeting rooms**
  ad hoc solution, based on the peculiarities of the room (availability of large monitors, 65" or more, video projection, automatic focus calibration on the speaker with the opportunity to include automation of several components with ad hoc domotical solutions, etc).

Requests

All supplies related to equipment or accessories, should be made through formal requests using the standard tool Help4U available on the website of Intesa Sanpaolo as stated in the applicable policies.

Malfunction Report

In order to report any possible malfunctions, the Customer should open an Incident in Help4U and can be assisted by Control Room VDC, dialing the phone number +0039 - 011-555.2599.

Responsibilities and obligations of the Customer

The Customer undertakes:

- not to alter or modify the connections of the equipment of the video conference workstation (monitor, codec, microphones etc.).
- to promptly inform Control Room VDC about any possible malfunctions or other various difficulties.

2.6.3 Real time collaboration tool

Introduction

The Real Time Collaboration service is provided through a software application that allows you to carry out chat, audio, video communications and share applications between users from your company PC

The provided solution includes the following features:

- find out the availability of a colleague through the presence service
- ability to send Instant Messaging (IM).
- Conferencing: 1 to 1 audio/video call and 1 to N audio/video call with traditional videoconferencing and traditional telephony systems
- document sharing
- whose features are described in following chapters.

Technical solution

Here following you can find a detailed description of all features included in provided solution.

Presence

Presence information enables users to approach colleagues at the right time with the right form of communication, to lead to a more productive work environment. A user's presence is a collection of information that includes availability, willingness to communicate, additional notes (such as location and status), and how the user can be contacted.

Instant Messaging (IM)

With the instant messaging, users can quickly message each other with timely information.

Conferencing

Collaboration tool includes support for IM conferencing, audio-conferencing, web-conferencing, videoconferencing, and application sharing, for both scheduled and impromptu meetings. All these meeting types are supported with a single client.

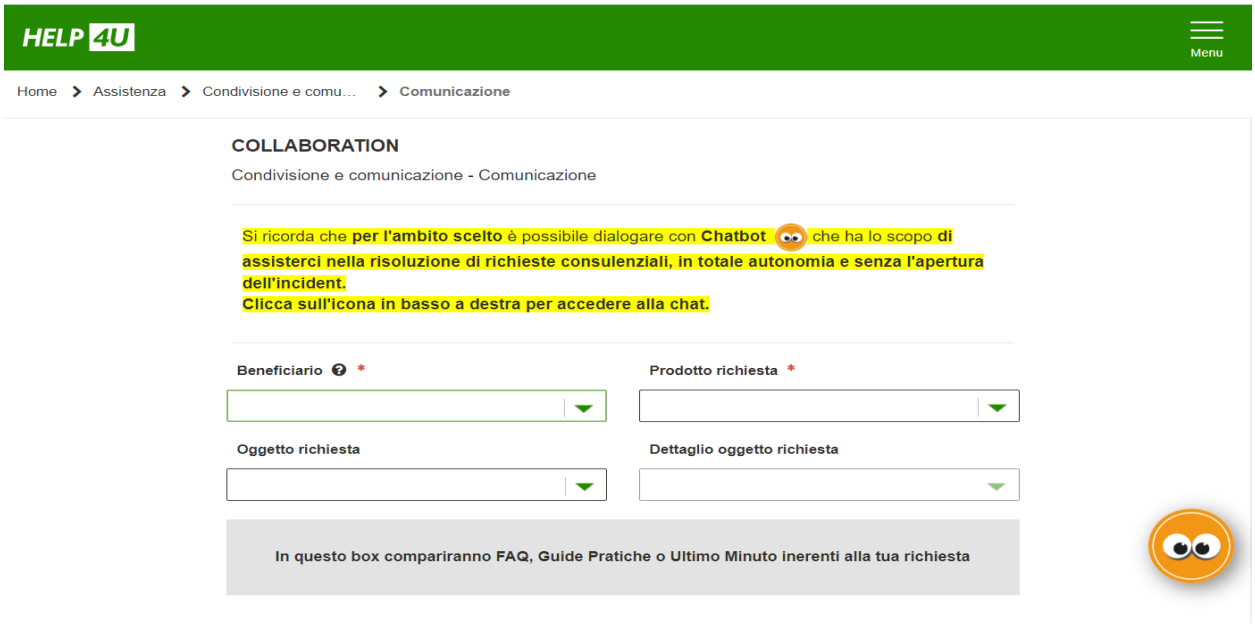
Conferences can seamlessly change and grow in real time. For example, a single conference can start as just instant messages between a few users and escalate to an audio conference with desktop sharing and a larger audience instantly, easily, and without interrupting the conversation flow.

Standard Profile Features

It provides the following functionalities:

- Presence.
- Chat.
- Desktop Sharing.
- Application Sharing.
- One to One Audio Conference.
- Multi Audio Conference.
- One to One Video Conference.
- Multi Video Conference.
- Online Meeting.

To open a ticket, the User's Branch should open a ticket using the standard ISP portal "Help4U" - Service Now. (Home > Assistance > Sharing and Comunication >…): requests for Document Area and Collaboration Services can be found here (an example follows)



2.7 Service Delivery

2.7.1 Regulatory constraints

In accordance with the requirements of the legislation on outsourcing, the Intesa Sanpaolo Supplier declares that the service will be provided from Italy. Any changes shall be agreed with the Customer Intesa Sanpaolo GTS and Operation Network in advance.

2.7.2 Target Calendar

All timeframes mentioned in the following chapters are based on Italian working days. Working days are from Monday to Friday.

Operational Help Desk – Provides assistance and support
8:30am – 1:30pm / 2:30 – 5:30pm – Monday to Friday, excluding holidays.

2.7.3 Support

Supplier will provide an adequate training to person identified by the Customer in order to give him the possibility of spreading the knowledge and setup a first level support. In addition, the Intesa Sanpaolo Supplier will provide second level support available through a web-based tool. Problems could be reported in English or Italian.

2.7.4 Obligations of the Customer

The client agrees to promptly notify the Supplier detected inefficiencies in the manner to be agreed between the Parties; verify that your Employee Personnel intended to use the operational tools made available by the Supplier is adequately trained and know how to use each type of documentation available to support normal activity; informs the Supplier about its plans or short-, medium- and long-term projects that may have direct or indirect influence on the provision of services, so as to enable the supplier to plan the management and control of the services and their adaptation the needs arising from these plans and projects.

2.8 Service Management

2.8.1 Critical Issues Management

2.8.1.1 Management of anomalies

Goal of management of anomalies is to analyze, formalize and fix all issues related to a non-compliance of delivery process that could potentially affect service levels. Two distinct areas could be identified:

- Management of anomalies related to service requests
- Management of anomalies related to provided services

The problems that are encountered by the Supplier when providing the Services will therefore be handled according to the procedures described below.

2.8.1.2 Management of anomalies related to service requests

If Customer detects a supposed case of non-compliance of service request management processes, such in case service delayed or not provided at all, complains must be sent to the Supplier's unit that received the original request.
In case of repeated and systematic non-compliance in on-demand service delivery processes, Representative of the Customer may call upon Representative of the Supplier.

2.8.1.3 Management of anomalies related to provided services

This process defines the interfaces to involve and the escalation paths to be followed according to problem severity.
Problem is classified by the Supplier detecting it (directly or on Customer 's input) in order to properly define its level of severity and therefore which person or team to involve to properly manage it.
In any case the Representative of the Supplier will promptly report the problem detected to the Representative of the Customer.
Since the actual impact can only be measured afterwards, in the early phase only the estimated impact would be considered.
On the base of problem severity level, different Parties could be involved with different approaches, following the well-known escalation process.

2.8.2 Meetings

2.8.2.1 Recurring meetings on service level

Meetings are called by the Supplier with the purpose of evaluating Customer satisfaction on provided services.
Special focus is made on:

- Check of service level guaranteed in the last period of time.
- Actions for increasing service level.
- Financial questions related to provided services.

This kind of meeting is held usually every year, except in case Supplier and Customer agree on other scheduling. Parties can agree on holding the meeting using a videoconference system.
Following persons attend at the meeting:

- Supplier Representative owner of relationship with Customer.
- Representative of the Customer.
- Other persons responsible for face arguments into agenda.

Two days before the meeting, Representative of the Supplier will send following documents:

- Meeting agenda including document related to cover arguments.
- Previous meeting minutes.

After the meeting, Representative of the Supplier will:

- Write a minute of the meeting including list of attending persons, examined arguments, meeting decisions.
- Send a draft of the above minutes to all attendants.
- Wait 5 days in order to receive comments from the attendants,
- Publish the agreed final version of the minutes to the meeting attendants.

2.8.2.2 Meetings on Customer Request

At Customer requested meetings will attend:

- Representative of the Supplier.
- Representative of the Customer.
- Other persons useful to face arguments in agenda.

This kind of meeting could not be called more than two times per year, except in case Supplier agree on different frequency due to specific critical issues or due to some specific running project.

2.8.2.3 Changes to the provided service

New services activation or essential modification to the existing ones could be originated from extraordinary requests and with following consequences:

- Definition of new products/services provided to the Customer.
- Substantial modification of provided services.

In these circumstances it is necessary to activate the provided service change process in order to manage and formalize to the Customer an agreement modification proposal. The validity of proposed modification will be effective only after approval from both Parties. The change process has to be guide by Digital Business Partner

2.8.2.4 Change Management scope

Provided service change process can be activated:

- after Representative of the Customer request.
- after Representative of the Supplier request.

2.8.3 Communication between the Parties

Communication between the Parties could be done using e-mail or any other agreed tool but it must be only in English.

3 Main Services / Applications provided by GTS

3.0 Main Services/applications

SIRE Core Business

3.0.1 Content of the service

“GTS” provides Foreign Branches, that accepted an outsourced service and this Service Level Agreement, with a centralized SI/RE (“Sistema Informativo Rete Estera”, later SIRE) management supplied in conformity with Head Office standard.

The current IT architecture is based on SIRE centric integrated with satellite systems and target applications (Front Office systems, Payment HUB, Credits, DRM, Planning and Control, General Accounting etc.).

System Characteristics – General Overview

Multi-Bank
The Foreign Network in the scope includes ISP foreign branches and ISP Ireland. Currently the system manages different bank entities by separated installation and individual configuration of templates and data flows according to each bank needs.

Multi-Branch
Currently the system manages different branches of ISP by separated installations and individual configuration of reports, templates, and data flows according to each branch needs.

Multi-Currency
For each separated installation (one per branch), it is possible to have individual set of foreign currencies, a local currency of balance sheet and P&L statement and a country currency.

Multi-Calendar
For each country, where the branch is located, it is possible to have individual calendar with holidays of the local currency.

Multi-Time zone
Currently the instances are grouped in the partitions according to the criteria of the nearest time zone. For example, all European branches (London excluded) and Istanbul are installed on European server, London ISP, London IMI on the GMT server, Mid Oriental branches that follow Islamic calendar are on UAE server, Asian branches are on SEA server and finally US branches are on EST server. Within the same server, the system time is that of the prevalent time zone.

Access and Navigation Security
System access habilitation, authority level and available functionality are managed by authorization group according to ISP policy on the matter.

Security and Audit requirements
The following requirements are fulfilled:

- It is possible to profile users according to roles and branches department.
- The association between users and profiles is obtained by a central system.
- An Audit trail is available for every transaction.

3.0.2 Connection to the Application

The access to the SIRE Application is done using 5250 client and based on the standard SPIMI's domain connection:
The system architectures are supported by:

- Technology farms/Campus located in Moncalieri for production
- Settimo Torinese for Business Continuity
- Parma for Disaster Recovery

3.0.3 Availability of the service - KPI

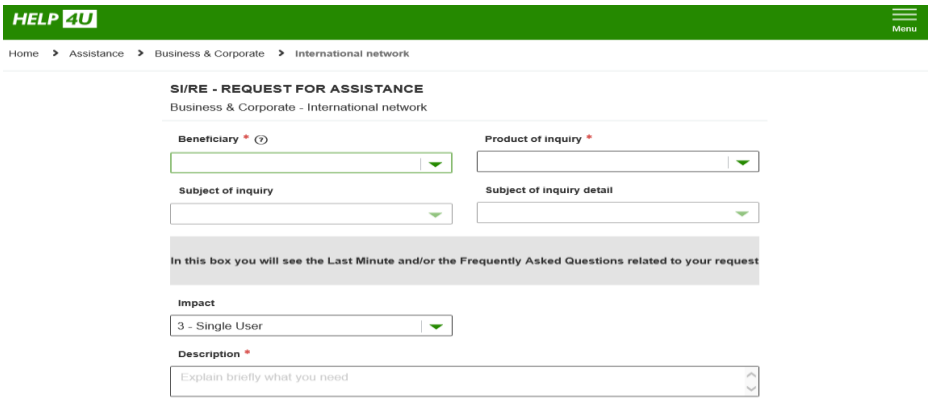
There are two levels of support:

- The First Support Level is in charge of “HUB” Support for First Level of resolution
- The Second Level is divided into “SIRE_1” and “SIRE_2“

The issues must be categorized as follow:

- Service Request
- Incident

To open a ticket, the User’s Branch should open a ticket using the standard ISP portal “Help4U” - Service Now.



User’s Branch doesn’t have to contact directly SIRE HD to open a ticket.
SIRE HD (online) support is guaranteed from Monday till Friday, from 8:30 till 18:30 (CET).
Other availability (only in case of emergency - On-call service) is guaranteed:

- Monday – Friday: 18:30 – 8:30 (CET)
- Saturday – Sunday: 8:30 – 24:00 (CET)

KPI AS400 – for SIRE CORE

a) Facility Management - Availability and time to re-start: AS400 - Secure FTP (SSH - Transport Component)
Servers’ availability, percentage of system availability time respect to total, for Intel / AS400 based systems based on 7x24 application services.

Formula: Ratio: 100 * (∑i of availability time of system) / (∑i of total time of service in the month)
Observation time = 24x7

The proposed SLA for yearly availability is 99,5%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
FACILITY MANAGEMENT - Availability and time to re-start: AS400 - Secure FTP (SSH - Transport Component)	Servers’ availability, percentage of system availability time respect to total, for Intel / AS400 based systems based on 7x24 application services. Ratio: 100 * (∑i of availability time of system) / (∑i of total time of service in the month)	99,5%	0	Av

a) Facility Management - Availability and time to re-start: AS400 - Server Component
Servers' availability, percentage of system availability time respect to total, for Intel / AS400 based systems based on 7x24 application services.
Formula: Ratio: 100 * (∑i of availability time of system) / (∑i of total time of service in the month)
Observation time = 24x7
The proposed SLA for yearly availability is 99,9%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
FACILITY MANAGEMENT - Availability and time to re-start: AS400 - Server Component	Servers' availability, percentage of system availability time respect to total, for Intel / AS400 based systems based on 7x24 application services. Ratio: 100 * (∑i of availability time of system) / (∑i of total time of service in the month)	99,9%	0	Av

Following restrictions apply to KPI computation: WAN, LAN and related server anomalies will not affect KPI computation.

3.0.4 Data Layer

Introduction of a new summary system (Data Layer) to cover the functionality of SIRE for FEs in budgeting and accounting, reporting to local authorities, and to Head Office functions.
Typically, supervision is guaranteed starting from the evening/night of the last day of the month to ensure the success of the EOD (End of Day)/EOM (End of Month) batches and the sending of the provisional files to Supervision (desired by 7 am the following morning).
Subsequently, the evolutions of the first days of the following month are followed (T1, T2 and T3) until the last validation of the balance in T+3 made by New York with conclusion around midnight or in any case in the night between the third and fourth working day.

Service	Day coverage	Hourly coverage
Ordinary service	All working days Italian calendar	08:30 - 18:30 (CET)
Availability	- Last day of previous month - First, second and third day of the following month	From 6.30pm to 8.30am (CET) the following day

To open a ticket, the User's Branch should open a ticket using the standard ISP portal "Help4U" - Service Now.

3.1 Corporate Banking

3.1.1 Content of the service

The Supplier shall ensure the provisioning of the following macro-activities; the relationship between the Inbiz application and the IMI CIB Division takes place through the Global Transaction Banking Department within the Division.

- ***Internet Corporate Banking (Inbiz)***

  The service consists of:
  - Making available all applications covered by the service.
  - Providing corrective maintenance of all applications covered by the service.
  - Providing regulatory maintenance of all applications covered by the service.
  - Providing evolutionary maintenance of all applications covered by the service.
  - Planning and delivering the service.
  - Providing appropriate test and production environments.
  - Providing operational and technical support.

  Corrective maintenance consists of:
  - Troubleshooting application errors.
  - Planning and applying all changes needed in order to restore proper operation level of all applications including incidental restore of databases.

  Moreover, Integrated Application Management includes provisioning of all tasks needed to fix incidents as listed below:
  - Identification of incident cause.
  - Analysis, implementation, and test of temporary workarounds (bypass).
  - Analysis, implementation, and test of final corrective solutions.
  - Release in test environment of corrective solutions.
  - Release in production environment of corrective solutions.

  Corrective maintenance does not change design and features of Applications and Databases. Incidental regulatory or evolutionary maintenance tasks due to corrective maintenance will be managed as explained hereinafter.

  Regulatory Maintenance includes updates of applications covered by the service due to legal requirements (including national law and regulations either of the Customer or the Supplier), in accordance with the terms and conditions set out in the Agreement.

  Evolutionary Maintenance includes updates of applications covered by the service, due to changes of Hardware and Software infrastructural components and updates applied to improve quality of applications.

- ***Trade***

  The “Trade” service allows management of following products:
  - Domestic guarantees.
  - International guarantees.
  - Import letters of credit.
  - Export letters of credit.

- Import documentary collection.
- Export documentary collection.

Managing the above-mentioned products means allowing entry of the dossier with possibility of digital signature of request for Inbiz portal and execution of organizational workflow from the relevant portal.

- ***Cash Pooling***

Cash Pooling service allow centralization of management of financial resources of a holding having different companies in different countries.
This service would give the possibility of transferring on a main bank account, all liquidity positions of the other bank accounts present in Supplier subsidiary banks of branches. Two different systems can be used:

- "Zero Balance", for zeroing the accounts and sweep the balances of lead accounts to Nostro accounts at the end of day.
- "Cash Concentration", for transferring account balances.

- ***Host to Host***

Host-to-host connections.
General features of host-to-host connections.

Connection method

The types of connection between the Company and the branch and the codes for accessing and using the Service are found hereunder:

Access procedure	Transmission protocol	Codes for using the Service
Dedicated line (CDN)		*Username + Certificates*
	SFTP (on SSH)	*Username + Public keys (DSA or RSA 1024bit)*
	FTPS (on SSL)	*Username – Password + Certificates*
	HTTPS (or other encrypted protocols)	*Username – Password*
VPN		*Username + Certificates*
	Non-encrypted space	*Username*
	SFTP (on SSH)	*Username + Public keys (DSA or RSA 1024bit)*
	FTPS (on SSL)	*Username – Password + Certificates*
	HTTPS	*Username – Password*
	Non-encrypted Protocols	*Username – Password*
Internet	*SFTP (on SSH)*	*Username + Public keys (DSA or RSA 1024bit)*
	FTPS (on SSL)	*Username – Password*
	HTTPS (or other encrypted protocols)	*Username – Password*

Technical Standards of dataflows

The Electronic Dataflows (hereinafter the "Dataflows") must comply with the following technical standards:

- CBI, available at www.cbi-org.eu.
- Swift, available at www.Swift.com

- Agreed upon between the Customer and the branch on a prior basis.

Availability of the service
The service is made available to the Customer on a continuous basis. The ordinary maintenance is carried out during night-time hours, normally between 12:00 midnight and 3:00 a.m.
At the time of the service activation, the branch provides the Customer with telephone references and electronic mail addresses for assistance, which is offered during office hours (8:25 a.m. to 4:55 p.m., Monday-Friday). Any particular needs must be indicated by the Customer and approved by the branch.

- ***Interactive Cross Platform (IXP)***

  IXP (Interactive Cross Platform) architecture is to provide access to common application services, residing on different technological platforms, to "requesting" applications, removing any need to know their physical location and/or the technology of how they communicate.

  The IXP infrastructure in the Application Server environment provides an execution environment, where requesting application services, or services called by other applications that use the IXP architecture, can reside.

  The solution uses Java classes and is consistent with the J2EE architectural model, and therefore it is open to the various Application Servers that conform to this architecture.

  The IXP architecture is made up of three components:
  - A requesting component, or IXP-Requester.
  - A format conversion support component (ASCII/EBCDIC and vice-versa), IXP-Encoding.
  - A receiving component or IXP-Server.

  The IXP services supported can be divided into synchronous and asynchronous services.

  IXP Use the following layer protocols for exchange asynchronous messages: Websphere MQ and SPAZIO File Transfer

3.1.2 Service Delivery

Target Calendar
All timeframes mentioned in the following chapters are based on the so-called “Target Calendar”.

This calendar is based on European Central Bank decision related to Trans-European Automated Real-time Gross Settlement Express Transfer (TARGET) system.

More information on Target Calendar could be found at the following Internet URL:
http://www.ecb.int/press/pr/date/2000/html/pr001214_4.en.html

Availability timeframes of applications

For all applications covered by the service, with the exceptions of scheduled maintenance, availability will be guaranteed during following timeframes:

SERVICE	TIME FRAME	NOTE
Availability with on-site support	Monday – Friday from 8.25 to 16.55 (CET)	TARGET CALENDAR
Availability without on-site support	All other days and timeframes	No measurement for Service Level purpose

Every Sunday, between 02:00 and 07:00 AM CET, applications will not be available due to ordinary maintenance tasks and databases backup.

During all other timeframe applications should be available even if this could not be guaranteed in advance.

Other maintenance tasks are usually scheduled on Saturday or Sunday, after agreement between Supplier and Customer. Both Parties agree that maintenance tasks will be scheduled taking in proper consideration their severity in relation with Service need.

Notification of maintenance tasks will be done as described in chapter “Communications between parties” at least 5 days in advance.

Corrective Maintenance Tasks

Corrective Maintenance tasks, of course, could not be planned in advance, since they are required when some process is stuck or is not working properly. In these cases, support request will follow standard support process and will be done using standard trouble ticketing system.

In order to solve, even temporarily, the problem, the Supplier could put in place a workaround not necessarily based on IT procedures.

Whenever problem resolution would require operating on data or some support by the Customer, the latter will ensure involvement of needed Customer Corporate functions.

Starting from the notification acknowledgment (see following table), the Supplier will start troubleshooting, identifying the reason of the problem and technical activities to perform in order to remove it, keeping informed the Customer.

At the end of corrective task, Supplier will inform Customer about actions carried out.

Incidents are classified according to severity:

Severity	Description
High	Prevents operations from being executed and has a serious impact on branch customers or on external supervisory bodies.
Low	Slowdown of operations or other problems without serious impact on branch customers or on external supervisory bodies.

Start time of troubleshooting activities by the Supplier are defined in the following table based on severity level and therefore also on urgency of reported problems.

Severity	Notification acknowledgment
High	Within 2 working hours
Low	Within 8 working hours

Supplier's working hours are Monday – Friday from 8:25 to 16:55, with respect to Target Calendar.
The Customer will timely be informed about estimated incident resolution.

Maintenance Interventions due to regulatory requirements
Considering that the interventions due to regulatory requirements do not refer to changes of the basic technical characteristics, the execution and release of such occur in compliance with the time frame set by the Supplier and after the allocation to the Supplier – in accordance with the operative processes of Intesa Sanpaolo Capital Budget Department – of the necessary financial resources for the interventions.

The maintenance requirements having a regulatory nature that refer to the target IT system fall under the competences of the Representative of the Customer.

Without prejudice to Article 4.4. of the Agreement, for the requirements that are not related to the target IT system, or to its customization, the necessary specifications imposed by the new regulatory requirements will be provided by the Customer.

The necessary functional analysis activity related to the maintenance interventions will be normally carried out by the Supplier. for peculiar activities, for which the Customer ’s support is required, the Supplier may ask the Customer ’s support.

In any case, the release of the updates should guarantee the Customer to comply with the deadlines set forth by the new legal provisions in force.

Development and Optimization Maintenance Interventions
The Supplier undertakes to provide the Customer with adequate reports on the progress of the development plans related to the application portfolio with respect to the areas for which the Customer submitted a specific request or which are related to its own business.
The Customer will officially request the Supplier for development and optimization maintenance interventions by means of the Representative of the Customer.
The Supplier will assess the impact of the intervention and its feasibility.
Should the intervention be feasible, the Supplier undertakes to make and deliver to the Customer a technical - economic offer.

The fulfilment of the interventions will be, in any case, subordinated to the allocation to the Supplier – in accordance with the operative processes of Intesa Sanpaolo Capital Budget Department - of the necessary financial resources.

Regulatory Maintenance Tasks

Given that Regulatory Maintenance applies to situations wherein the basic technical characteristics remain unchanged, such maintenance shall be carried out according to schedules established by the Supplier.

However, release of relevant updates, must, in any case, ensure the Customer's compliance with deadlines established by the applicable law or regulation.

Analysis of required changes to the application is performed by the Supplier with support of the Customer when needed and requested.

Evolutionary Maintenance Tasks
The Supplier agrees to provide on a regular basis the Customer with information on the progress of development plans for relevant application systems. Frequency of updates will be defined by Supplier and Customer based on their specific needs.

In case development plans involve Customer development activities, the plan should be agreed with the Customer.

The Customer could request the Supplier to provide minor Evolutionary Maintenance Tasks. These requests will be submitted by the representatives referred to under "Communication between the Parties". The Supplier will evaluate technical feasibility of the task and the relevant effort needed.

In case such intervention will be feasible, the Supplier will prepare a technical-financial proposal to be given to the Customer as soon as possible, based on request complexity.

Supplier liabilities and obligations
The services provided by the Supplier under the Agreement are mainly operated from Italy.
The Supplier will ensure:

- Respect of agreed service levels.
- Regular measurement of agreed KPIs.
- Periodic information to Customer regarding future projects affecting provisioning of Service.

Customer liabilities and obligations
The Customer will:

- Give prompt notification to the Supplier about problem affecting Service using provided Trouble Ticketing System.
- Verify that all users are properly trained and able to use all the types of documentation available in support of ordinary operations.
- Give prompt notification to the Supplier about law or regulation changes affecting Service.

3.1.3 Availability of the service - KPI

The Supplier shall ensure:

- efficiency and quality of provided Services.
- flexibility to safeguard the mutual interest of the Parties.
- reliability and security of provided Services.

The Supplier has an organizational unit, independent from service delivery units, with the goal of monitoring quality and operations, using technological tools (system logs, application logs and monitoring tools) to ensure the adequacy and accuracy of measurements.

Measurement of Service Level is based on KPI associated to different products and referring to following criteria:

- Av = Service Availability
- Ad = Service Adequacy of the service in terms of absence of errors in relation to the specifications

Due to the nature of provided services and their characteristics, each criterion (Availability and Adequacy) may contribute differently to the definition of the quality of Services and therefore they can get a different score that represents the corrective element which, applied to the measure, will give, as a result, a more realistic collocation of the analysed component in the overall service.

Service Level reports are usually produced on a monthly basis, containing information about previous month and made available to the Customer in electronic format and, if required, on paper.

In the following tables are listed provided service levels. Tables include Product Code, KPI, measurement methodology, kind, Target (expected value) and Tolerance (Maximum percentage difference from target value not affecting Service Level). The latter two won't be defined until the end of KPI Stabilization period (see below).

Calculation of Service Level won't consider all those problems or disruptions whose causes have been identified in technological infrastructures or applications under Customer responsibility.

KPI	Measurement Metrics	SLA	Tolerance	Indicator
Inbiz - Availability	Actual availability of Transactional System/Agreed Availability * 100%	97	2	Av
Inbiz - taking charge of problem solving	Average time to take charge of tickets with a maximum threshold of 2 hours	95	-	Ad

Average ticket processing time: for high priority tickets, maximum 12 hours; for normal priority, maximum 54 hours. For critical/emergency issues, resolution is expected within 2 hours.

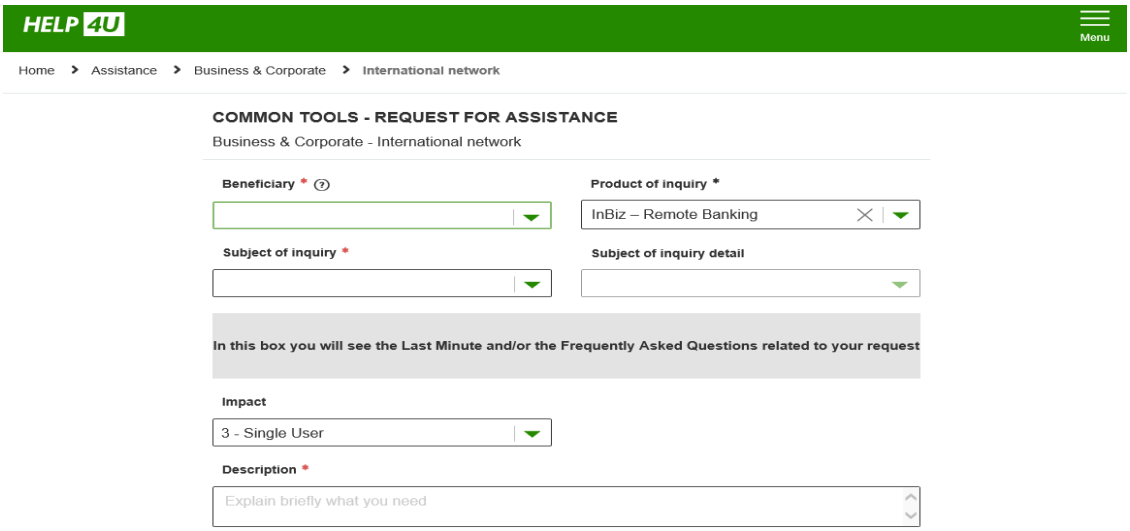
KPI Stabilization

In order to better define thresholds and to fine tune monitoring and reporting systems, it is agreed that within an initial grace period of 6 months, KPI will be measured, and report will be delivered but with no effect on Service Level. At the end of this period, based upon the experience, KPI set and relevant thresholds will be defined. Grace period will be specific for each service: therefore 6 months period will start when each service goes live.

Vulnerability Assessment test

GTS provides a service of network security level evaluation, to undertake the relevant vulnerability assessment activities and define and manage the action plans according to assessment results. For the critical applications supporting foreign branches has been defined a yearly VA/PT plan. On the Inbiz solution a yearly Web Application Penetration Test (WAPT) will be also executed to verify possible vulnerabilities and consequent risk mitigation activities.

To open a ticket, the User's Branch should open a ticket using the standard ISP portal "Help4U" - Service Now.



3.1.4 Service Management

Critical Issue Management

Management of anomalies

Goal of management of anomalies is to analyze, formalize and fix all issues related to a non-compliance of delivery process that could potentially affect service levels. Two distinct areas could be identified:

- Management of anomalies related to service requests.
- Management of anomalies related to provided services.

The problems that are encountered by the Supplier when providing the Services will therefore be handled according to the procedures described below.

Management of anomalies related to service requests

If Customer detects a supposed case of non-compliance of service request management processes, such in case service delayed or not provided at all, complains must be sent to the Supplier's unit that received the original request.

In case of repeated and systematic non-compliance in on-demand service delivery processes, Customer Delegate may call upon Supplier Delegate.

Management of anomalies related to provided services

This process defines the interfaces to involve and the escalation paths to be followed according to problem severity.

Problem is classified by the Supplier detecting it (directly or on Customer's input) in order to properly define its level of severity and therefore which person or team to involve to properly manage it.
In any case the Supplier Delegate will promptly report the problem detected to the Customer Delegate.
Since the actual impact can only be measured afterwards, in the early phase only the estimated impact would be considered.
On the base of problem severity level, different parties could be involved with different approaches, following the well-known escalation process.

Meetings

Recurring meetings on service level

Meetings are called by the Supplier with the purpose of evaluating Customer satisfaction on provided services.

Special focus is made on:

- Check of service level guaranteed in the last period of time.
- Actions for increasing Service Level.
- Financial questions related to provided services.

This kind of meeting is made usually every six months, except in case Supplier and Customer agree on different scheduling.

Following persons attend at the meeting:

- Supplier delegate as owner of relationship with Customer.
- Customer delegate.
- Other persons useful to face arguments in agenda.

Two days before the meeting, Supplier delegate will send following documents:

- Meeting agenda including document related to arguments to cover.
- Previous meeting minutes.

After the meeting, Supplier delegate will:

- Write meeting minutes including list of attending persons, examined arguments, meeting decisions.
- Send a draft of the above minutes to all attendants.
- Wait 5 days to receive comments from the attendants,
- Send the agreed final version of the minutes to meet attendants.

Meetings on Customer Request

At Customer requested meetings will attend:

- Supplier delegate.
- Customer delegate.
- Other persons useful to face arguments in agenda.

This kind of meeting is could not be called more than three times per year, except in case Supplier agree on different frequency due to specific critical issues or due to some specific running project.

Changes to the provided service

New services activation or essential modification to the existing ones could be originated from extraordinary requests and with following consequences:

- Definition of new products/services provided to the Customer.
- Substantial modification of provided services.

In these circumstances, it is necessary to activate the Provided Service Change Process in order to manage and formalize to the Customer an agreement modification proposal. The validity of proposed modification will be effective only after approval from both parties.

Change Management scope

Provided Service Change Process can be activated:

- after Customer delegate request.
- after Supplier delegate request.

3.2 AML Safewatch (BSA)

3.2.1 Content of the service (SafeWatch)

The AML support service is intended to cover the maintenance and support application services related to:

- Eastnets Safewatch Profiling
- Eastnets Safewatch Filtering and its interfaces
- Service provision of IBM's Atlas license and Worldcheck for ISP Foreign Network.

The in-scope applications and the in-scope Companies and Branches are represented in the table hereafter:

	Frankfurt	Hong-Kong	Istanbul	London	Madrid	NY	Paris	Shanghai	Singapore	Tokyo	Warsaw	Abu Dhabi	Banca IMI London	Sydney	Dubai
SafeWatch Filtering (Foreign Branches)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SafeWatch Profiling (Foreign Branches)	x	x	x	x	x		x	x	x	x	x	x			x
FM Support	x	x	x	x	x	x	x	x	x	x	x	x	x		x
IBM Atlas WorldCheck	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

The total number of concurrent users for Safewatch Filtering within this perimeter is 50 users at the time of the offer. They are not linked to specific BICs and must be considered overall.
The other applications present in this offer (Safewatch Profiling, Box Reporting) are limited to 70 users each.

3.2.2 Service Coverage

Support service's single point of contact is provided by GTS throw Intesa Sanpaolo Servitia's Help Desk as follows:
- Monday to Friday

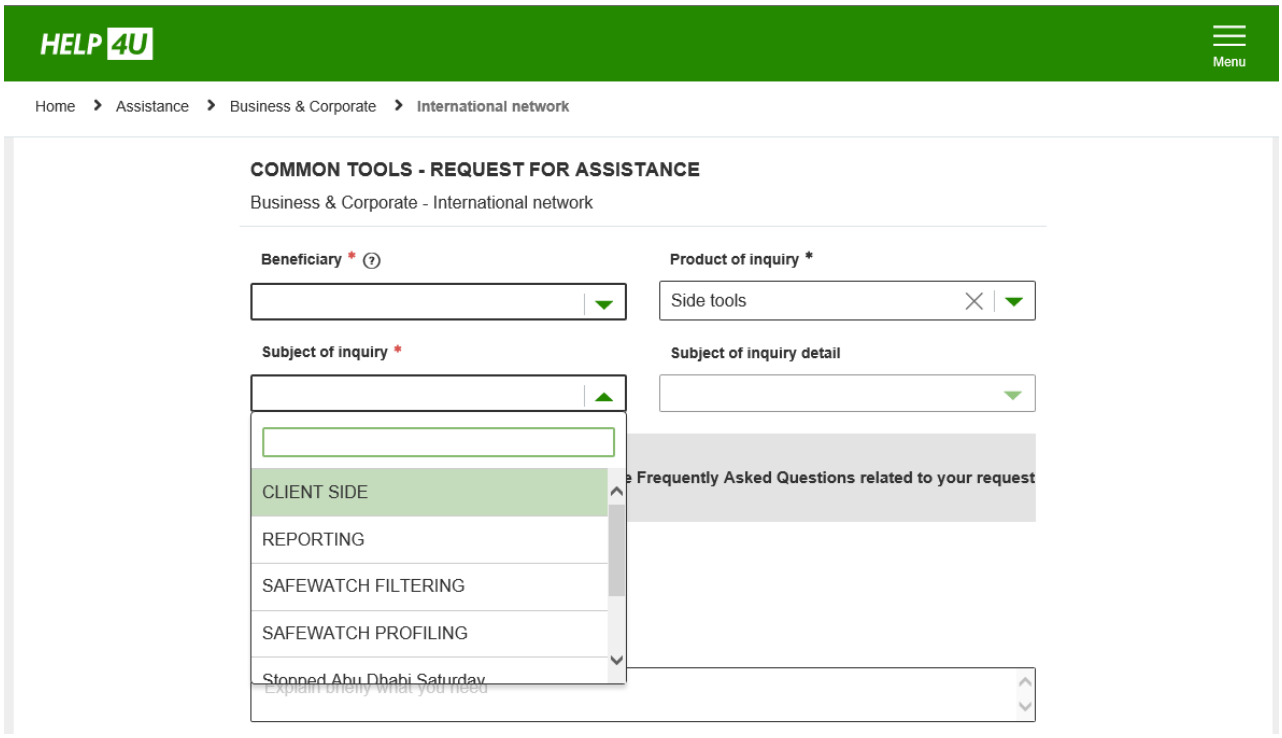
- 8.00h to 18.00h (GMT + 1)
- Saturday on call for Abu Dhabi regarding blocking issues (only for Filtering)

Outside this coverage period, Intesa SANPAOLO GTS by Intesa Sanpaolo Servitia will provide best effort service but not covered by KPI.

Assistance on network and hardware problems within the scope of the service – as these infrastructures

Support service's single point of contact is provided by GTS Help Desk (Infrastructural & Distributed Systems Dept). The Foreign Branch staff must immediately communicate any kind of problem or malfunctioning that occurred to a Regulatory Reports process or service. the service is available 24/24 hours and 7 days per week.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Common Tools – Request for Assistance – SafeWatch".



3.2.3 Availability of the service - KPI

GTS Help Desk shall provide first-line support and take care of internal escalation of tickets towards other departments/providers ensuring correct routing of calls upward second level support.

It is agreed that GTS Help Desk will act – according to the guidelines set out in this document - as single entry-point for the purposes herein described.

Errors, problems, and requests shall be reported to Help Desk as follows:

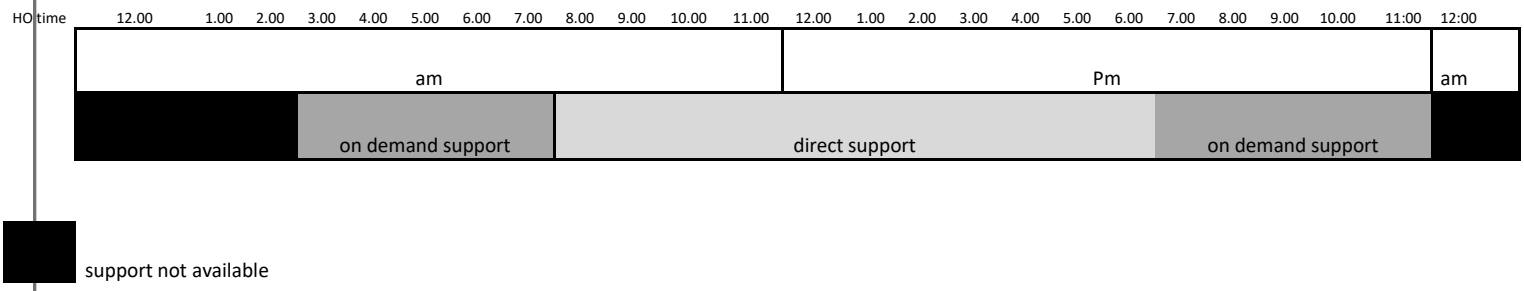
- by using the specifically designed web tool (Service Now). the Help Desk Group must dispatch it within the following 15 minutes to the relevant Maintenance Team,

confirming the execution to the Foreign Branch as soon as the Problem Determination Task has been terminated.

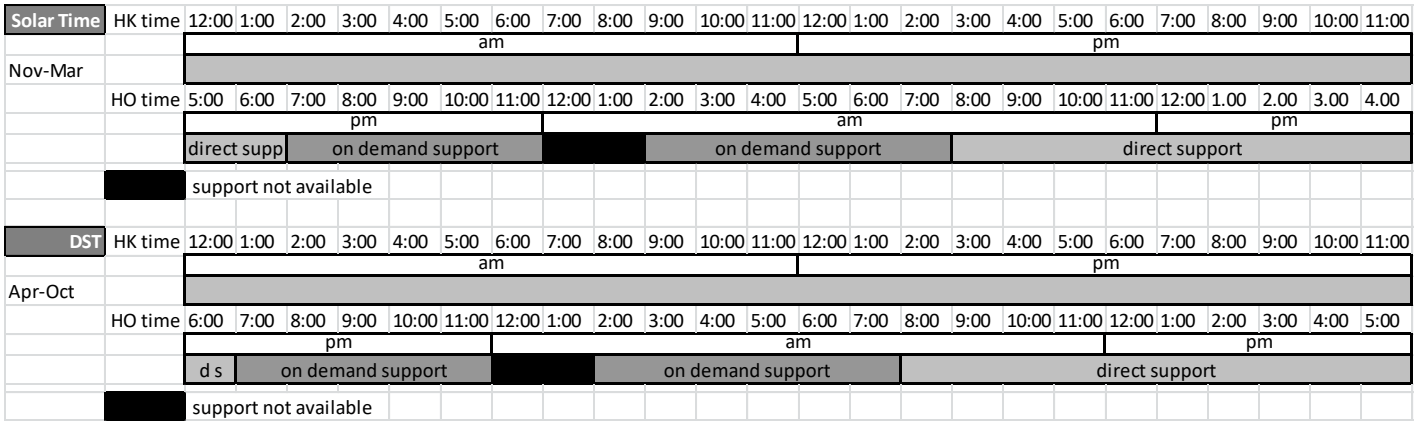
Alternatively, the Help Desk Group ServiceDesk Finanza can be reached via phone. ServiceDesk Finanza, who operate under a 24*5 service window, if necessary, will address to the appropriate 3rd level support.

Team Phone Service Desk Finanza +39 02 72612999
Email ServiceDesk.Finanza.gso@intesasanpaolo.com

Below a table with the different type of contact of the AM HO support, based on the project phase:



Taking as example the HK Branch:



On request, the Help Desk Group will keep the Foreign Branch staff updated about progresses on reported problems.
For non-critical problems, errors or questions the Help Desk Group may postpone the intervention of the relevant Maintenance Team till the day-after (from 08:30 a.m. to 04:45 p.m. CET)

The Supplier will create new KPI in according with business priorities.

3.2.4 Service Management

The service assistance generally covers defects and faults in the software and its interfaces' input / output data files, as well as troubleshooting when needed.
It shall provide new users' profile activation when requested.

It is understood that the Help Desk Group shall also ensure correct routing to tickets whose ongoing analysis should reveal an issue concerning network or hardware as to guarantee a seamless chain of support within the Group.

GTS support service as described will remedy any programming error attributable to its or vendors' development that is reported, by suitable corrective action or workaround.
It shall give proper evidence of known fix/action times and procedures.

This support agreement does not obligate GTS to provide maintenance or support services required because of personal or not authorized modifications – where applicable - to any computer program incorporating or carrying all or any part of the applications and modules described in the agreement.

The recipient shall comply with the vendor's limitations and terms of products' usage. The provider shall not be liable for any user's breach of these terms and limitations.

Response time:
Response time for all reported problems and errors within service's time and calendar is 2 hours.
New user ID requests are excluded, as well as parameterizations and ad hoc searches.

Help Desk - Response Time		
Min Response Time	**Max Response Time**	**Target**
1 h	2 h	>= 95%

Solution time:
When the error, bug or problem depends on a faulted component, source code or other element provided by the vendors and it is fixable by the vendor only via a development change of the code, a workaround, or by replacing the faulted component, the solution will be provided under the best effort delivery method.

As for vendors whose KPIs are not specified in the present document, the solution time is managed as best effort according to GTS "GICT" priority attribution and depending on provider's specific conditions and availability.
For errors or problems deriving directly from components or modules managed by Intesa Sanpaolo Servitia unless it is by any means subject to limitations imposed by any third party (vendor or Company), the corrective action - either by replacing, correcting the fault component/code, providing specific workaround and/or other service - shall be provided for blocking issues within 15 working hours at the latest starting from Service Now by IS Servitia, with the exception of Cadet+, for which the solution time (fix/workaround) is 8 working hours.
For avoidance of doubt blocking issues apply only when customer activity is blocked and tickets priority remains unchanged as managed by GICT.
For avoidance of doubts, as applicable ticketing system upon Client request is not the one of ISS but provided by the Client itself, relevant management and monitoring (especially at KPI level metrics) is subject to the availability of relevant granular functionalities allowing to measure metrics pertinent to ISS specifically excluding metrics accumulation deriving from any other party.

Deployment on Italian FARM is subject to ISP deployment change rules and scheduling. Intesa Sanpaolo Servitia does not respond for any fault, delay or other problems that may occur on the part of the interface related to the mainframe environment since it does not act as referent on the mentioned environment.

When the error or problem concerns directly a component or module or part managed by GTS, and it is not by any means subject to limitations imposed by any third party (vendor or Company), the corrective action - either by replacing or correcting the fault component/code, or providing specific workaround and/or other service - shall be provided under a solution time of 4 working days at the latest, starting from Service Now by the Help Desk Group. The creation of new user IDs can be requested via Service Now.

	Help Desk - Solution Time KPIs (subject to limitations and clauses described above)		
	Min Solution Time	**Max Solution Time**	**Target**
Ticket Priority: High (Blocking Issues)	10 h	15 h	>= 95%
Ticket Priority: Low	45 h	70 h	>= 95%

3.3 AML NetReveal Transaction Monitoring

3.3.1 Content of the service (NetReveal)

The AML NetReveal support service is intended to cover the maintenance and support application services related to:

- NetReveal® AML
- NetReveal® AML Correspondent Banking

The in-scope Branches are:

1. London
2. Sydney
3. Frankfurt
4. Madrid
5. Paris
6. Warsaw
7. Hong Kong
8. Shanghai
9. Singapore
10. Tokyo
11. Dubai
12. Abu Dhabi

3.3.2 Service Coverage

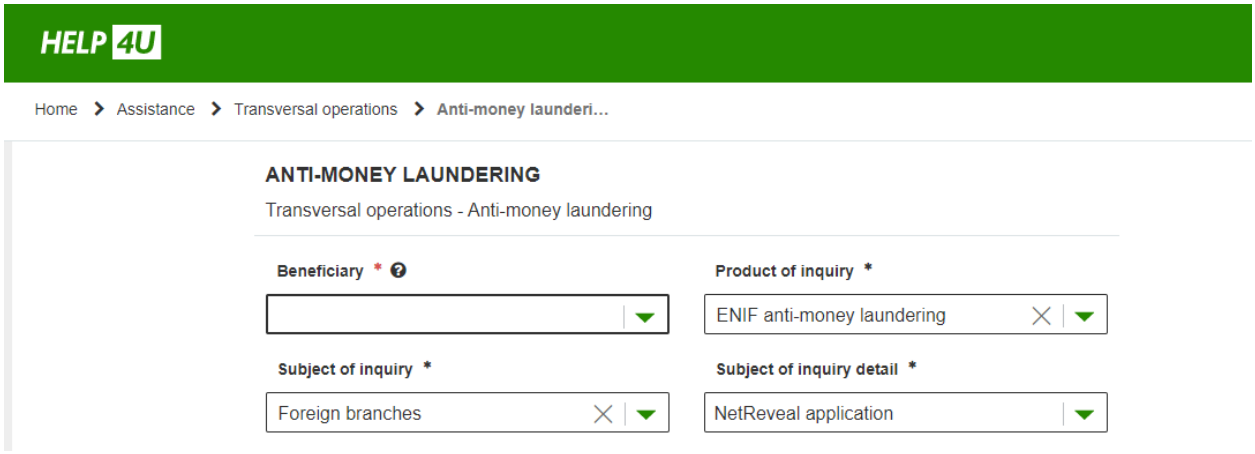
Support service's single point of contact is provided by GTS through Help Desk as follows:
- Monday to Friday
- 08:30 a.m. to 04:45 p.m. CET

Outside this coverage period, Intesa SANPAOLO GTS will provide best effort service but not covered by KPI.

Assistance on network and hardware problems within the scope of the service – as these infrastructures

Support service's single point of contact is provided by GTS Help Desk (Infrastructural & Distributed Systems Dept).

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Assistance – Transversal operations – Anti Money Laundering - ENIF_Anti_Money_Laundering – Foreign branches – NetReveal application".



3.3.3 Availability of the service - KPI

GTS Help Desk shall provide first-line support and take care of internal escalation of tickets towards other departments/providers ensuring correct routing of calls upward second level support.

It is agreed that GTS Help Desk will act – according to the guidelines set out in this document - as single entry-point for the purposes herein described.

Errors, problems, and requests shall be reported to Help Desk as follows:

- by using the specifically designed web tool (Service Now). the Help Desk Group must dispatch it within the following 15 minutes to the relevant Maintenance Team, confirming the execution to the Foreign Branch as soon as the Problem Determination Task has been terminated.

Alternatively, the Help Desk Group Servicedesk Finanza can be reached via phone. Servicedesk Finanza, who operate under a 24*5 service window, if necessary, will address to the appropriate 3rd level support.

Team Phone Service Desk Finanza +39 02 72612999
Email ServiceDesk.Finanza.gso@intesasanpaolo.com

On request, the Help Desk Group will keep the Foreign Branch staff updated about progresses on reported problems.

For non-critical problems, errors or questions the Help Desk Group may postpone the intervention of the relevant Maintenance Team till the day-after (from 08:30 a.m. to 04:45 p.m. CET)
The Supplier will create new KPI in according with business priorities.

3.3.4 Service Management

The service assistance generally covers defects and faults in the software and its interfaces' input / output data files, as well as troubleshooting when needed.
It doesn't provide new users' profile activation.

It is understood that the Help Desk Group shall also ensure correct routing to tickets whose ongoing analysis should reveal an issue concerning network or hardware as to guarantee a seamless chain of support within the Group.

GTS support service as described will remedy any programming error attributable to its or vendors' development that is reported, by suitable corrective action or workaround.
It shall give proper evidence of known fix/action times and procedures.

This support agreement does not obligate GTS to provide maintenance or support services required as a result of personal or not authorized modifications – where applicable - to any computer program incorporating or carrying all or any part of the applications and modules described in the agreement.

The recipient shall comply with the vendor's limitations and terms of products' usage. The provider shall not be liable for any user's breach of these terms and limitations.

Response time:
Response time for all reported problems and errors within service's time and calendar is 2 hours.
New user ID requests are excluded, as well as parameterizations and ad hoc searches.

Help Desk - Response Time		
Min Response Time	**Max Response Time**	**Target**
1 h	2 h	>= 95%

Solution time:
When the error, bug or problem depends on a faulted component, source code or other element provided by the vendors and it is fixable by the vendor only via a development change of the code, a workaround, or by replacing the faulted component, the solution will be provided under the best effort delivery method.

As for vendors whose KPIs are not specified in the present document, the solution time is managed as best effort according to GTS "GICT" priority attribution and depending on provider's specific conditions and availability.

	Help Desk - Solution Time KPIs (subject to limitations and clauses described above)		
	Min Solution Time	Max Solution Time	Target
Ticket Priority: High (Blocking Issues)	8 h	12 h	>= 95%
Ticket Priority: Low	36 h	54 h	>= 95%

3.4 Centralized Elaboration of Regulatory Reports

3.4.1 Local Reporting

This document paragraph defines the service level and delivery, alongside the procedures and methods of support, in terms of both SW & HW infrastructures, provided by GTS, to produce regulatory reports as requested by Local Regulators. Duration of the agreement is yearly based.

The following specific solutions are in scope as of August 31st, 2017 for:

Branch	**Software Package/Supplier**
Madrid	Otesi/Otesi
Paris	OneSumx/Wolters Kluwer Financial Services & Sopra, Cogeprint
Frankfurt	Abacus DaVinci/BearingPoint
Warsaw	GPM/aSist, ION, Ognivo
Hong Kong	OneSumx/Wolters Kluwer Financial Services
Singapore	Reporter/Lombard Risk (Vermeg)

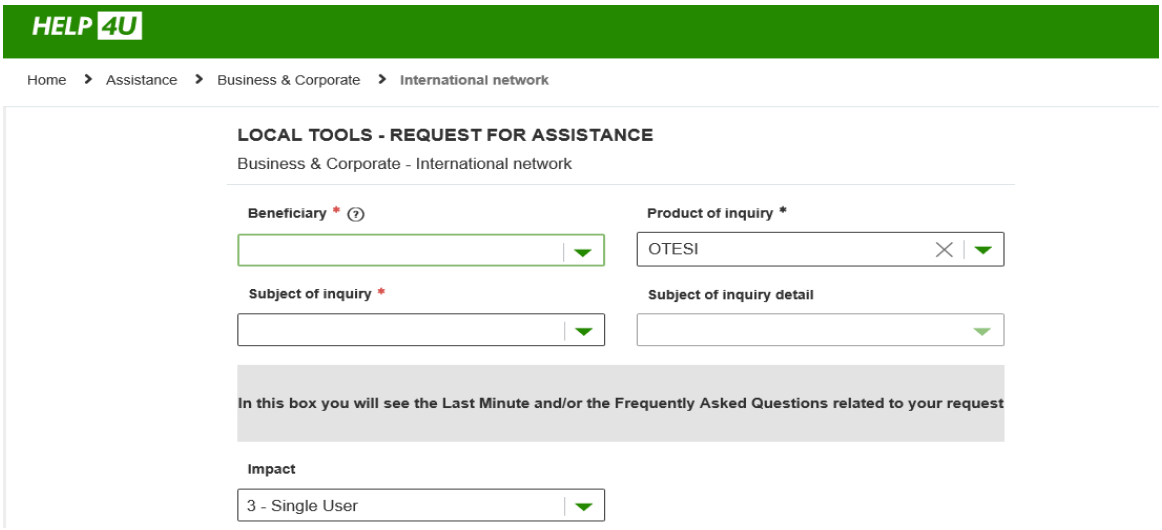
3.4.2 Service Coverage

Support service's single point of contact is provided by GTS throw Intesa Sanpaolo Servitia's Help Desk as follows:
- Monday to Friday
- 8.00h to 18.00h (GMT + 1)
- Saturday on call for Abu Dhabi regarding blocking issues (only for Filtering)

Outside this coverage period, Intesa SANPAOLO GTS by Intesa Sanpaolo Servitia will provide best effort service but not covered by KPI.

Assistance on network and hardware problems within the scope of the service – as these infrastructures

Support service's single point of contact is provided by GTS Help Desk (Infrastructural & Distributed Systems Dept). The Foreign Branch staff must immediately communicate any kind of problem or malfunctioning that occurred to a Regulatory Reports process or service. the service is available 24/24 hours and 7 days per week.
To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Local Tools – Request for Assistance – OTESI".



3.4.3 Availability of the service - KPI

GTS Help Desk shall provide first-line support and take care of internal escalation of tickets towards other departments/providers ensuring correct routing of calls upward second level support.

It is agreed that GTS Help Desk will act – according to the guidelines set out in this document - as single entry-point for the purposes herein described.

Errors, problems, and requests shall be reported to Help Desk as follows:

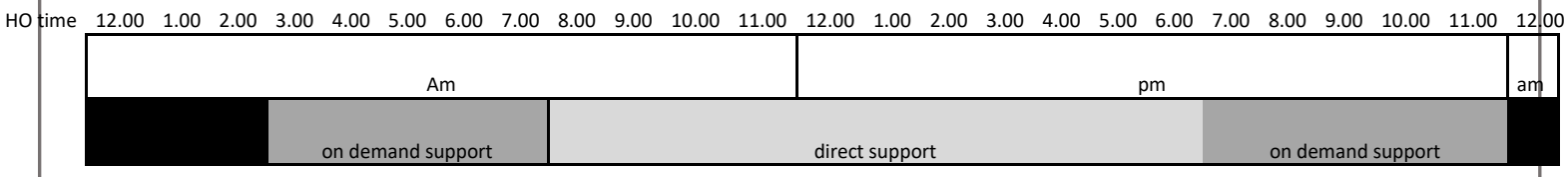
- by using the specifically designed web tool (Service Now). the Help Desk Group must dispatch it within the following 15 minutes to the relevant Maintenance Team, confirming the execution to the Foreign Branch as soon as the Problem Determination Task has been terminated.

Alternatively, the Help Desk Group Servicedesk Finanza can be reached via phone.

Servicedesk Finanza, who operate under a 24*5 service window, if necessary, will address to the appropriate 3rd level support.

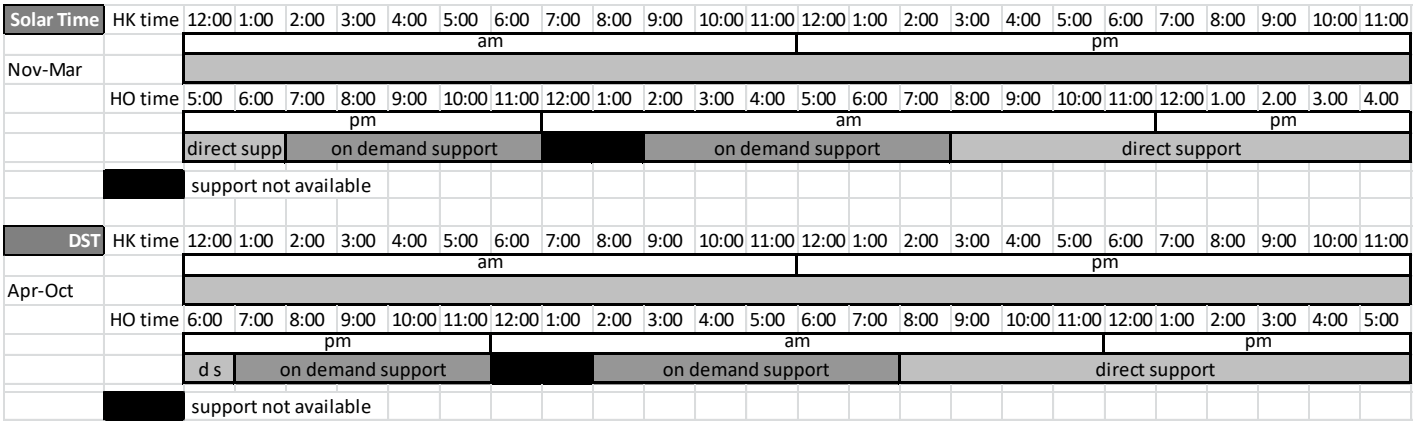
Team Phone Service Desk Finanza +39 02 72612999
Email ServiceDesk.Finanza.gso@intesasanpaolo.com

Below a table with the different type of contact of the AM HO support, based on the project phase:



support not available

Taking as example the HK Branch:



On request, the Help Desk Group will keep the Foreign Branch staff updated about progresses on reported problems.
For non-critical problems, errors or questions the Help Desk Group may postpone the intervention of the relevant Maintenance Team till the day-after (from 08:30 a.m. to 04:45 p.m. CET)

The Supplier will create new KPI in according with business priorities.

3.5 GIANOS 3D

3.5.1 Content of the service

GIANOS is managing topics and evolutionary regarding: New Appropriate Verification and Management of Group Risk Profiles

GIANOS's PROGRAMS

- Anomaly Generator for Suspicious Operations, called GIANOS® © Banks.
- Recycling Risk Profile Generator, named: GIANOS® © Banks - GPR.
- Compliance Management Third EU Directive, named: GIANOS® © - 3D.
- Internal Controls, named: GIANOS® © - Internal Controls CI
  The

The program operates in two ways. Through the first one it determines the recycling risk profile for all customers who, in the last 12 months compared to the moment of processing, have been entered in the Unique Informatic Archive (established as a company pursuant to Law 197/1991), with at least one registration accounting. in addition, with the second method by processing the data contained in a further special archive, defined as "Complementary", also generates profiles for customers that in the last 12 months have not carried out operation recorded in the AU.

GIANOS® GPR **to determine the customer's risk profile**, uses defined decision tables and updated by an interbank group (ABI-ARMA Committee) to which the user can add them manually changes and the customization of certain criteria and scores.
The diagnostic capacity of the algorithms is high. In fact, the GIANOS® program for the generation of anomaly indices for suspicious transactions, uses algorithms for the analysis of 37 economic behaviors of giving and having, therefore of 74 rules for the historicizing of data e the generation of unexpected extracts from 374 behavioral conditions. The new program

GIANOS® GPR - **for the Generation of Recycling Risk Profiles** - uses both the aforementioned combined, both additional 6 primary conditions, divided into 78 classifications and 7 variables of correction. The result is the attribution of a first recycling risk score to each customer based on the operations performed and the means used. This score, through 9 variables, 25 classifications and 32 refinement conditions are translated into 4 risk bands within of which the examined customers are included. The scores obtained are then further refined through the information obtained with the data that feed the c.d. Complementary Archive.

In summary, the GIANOS® GPR program interacts with the program that generates anomaly indices and allows you to:

- Observe the recycling risk profile referred to a specific month.
- Monitor the evolution of the risk profile over time.
- Insert a normal or reinforced audit.
- See the list of entered checks.
- Produce the list of profiles, and for each of them access to editing functions or display.
- Check the parameters used for profiling.
- Customize the risk parameters of each subject, modifying:
  1. the intervals of the scores assigned to each band.
  2. the scores associated with the specified value of each data.
  3. the scores associated with the defined conditions.

Furthermore, the program is equipped with a module for the checks dedicated to data management characterize the recycling risk profiling and, using usable maps a video, allows you to treat:

- the list of subjects with a risk profile.
- inclusion of the risk profile.
- the verification entry.
- the detailed data of the profiled subject.
- the list of the checks entered.

More in particular:

- the list of subjects with a risk profile allows, based on the selection parameters set by the user, to see the data of the profiled subjects and to export the data in a stream standard.
- the inclusion of the risk profile, allows to manually enter the score of the risk profile of a customer, in case the risk profile has not been processed by the procedure.
- the verification entry, allows to update manually the score that determines the customer recycling risk profile.
- the detailed data of the profiled subject, allow to see the detailed information on the profiled subject.
- the list of the checks entered, allows you to see all the checks entered for the subject under exam.

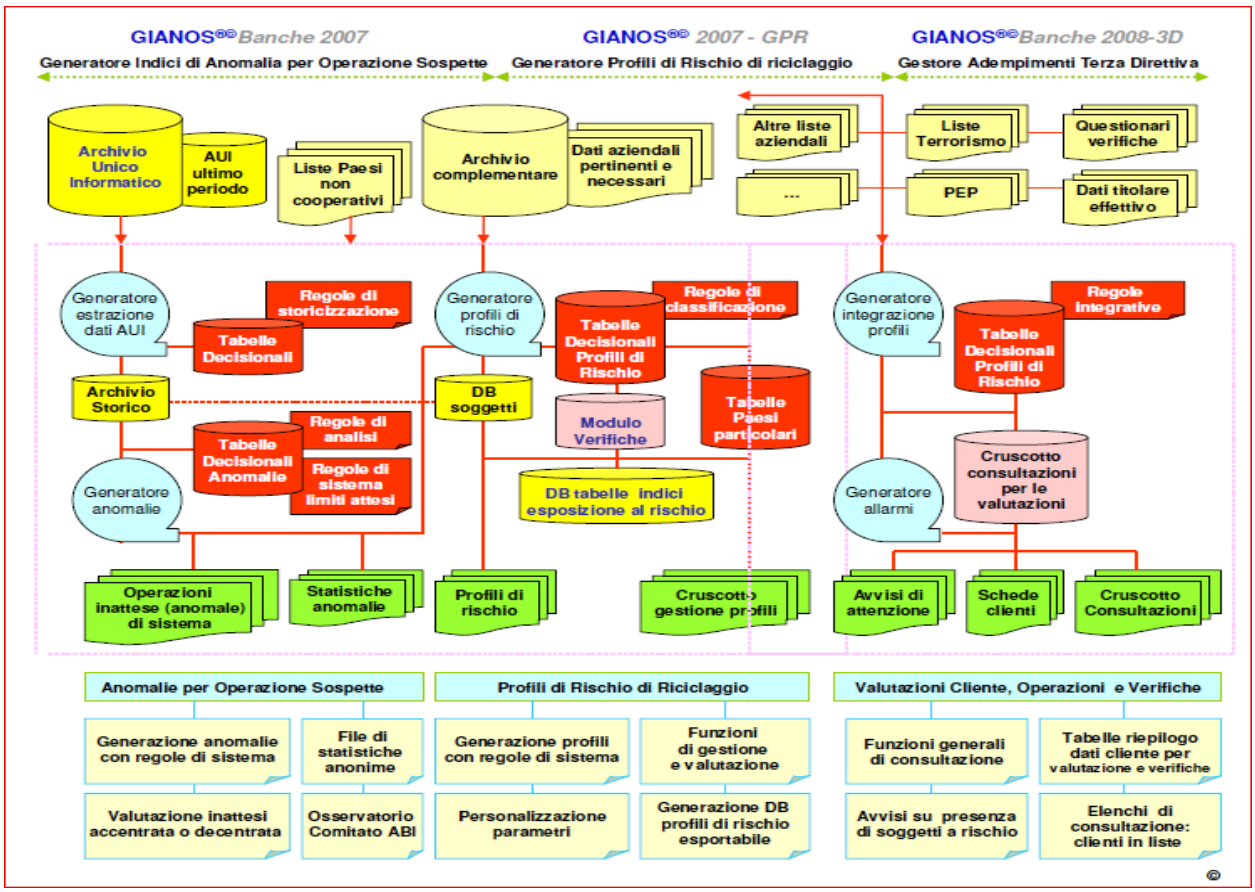
The implementation of the third GIANOS® program - called GIANOS® 3D follows the approval of the legislative decree 21 November 2007, n. 231 on prevention of the use of the financial system for laundering the proceeds of crime and financing of terrorism [which transposes the III directive on the subject.

The application is therefore accompanied by a dashboard for consulting and evaluating customers and from the generation of tables and utility graphs.
Furthermore, in consideration of the terms of entry into force of the Legislative Decree 231/2007, a specification component of the computer program was dedicated to KYC (Know Your Customer). It can be used to collect useful, relevant and necessary information carrying out of the most urgent new obligations.

The KYC component of GIANOS® 3D ensures the following macro functions:

- the management and compilation of a questionnaire in electronic format.
- the management of external and internal lists.
- calculation, scoring, and risk profile using GIANOSÂ® GPR.
- production and consultation of the customer's electronic cards.

The logical scheme of the set of the programs, archives and functions integrated together, which together they constitute a single application (called GIANOS 3D), it is the following:



3.5.2 Service Management

The Gravity Codes

In each case, a severity code is associated with failure and enhancement request. The severity code indicates what kind of problem the customer has.

Severity Level 1: the problem encountered will determine the inactivity of a critical business function. The Software will not be usable by Users in relation to any type of service operations. The typical gravity level 1 problems are: failure to operate an essential function. suspensions or interruptions of critical programs. critical applications out of order. significant logical problems.

data corruption. inability to use data from outgoing processes. lack of essential components. incorrect population of variable data in output systems. mask / dialogue suspensions. serious interface problems.

Severity Level 2: the problem encountered will determine the substantial deterioration of the company functions. The function will need to operate in a degraded state with a strong dependence on temporary solutions. The typical gravity level 2 problems are: severely limited essential functions. individual functional areas out of use, severe service degradation, serious limitations to essential up-stream or down-stream processes.

Severity Level 3: the problem encountered has a weak impact on the service. A non-critical problem with the Software in which the Users can continue to use the application or a temporary solution available. In any case, a prolonged exposure to the search for temporary solutions will affect the service. The typical gravity level 3 problems consist of: incomplete list of values, lack or error of labels, lack of concordance checks, typing errors.

Initial response times (taking charge of the problem) - (GMT + 1)

- Severity 1: 2 (two) hours (office hours)
- Severity 2: 4 (four) hours (office hours)
- Severity 3: 8 (eight) hours (office hours)

Description:

- **Severity Level 1**: the problem encountered will determine the inactivity of a critical business function. The Software will not be usable by Users in relation to any type of service operations. The typical gravity level 1 problems are: failure to operate an essential function. suspensions or interruptions of critical programs. critical applications out of order. significant logical problems. data corruption. inability to use data from outgoing processes. lack of essential components. incorrect population of variable data in output systems. mask / dialogue suspensions. serious interface problems.
- **Severity Level 2**: the problem encountered will determine the substantial deterioration of the company functions. The function will need to operate in a degraded state with a strong dependence on temporary solutions. The typical gravity level 2 problems are: severely limited essential functions. individual functional areas out of use, severe service degradation, serious limitations to essential up-stream or down-stream processes.
- **Severity Level 3**: the problem encountered has a weak impact on the service. A non-critical problem with the Software in which the Users can continue to use the application or a temporary solution available. In any case, a prolonged exposure to the search for temporary solutions will affect the service. The typical gravity level 3 problems consist of: incomplete list of values, lack or error of labels, lack of concordance checks, typing errors.

Resolution times

Resolution time means the time that elapses from the receipt by GTS of the information necessary to identify the problem at the time of the final answer: whatever it may be, even as an alternative remedy.

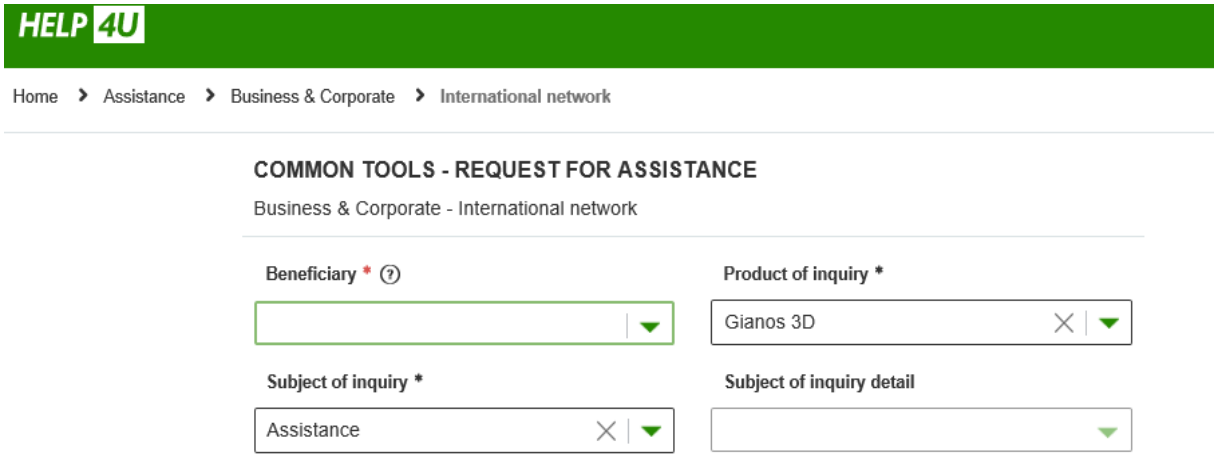
If the problem posed is due to a software defect, the resolution time represents the time elapsed so that an action plan and / or one or more solution procedures, if necessary, are released and delivered to the Customer. The Customer's time required to bring the software

corrections released by GTS to the production environment is excluded.
To ensure customers a quality service, it is customary for "GTS" to manage and resolve cases in a timely manner. Below are the resolution times based on the severity of the case.

Gravity - Total Resolution time
Severity 1 within 8 (eight) hours of receiving the information requested from the Customer to identify the problem, with software correction or indication of bypass intervention

Severity 2 within 24 (twenty-four) hours from receipt of the information requested from the Customer to identify the problem, with correction of the software or indication of bypass intervention where possible or with communication to the Customer of the time and of the resolution of the problem that will be implemented in the as soon as possible.
Severity 3 within 48 (forty-eight) hours from the receipt of the information requested from the Customer to identify the problem, the time and the methods for resolving the problem are communicated to the Customer.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Common Tools – Request for Assistance –Gianos3D".



3.6 FC-HUB

3.6.1 Content of the service

"GTS" provides Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized of regulatory reporting system (FC-HUB) management supplied in conformity with Head Office standard.

3.6.2 Connection to the Application

The access to the FC-HUB Application is done using the intranet ISP with below link. You need the enabling codes assigned by HELP4 and approved by own head office.

PRODUCTION ENV:
http://fcdh0wscf1000rp.sede.corp.sanpaoloimi.com/fchub/desktop/public/home.jsp

SYSTEM-TEST ENV:
http://fcdh0wscf1000rc.syssede.systest.sanpaoloimi.com/fchub/desktop/public/home.jsp

The system architectures are supported by 2 technology Farms/Campus:

- Torino – Moncalieri
- Torino – Settimo Torinese

3.6.3 Availability of the service

There are two levels of support:

- The First Support Level is in "SERVICEDESK.FINANZA.GSO" Support for "centralized Finanza GTS"
- "SERVICEDESK.FINANZA.GSO" will arrange and open the INCIDENT on HELP4 to FC-HUB Support (second level - Application Support)
- FC-HUB Support is organized to support for different regulation.
- "SERVICEDESK.FINANZA.GSO" is in charge of routing INCIDENT remedy to the correct FC-HUB support group, based on the problem/request.

To OPEN an INCIDENT, the User's Branch should

- Use the HELP4U Form
- Contact "SERVICEDESK.FINANZA.GSO" by e-mail:
  - In the email to SERVICEDESK it's always necessary to insert in TO, the **mailbox of the reference AM** & the **mailbox serviceDesk.Finanza.gso@intesasanpaolo.com.**
- Without opening an incident, you may not receive feedback.

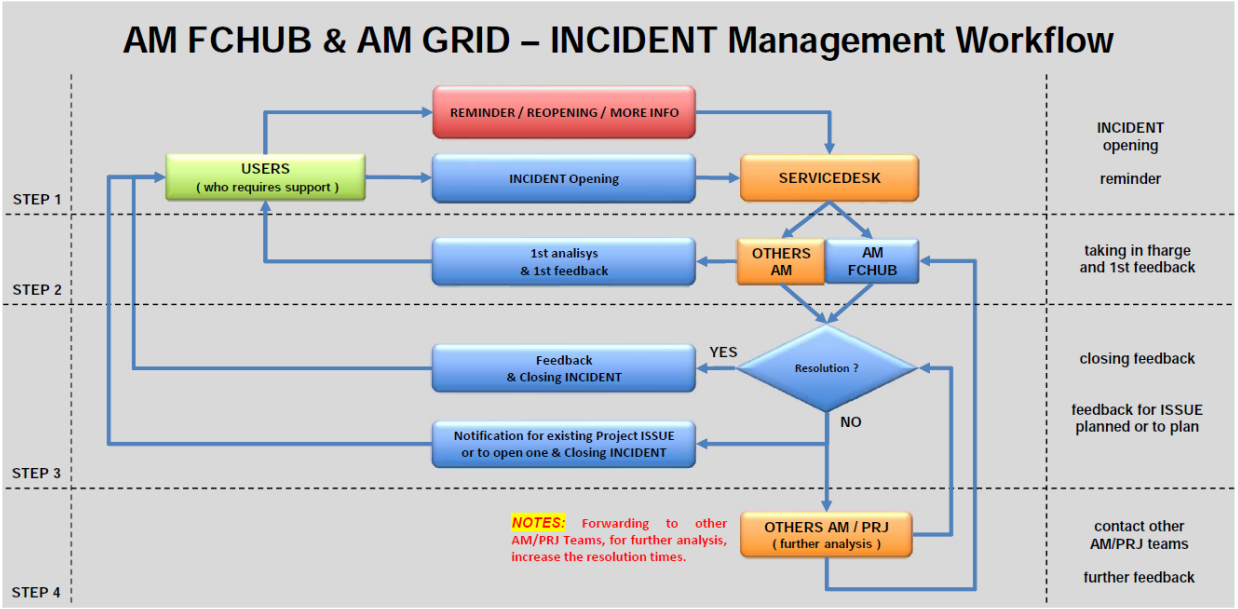
User's Branch does not have to contact directly AM Team to open an INCIDENT.

OPENING TIME: Monday to Friday from 07:30 AM to 07:30 PM (Italian Time)
CONTACT CENTER - AM FC-HUB: +39-0272658991
SERVICENOW (HELP4U) GROUPS: AM_FCHUB

MAILBOX CONTACTS:

REGULATION EMIR	am.emir@intesasanpaolo.com
REGULATION DFA	am.dfa@intesasanpaolo.com
REGULATION HKMA	am.hkma@intesasanpaolo.com
REGULATION MMSR	am.mmsr@intesasanpaolo.com
REGULATION SHS	am.shs@intesasanpaolo.com
REGULATION REMIT	am.remit@intesasanpaolo.com
REGULATION SFTR	am.sftr@intesasanpaolo.com
CONTRIBUTION EURIBOR	am.emmi@intesasanpaolo.com
DELEGATION REPORTS	am.grid@intesasanpaolo.com

GENERAL COMMUNICATION am.fchub@intesasanpaolo.com



3.7 Centralized SWIFT Messages management

3.7.1 Content of the service

"GTS" provides support for ISP Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized SWIFT Message management supplied in conformity with the SWIFT Standards.
All the following details are specified for the Intesa Sanpaolo Group.

3.7.2 Connection to the SWIFT Network

The access to the SWIFTNet Network is done using three (3) connections:

- Parma – CED
- Parma – CAMPUS
- Settimo Torinese

All the connections are type Alliance Connect GOLD with:

- Six (3x2) lines x 2048Kbps/E1 (each connection has both COLT and Orange line)
- Swift SAG + SNL + HSM cluster and separate Certificate
- Three (3) Message Interface (**BOX** Messaging HUB - product by *INTERCOPE International Communication Products Engineering GMBH*) in *Active/Standby* mode (in the following site: Moncalieri, Settimo Torinese, Parma) with Two active LT for each BIC, delivery subset in Shared mode, load balancing (single window for all Interbank Financial Messaging).
- Swift File Act/FIN/RMA services with "multiple distribution"

3.7.3 Availability of the service – KPI

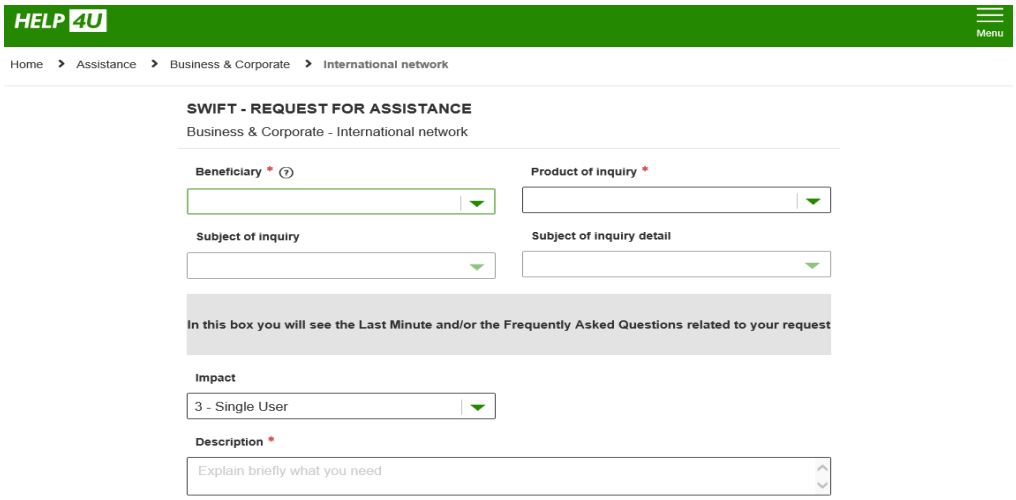
SLA computation is common for the all the entities belonging to Intesa Sanpaolo Group. It is based on the *SWIFT service availability*:

- Service availability is H23,5 x 6,5
- Service unavailable 15' to 30' every day at 03:00 a.m. (CET)
- SWIFT Network unavailable: from Saturday 04:00 p.m. GMT to Monday 04:00 GMT

No scheduled stops of service, inside the service timeframes, are admitted.

The Supplier will create new KPI in according with business priorities.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now.



3.8 Centralized Kondor +

3.8.1 Content of the service

"GTS" provides Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized KONDOR+ management supplied in conformity with Head Office standard.

3.8.2 Connection to the Application

The access to the Kondor+ Application is done using Citrix and based on two connections:

- Milano – CAMPUS 1
- Milano – CAMPUS 2
- Parma – DR

3.8.3 Availability of the service - KPI

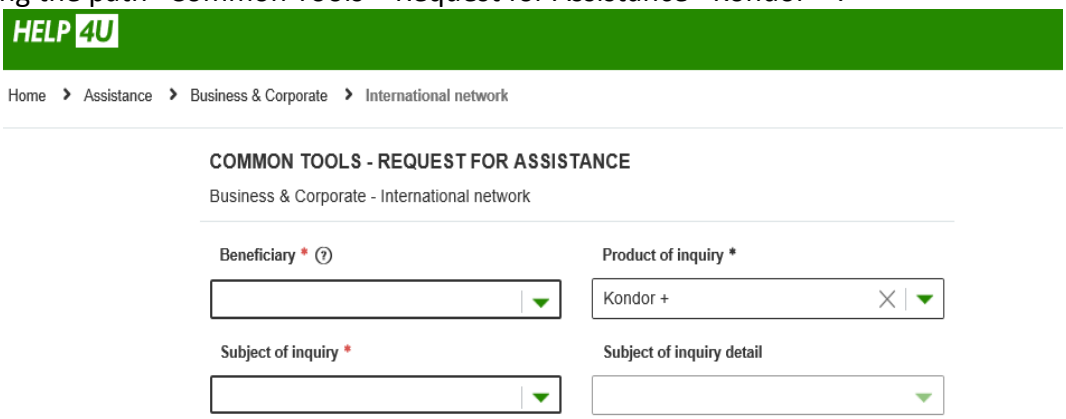
There are three levels of support:

1. The First Support Level: local help desk (as is).
2. The Second Level: Head Office (HO First Level).
3. The Third Level (HO Second Level): take in charge of the ticket forwarded by the Help Desk HO First Level.

The issues must be categorized as follow:

- Service Request (CR)
    - Is a not blocking issue that will be managed only during the direct support period. If HO First Level will receive a CR during the on-demand support period, it will be taken in charge at the beginning of the direct support period.
- Incident Request (IR)
    - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Common Tools – Request for Assistance –Kondor+".



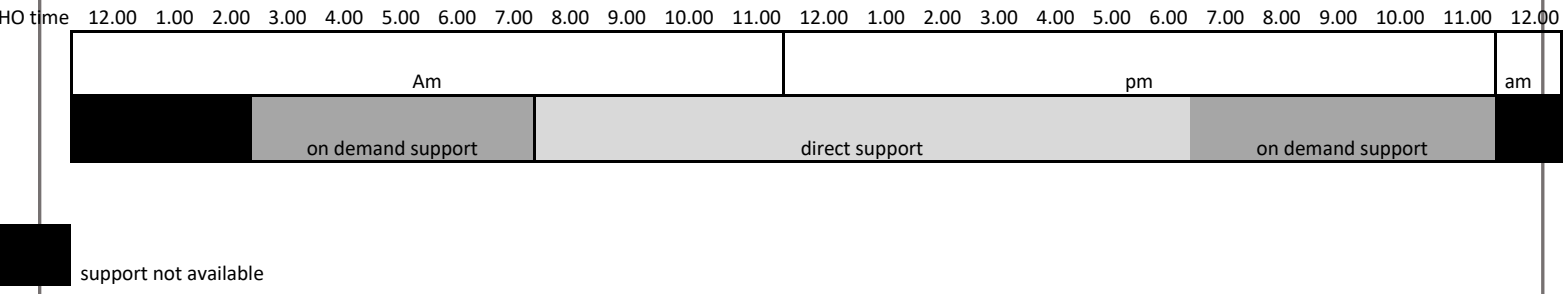
The process should be the following:

- End user should log a ticket web into International Network (ISP on «Common TOOLS» and Capital Markets on «Capital Markets TOOLS»).
- Next, end user must select Kondor+ and the branch from which the ticket is sent to (HK as example for the present document).
- Help Desk in HK should analyze the ticket, diagnose it, and if the problem was local (mainly related to the local workstation), fix it. Otherwise, the problem related to the centralized applications (Kondor+), help desk should pass through the Common Tools queue addressing the ticket to the Servicedesk Finanza.

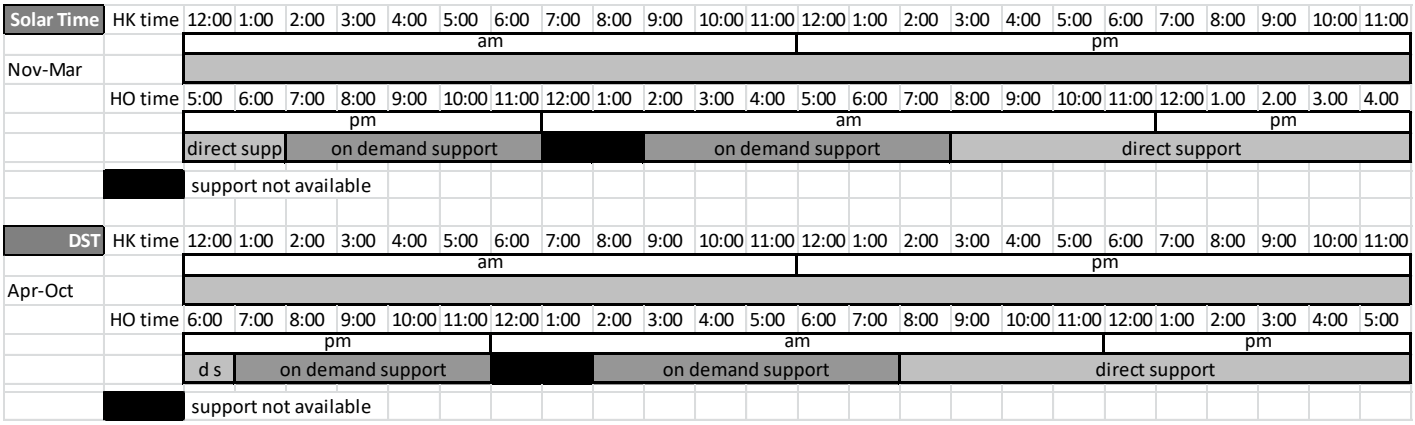
Servicedesk Finanza, who operate under a 24*5 service window, if necessary, will address to the appropriate 3rd level support.

Team Phone Service Desk Finanza +39 02 72612999
Email ServiceDesk.Finanza.gso@intesasanpaolo.com

Below a table with the different type of contact of the AM HO support, based on the project phase:



For the Hong Kong Branch only:



Taking as example the HK Branch:

Based on the Hong Kong time, during the solar time period, from 2.00am to 7.00am and from 9.00am to 3.00pm the AM support will manage only the Incident Request (INC) via on-demand support. all Service Request (CR) coming during this period, will be performed starting from 3.00pm.

From 3.00pm to 2.00am AM support will take in charge Change Request (CR) and Incident Request (INC) via direct support. From 7.00am to 9.00am there isn't any support.

During the Daylight-Saving Time the phases are anticipate by one hour.
The same kind of thinking should be applied at the American and European time zone.

KPI

SLA computation is based on Service availability.

a) KONDOR Availability: Service availability

The service availability is computed as percentage measured on application components.
The proposed SLA for yearly availability is 98%

KPI	Measurement Metrics	SLA	Tolerance	Indicator
KONDOR Availability: Service availability	Service availability percentage measured on application components	98%	2	Av

b) KONDOR Percentage: Service unavailability time

Maximum continuous time of service unavailability (minutes). Unavailability time counter will be reset after each major resolution.

KPI	Measurement Metrics	SLA	Tolerance	Indicator
KONDOR Percentage: Service unavailability time	Maximum continuous time of service unavailability (minutes). Unavailability time counter will be reset after each major resolution.	n.a.	n.a.	P

The Supplier will create new KPI in according with business priorities.

3.9 Centralized Back End Trade Finance System “Eximbills”

3.9.1 Content of the service

“GTS” provides Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized Back End Trade Finance System (Eximbills Enterprise Application) to manage Trade Finance Business.

3.9.2 Connection to the EE Application

The access to the Eximbills Enterprise Application is via web browser based on HTTP connection:

- Moncalieri and Settimo Torinese (EE Live)
- Parma (EE DR)

3.9.3 Availability of the service - KPI

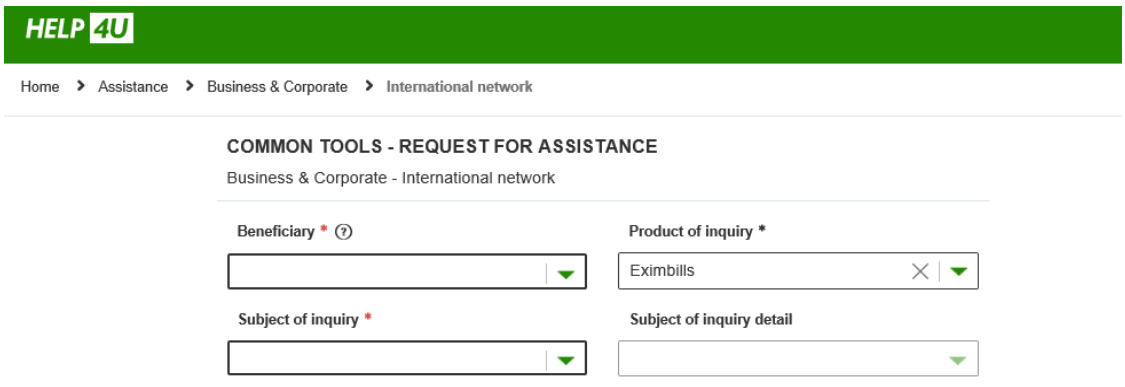
Support is available in three levels:

1. The “First Level” support is local, in charge to the branches AS-IS help desk (in the below HK is mentioned as an example).
2. The “Second Level” support is in charge to GTS, named Head Office (HO) 2nd level.
3. The “Third Level” support is in charge to the Supplier.

The issues must be categorized as follows:

- Service Request (CR)
    - Is a not blocking issue that requires a change in the system (configuration or implementation). will be managed only during the HO direct support period. If HO 2nd Level will receive a CR during the “no CR support period”, it will be taken in charge at the beginning of the direct support period for Change Requests.
    - Is a not blocking issue that does not require a change in the system (configuration or process). will be managed in the direct support period. If the 24*7 2nd Level team will receive this type of CR it will be taken in charge as soon as possible.
- Incident Request (IR)
    - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User’s Branch should use the standard ISP portal “Help4U” - Service Now, following the path “Common Tools – Request for Assistance – Eximbills”.



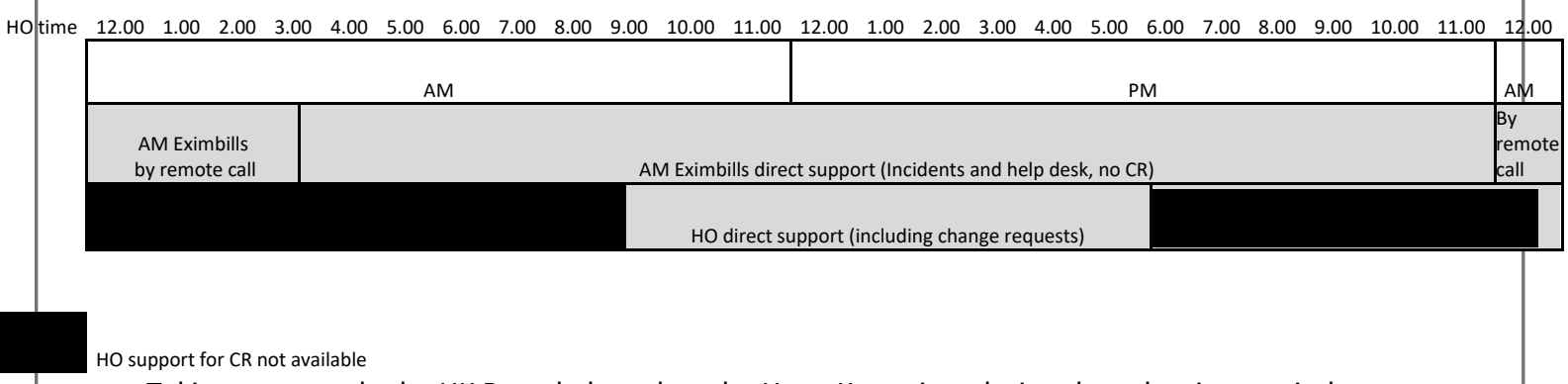
The process should be the following:

- End user should log a ticket web into International Network
- After, end User must select EXIMBILLS application.
- Help Desk, as an example the one in HK, analyze the ticket, diagnose it, and if the problem can be solved locally (mainly related to the local workstation) fix it. Differently, the problem related to the centralized application (Back End Trade Finance) must pass through the Common Tools queue escalating the ticket to the AM Eximbills 2nd Level: "Sistemi Applicativi Target" → "Rendicontazione contabilità e estero" → "Eximbills" or to "Presidio AS 400" in case of Infrastructure or SIRE related issues.

"AM Eximbills" service operates under a 24*5 availability window, if necessary, the ticket will be address to the appropriate 2nd and 3rd level support team.

AM Eximbills email	AM_Exibmills@intesasanpaolo.com
AM Eximbills phone	numbers will be provided to 1st level persons

Below a table with the different type of contact point for AM HO 2nd level support, based on the project phase:



Taking as example the HK Branch, based on the Hong Kong time during the solar time period:

- from 06.00am to 09.00am the AM support is available by remote call and will manage blocking Incidents only
- from 09.00am to 04.00pm and from 01.00am to 06.00am the AM support will manage Incident Requests, not blocking issues and Service Requests which don't requires system changes. All Change Requests raised during this period, will be performed starting from 04.00pm
- from 04.00pm to 01.00am AM support will take in charge Change Request (CR) and Incident Request (INC) via direct support
- during the Daylight-Saving Time the phases are anticipate by one hour.

The same approach is also applied to the American and European time zones.
The Supplier will create new KPI in according with business priorities.

3.10 Centralized Ricora

3.10.1 Content of Service

Ricora is an application aimed to handle reconciliation of SWIFT messages MT940 and MT950 (Cash) and MT535 (Securities). The tool allows reconciliation activity of statements suitable for different kinds of accounts: Our Accounts, Reciprocal Accounts between Banks, Eba Account,

Internal Accounts. Also, reconciliation regarding the issuance and settlement of securities, in particular: Statements of Holdings and Statements of Transactions.

3.10.2 Connection to the Application

The access to the Ricora Application is done using the Intesa Sanpaolo's intranet through Single Sign On. Enabling codes assignment is necessary to access the tool.
The access to the Ricora Application is via web browser and the architecture relies on the following data centers:

- Moncalieri (Production Site)
- Parma (Secondary Site)
- Parma (BCP Site)

3.10.3 Availability of the service – KPI

- Availability timeframes of application

Application	Ordinary Hours (with Service Unit presence)	Ordinary Availability	Reperibilità Festiva (per disaster/recovery e attività ordinarie)
RICORA	Every working day from 7.00 to 17.00	• from 5:00 p.m. to 7:00 a.m. the following day, on all business days Monday through Thursday • from 5:00 p.m. on Friday to 9:00 p.m. on Saturday. • from 6.00 a.m. to 8.00 a.m. on Monday mornings and on working days following a midweek holiday • From 8:30 a.m. to 8:00 p.m. on target holidays	All periods not already covered by Ordinary Hours or Ordinary Availability

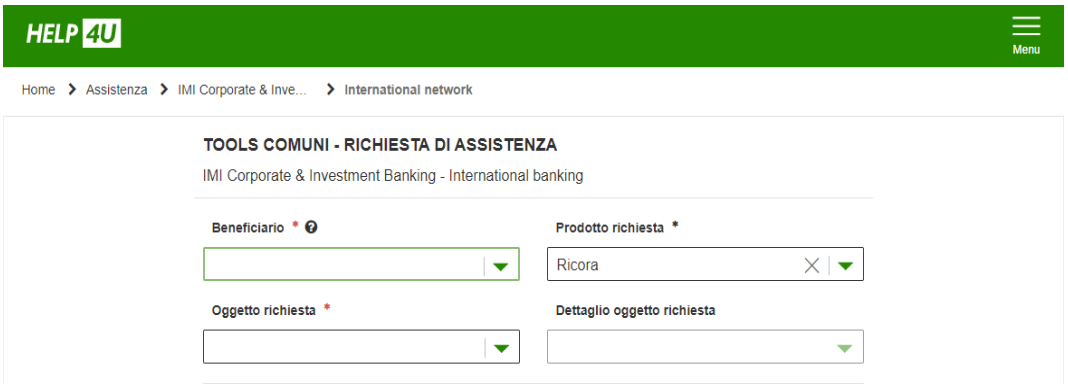
- Incident classification and Resolution time

Priority	Severity	Description	Intervention	Maximum resolution time*	Fraction of delay (for penalties calculation)
1	Major	Emergency Incident	Immediate action to unblock major disruptions in operations	2h	0,5h
2	Severe	Urgent Incident	Urgent intervention to restore partial disruptions in operations	8h	2h
3	Medium	Incident	Intervention to restore limited impacts on functionality, which however affect the regular operations of the company.	36h	8h
4	Low	Incident ASAP	Intervention to be performed as soon as possible	100h	2 giorni (*)
5 (**)	Residual	Schedulable Incident	Intervento da inserire in rilasci pianificati (release) unitamente a	Not Expected	Not expected

			interventi di manutenzione migliorativa		

- Quality of provided services (KPI)

Incident requests can be submitted using Help4U tool by the following path:
Home > Assistenza > IMI Corporate & Investment Banking > Tool Comuni – Richiesta di assistenza



KPI

Descrizione	Valore OBIETTIVO	Measurement	Tolerance	Indicator
Average time of taking charge of tickets (PIC):	Score > 95% (1)	Monthly	2 (3)	Adequacy
Average Processing Time (TDL)	Score > 95% (2)	Monthly	2 (3)	Adequacy

(1) Average ticket handling time (PIC)
• The score is determined by considering the average value of the scoring referred to the timing of taking charge of the individual tickets in the period
• Take charge minimum threshold: 1h
• Take charge maximum threshold: 2h
• Individual ticket scoring is expressed as a percentage based on the distance between the minimum and maximum thresholds.
• If measured time is <= 1h scoring is 100%.
• If measured time is between 1h and 2h scoring is (1-((measured time-min threshold)/(maximum threshold – min threshold))*100
• If measured time is > 2h scoring is 0

(2) Average processing time (TDL)
• The score is determined considering the average value of the scoring referring to the timing of processing of the individual tickets in the period
• High priority ticket:
  - Processing minimum threshold: 8h
  - Processing maximum threshold: 12h
• Normal priority ticket:
  - Processing minimum threshold: 36h
  - Processing maximum threshold: 54h

• If measured time is <= min threshold scoring is 100%.

• If measured time is between min threshold and max threshold scoring is (1-((measured time-min threshold)/(maximum threshold – min threshold))*100
• If measured time is > max threshold scoring is 0

(3) Tolerance
Incident > 30 days Backlog

3.11 Centralized IrionDq

3.11.1 Description and content of the service

IrionDq is a reconciliation tool developed on SQL Server platform, used to reconcile SIRE and Kondor+.
Foreign Branches that accepted an outsourced service and this Service Level Agreement, are provided by "GTS" with a centralized IrionDq management supplied in conformity with Head Office standard.

3.11.2 Connection to the Application

The access to the IrionDq Application is done using Citrix and based on the standard SPIMI's domain Citrix connection.

The system architectures are supported by 2 technology farms/Campus:

- Torino – Moncalieri
- Torino – Settimo Torinese

3.11.3 Availability of the service - KPI

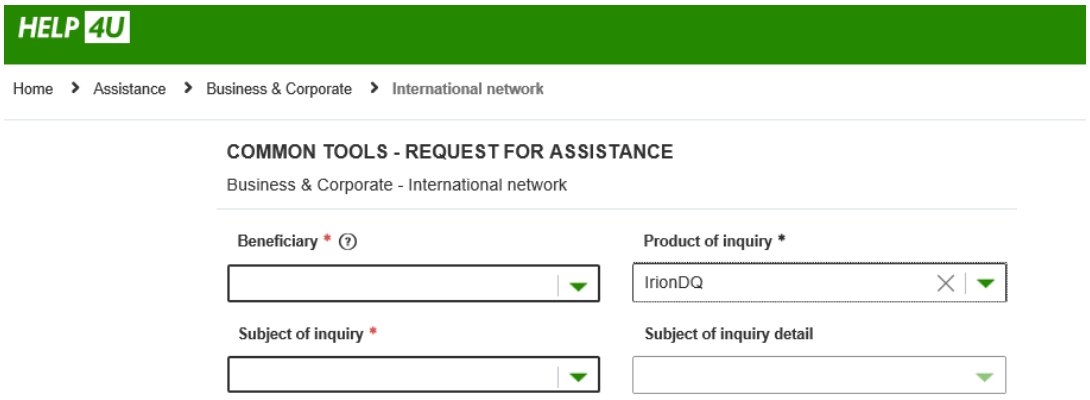
There are three levels of support:

- The First Support Level will remain in charge on local HUBS (HK as example for the present document) help desk (as is). GTS "SERVICEDESK.FINANZA.GSO" Support for "centralized Finanza GTS" will be 2° level support of the IrionDq Software
- The Hub will contact "SERVICEDESK.FINANZA.GSO", advising via mail and SERVICEDESK.FINANZA.GSO" will arrange and open the remedy ticket to riconciliazioni.DOF" Am supporto IrionDQ, otherwise the Hub will open the ticket directly to "riconciliazioni.DOF"
- GTS "riconciliazioni.DOF" will be 3° level support of the IrionDq Software in working hours (local time ITA) time 08:00-18:30 from Monday to Friday.

The issues must be categorized as follow:

- Service Request (CR)
  - Is a not blocking issue that will be managed only during the direct support period. If HO First Level will receive a CR during the on-demand support period, it will be taken in charge at the beginning of the direct support period.
- Incident Request (IR)
  - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Common Tools – Request for Assistance – IrionDq".



The process should be the following:

- End user should log a ticket web into International Network (ISP on «Common TOOLS» and IrionDq on «IrionDq»).
- After, end user has to select IrionDq and the branch from which the ticket is sent to (HK as example for the present document).
- Help Desk in HK should analyze the ticket, diagnose it, and if the problem was local (mainly related to the local workstation), fix it. In case the problem was related to the centralized application (IrionDq), help desk should pass through the Common Tools queue addressing the ticket to the GTS Help Desk.

E-mail SERVICEDESK.FINANZA.GSO <ServiceDesk.Finanza.gso@intesasanpaolo.com>
E-mail riconciliazioni.DOF <riconciliazioni.DOF@IntesaSanpaolo.com>

The Supplier will create new KPI in according with business priorities.

Following, the service coverage per day referred to the local time.

			COUNTRY OFFICE STATUS END-USER							A.M. SERVICE TIMETABLE (LOCAL TIME)		A.M. SERVICE STATUS						
ANTE(-) POST(+)	DELAY (H)	COUNTRY (HUB/SPOKE)	Monday	Tuesday	Wednesday	Thurday	Friday	Saturday	Sunday	TIME START	TIME END	Monday	Tuesday	Wednesday	Thurday	Friday	Saturday	Sunday
-1	06:00	New York	Open	Open	Open	Open	Open	Close	Close	2:00	12:30	Open	Open	Open	Open	Open	Close	Close
-1	01:00	London	Open	Open	Open	Open	Open	Close	Close	7:00	17:30	Open	Open	Open	Open	Open	Close	Close
0	00:00	Frankfurt	Open	Open	Open	Open	Open	Close	Close	8:00	18:30	Open	Open	Open	Open	Open	Close	Close
0	00:00	Madrid	Open	Open	Open	Open	Open	Close	Close	8:00	18:30	Open	Open	Open	Open	Open	Close	Close
0	00:00	Paris	Open	Open	Open	Open	Open	Close	Close	8:00	18:30	Open	Open	Open	Open	Open	Close	Close
0	00:00	Warsaw	Open	Open	Open	Open	Open	Close	Close	8:00	18:30	Open	Open	Open	Open	Open	Close	Close
1	02:00	Istanbul	Open	Open	Open	Open	Open	Close	Close	10:00	20:30	Open	Open	Open	Open	Open	Close	Close
1	02:00	Doha	Open	Open	Open	Open	Close	Close	Open	10:00	20:30	Open	Open	Open	Open	Open	Close	Close
1	03:00	Dubai	Open	Open	Open	Open	Close	Close	Open	11:00	21:30	Open	Open	Open	Open	Open	Close	Close
1	03:00	Abu Dhabi	Open	Open	Open	Open	Close	Close	Open	11:00	21:30	Open	Open	Open	Open	Open	Close	Close
1	07:00	Hong Kong	Open	Open	Open	Open	Open	Close	Close	15:00	1:30	Open	Open	Open	Open	Open	Close	Close
1	07:00	Shanghai	Open	Open	Open	Open	Open	Close	Close	15:00	1:30	Open	Open	Open	Open	Open	Close	Close
1	07:00	Singapore	Open	Open	Open	Open	Open	Close	Close	15:00	1:30	Open	Open	Open	Open	Open	Close	Close
1	08:00	Tokyo	Open	Open	Open	Open	Open	Close	Close	16:00	2:30	Open	Open	Open	Open	Open	Close	Close
1	10:00	Sydney	Open	Open	Open	Open	Open	Close	Close	18:00	4:30	Open	Open	Open	Open	Open	Close	Close

3.12 Centralized Splunk

3.12.1 Content of the service

"GTS" provides Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized SPLUNK management supplied in conformity with Head Office standard.

3.12.2 Connection to the Application

The access to the SPLUNK Application is done using Citrix and based on two connections:

- Settimo Torinese – PRODUCTION
- Parma – DR

Data are forwarded to Splunk architecture based on the following representation:

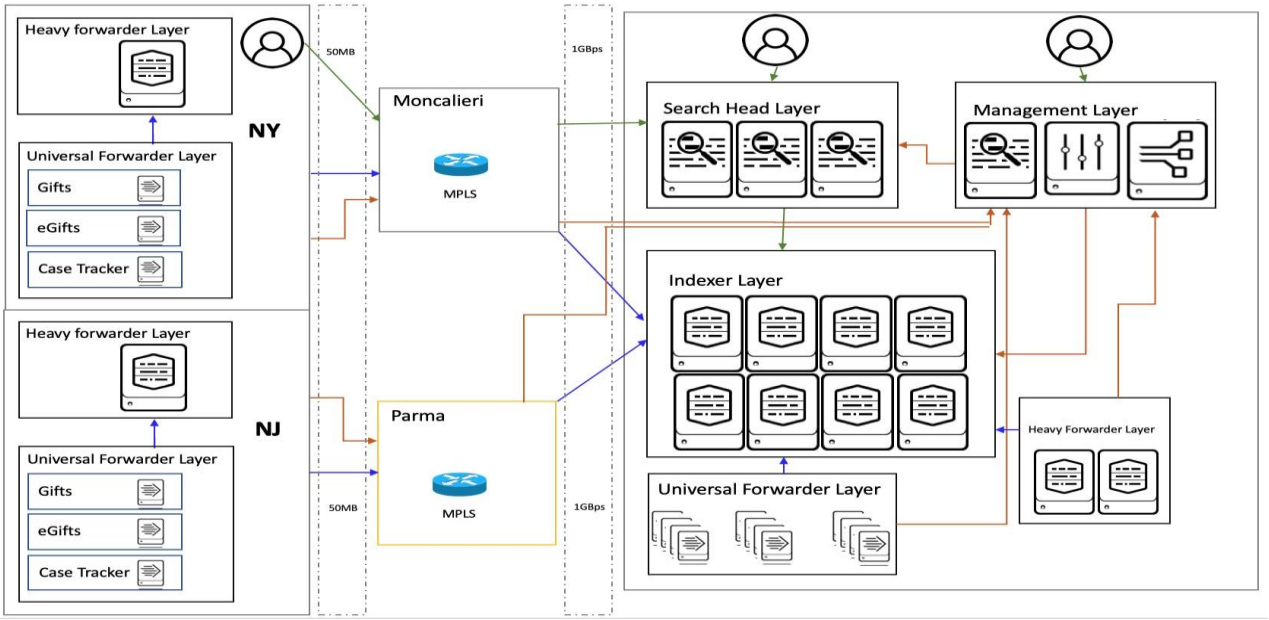


Figure 1 - Global Splunk Architecture

3.12.3 Availability of the service – KPI

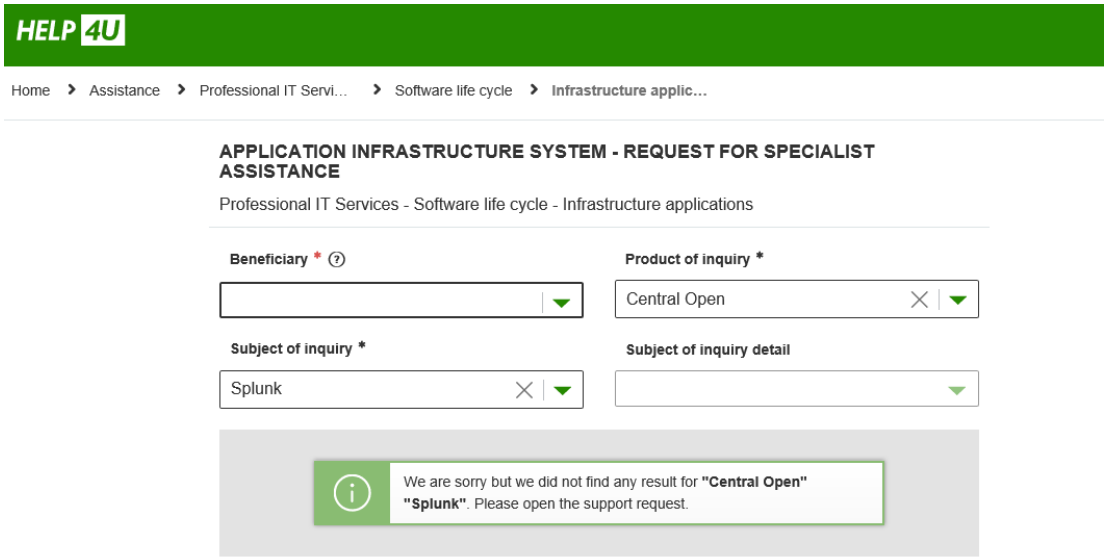
There are three levels of support:

1. The First Support Level: local help desk (as is).
2. The Second Level: Head Office (HO First Level).
3. The Third Level (HO Second Level): take in charge of the ticket forwarded by the Help Desk HO First Level.

The issues must be categorized as follow:

- Service Request (CR)
    - Is a not blocking issue that will be managed only during the direct support period. If HO First Level will receive a CR during the on-demand support period, it will be taken in charge at the beginning of the direct support period.
- Incident Request (IR)
    - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Service Now, following the path "Assistance – Professional IT Services – Software Life Cycle – Infrastructure Applications – Splunk[13]".



The process should be the following:

1) End User must contact Local IT for first level support. Local IT must use documentation and knowledge base provided from GTS to solve autonomously the issue.
2) If Local IT is unable to solve the issue, End User have to login in Help 4U portal from ISP internal network.
3) Once logged in, end user must digit splunk to correctly address the issue. HO First Level will receive it. It is extremely important to give full description of the problem using the "note" field. It is also possible to add some attachments.
4) HO first level will analyze the problem and ask for more information, if necessary. Then they will forward the ticket to HO second level.
5) HO second level will analyze and solve the problem, addressing it to the vendor if necessary.

HO second level operate with "Best Effort" SLA, only during working hours (8.30 am – 16.45 pm CET)

3.13 Murex

3.13.1 Content of the service

"GTS" provides Foreign Branches, having accepted that outsourced service and this Service Level Agreement, with a centralized Murex management supplied in conformity with Head Office standard.

3.13.2 Connection to the Application

The access to the Murex Application is done using Citrix and based on the standard SPIMI's domain Citrix connection:

[13] https://isgs.service-now.com/service_portal_isgs

The system architectures are supported by 2 technology farms/Campus:

- Torino – Moncalieri
- Torino – Settimo Torinese

3.13.3 Availability of the service

There are two levels of support:

- The First Support Level is in charge of "SERVICEDESK.FINANZA.GSO" Support for "centralized Finanza GTS"
- "SERVICEDESK.FINANZA.GSO" will arrange and open the remedy ticket to AM-Murex Support (second level support)
- AM-Murex Support is organized in 3 different groups:
  - MXSUPPORTFO: functional and FO support
  - MXSUPPORTBO: integration support
  - MXSupportREPMD: market data and Reporting support
- "SERVICEDESK.FINANZA.GSO" is in charge of routing ticket remedy to the correct Murex support group, based on the problem/request.

The issues must be categorized as follow:

- Service Request
- Incident

To open a ticket, the User's Branch should contact "SERVICEDESK.FINANZA.GSO":

- by e-mail: ServiceDesk.Finanza.gso@intesasanpaolo.com
- by phone: (+39) 02 8794 9600 or 02 8793 2999

User's Branch does not have to directly contact AM-Murex to open a ticket.

AM-Murex support is guaranteed 24 x 5, from Monday at 00:00 till Friday at 23:59 Italian Time
The Supplier will create new KPI in according with business priorities.

3.14 Centralized Loan IQ

3.14.1 Description and content of the service

Loan IQ is an application designed to manage loans.
Foreign Branches that accepted an outsourced service and this Service Level Agreement, are provided by "GTS" with a centralized Loan IQ management supplied in conformity with Head Office standard.

3.14.2 Connection to the Application

The access to the Loan IQ Application is done using Citrix and based on the standard SPIMI's domain Citrix connection.

The system architectures are supported by technology farms/Campus:

- Torino – Moncalieri

3.14.3 Availability of the service – KPI

There are two types of support:

- Front end support.

- System integration support.

The issues must be categorized as follow:

- Service Request (CR)
  - Is a not blocking issue that will be managed only during the direct support period.
- Incident Request (IR)
  - Is a blocking issue that will be managed as soon as possible during the direct support and on-demand period.

To open a ticket, the User's Branch should use the standard ISP portal "Help4U" - Assistenza Specialistica - IMI Corporate & Investment Banking - International network- "Tools comuni - Richiesta di assistenza- Loan IQ FN".

The user can also contact the Loan IQ support team by email AM.LAS.FN@intesasanpaolo.com .

AM-Loan IQ (online) support is guaranteed:

- For front end support from Monday till Friday, from 8:30 till 18:30 (Italian Time).
- For System integration support from Monday till Friday, from 8:30 till 22:00 (Italian Time).
- For System integration support from Monday till Friday, from 8:30 till 24:00 (Italian Time) for the end of month.

Other availability (only in case of emergency - On-call service) is guaranteed:

- Monday – Friday: 18:30 – 8:30 (Italian Time)

Below, the SLAs and KPIs will be highlighted and explained:

- Service levels for corrective maintenance:

Priority	Severity Incident	Description	Type of intervention	Maximum solution time *	Delay fraction (for calculation of penalties)
1	Major	Incident in Emergency	Immediate intervention to unblock serious business interruptions	12h	0,5h
2	Grave	Urgent Incident	Urgent intervention to restore partial interruptions to operations.	24h	2h
3	Medium	Incident	Intervention to restore limited impacts on functionality, which in any case affect the regular operation of the company.	54h	8h
4	Low	Incident ASAP	Intervention to be performed as soon as possible	150h	2 giorni (*)
5 (**)	Residual	Schedulable incident	Intervention to be included in planned releases together with improvement maintenance interventions	Not Expected	Not Expected

(*) except in exceptional cases subject to planning and agreed in advance with the operational contact.

(**) N.B. if an accident / priority 5 ticket is received, the same earned be processed with priority 4.

In the case of Applications for which it is not possible to intervene on the source code, the guaranteed service levels will be related to:

- At the time of activation of the Third-Party Supplier.
- Compliance with feedback and escalation procedures, especially in relation to possible temporary "bypass" corrective actions.
- At the time of resolution for temporary corrections (where possible) to overcome or mitigate the anomalies found.

Service Levels for Third Party SW:

Priority	Severity Incident	Description	Maximum ACTIVATION time	Delay fraction (for calculation of penalties)
1	Major	Incident in Emergency	0,5 h	10 min.
2	Grave	Urgent Incident	1 h	20 min.
3	Medium	Incident	4h	1h
4	Low	Incident ASAP	8h	2h
5 (**)	Residual	Schedulable incident	Not Expected	Not Expected

(**) N.B. if incidents / priority 5 tickets are received, they must be processed with priority 4.

- Service levels for evolutionary maintenance, for the support of occasional requests and for the management of tickets:

Priority	Description	Maximum time of Realization	Delay fraction (for calculation of penalties)
	Evolutionary maintenance	To be defined from time to time	1 day
	Support Occasional Requests	To be defined from time to time	1 day

- Qualitative parameters of the services performance not subject to penalties:
  - SLA (Service Level Agreement) related to ticket management.

Description	GOAL value
Average time to take charge of tickets (PIC):	Score > 95%
Average Processing Time (TDL)	Score > 95%
Backlog ticket with seniority greater than 1 month	0

3.15 MOBU

3.15.1 Description and content of the service

The MOBU dashboard is a messaging monitoring system for incoming and outgoing payments of the Foreign Branches. The tool aims to track the life cycle of all the Swift messages and SEPA, Local payments instructed and received by the Branches.

3.15.2 Connection to the Application

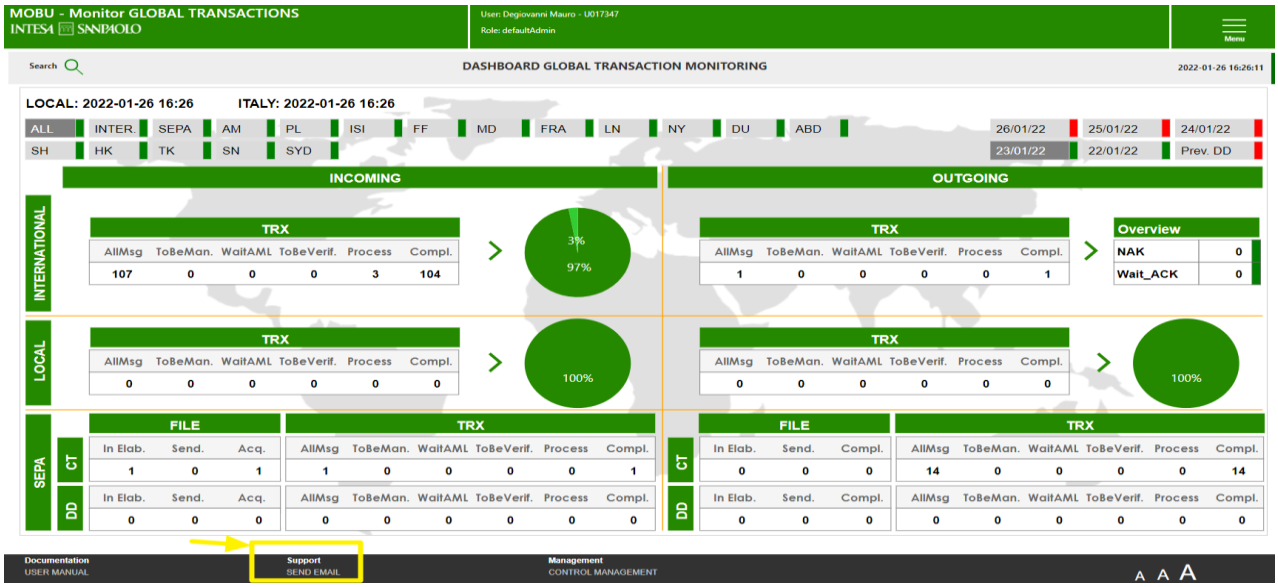
The tool complies with the bank's security guidelines, with access controlled by user profiling which guarantees visibility cones and access restrictions depending on the user who is accessing.
The MOBU dashboard has as input systems SIRE and BOX and therefore tracks the states (i.e., AML blocked, ACK/NAK, SIRE executed, etc.) coming from the two systems.

3.15.3 Availability of the service - KPI

Support service is provided by GTS:

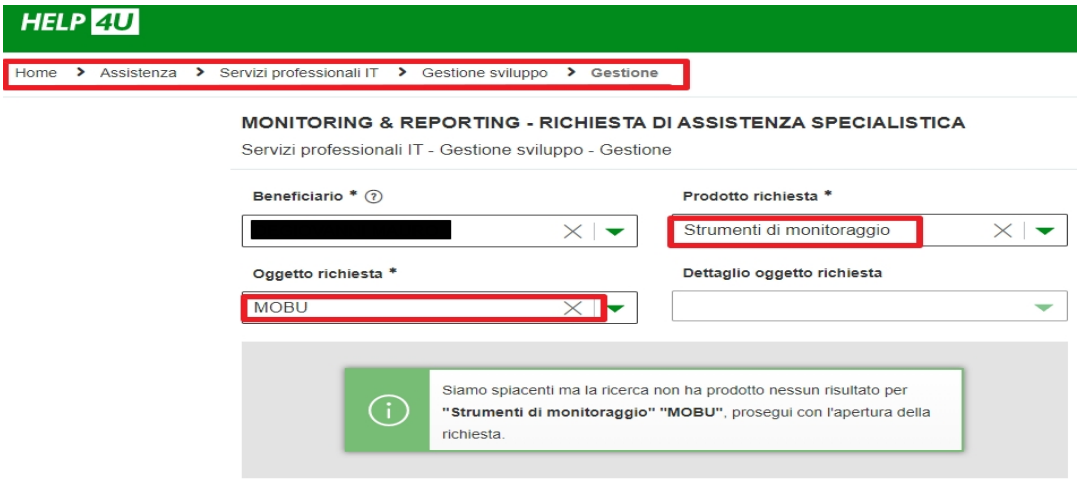
- The service is available 24/24 hours and 7 days per week.
- It is possible to contact support service via email or via standard ISP portal "Help4U" - Service Now.

To contact support service via email, the user should use the link in the footer of the dashboard MOBU or using the email address "SupportoMonitorMOBU@intesasanpaolo.com".



To open a ticket, the user should use the standard ISP portal "Help4U" - Service Now, following the path "Monitoring & Reporting – Richiesta di Assistenza specialistica" and choosing:

- "Strumenti di monitoraggio" as product of inquiry.
- "MOBU" as subject of inquiry.



3.16 Core Banking System WinBank - for Istanbul Branch only

3.16.1 Content of the service

"GTS" provides Istanbul Branch, having accepted that outsourced service and this Service Level Agreement, with a local core banking system – **WinBank** – in addition to the **SiRe** application, management supplied in conformity with Head Office standard.

3.16.2 AM additional service in the scope of WinBank

In the context of WinBank AM additional service "GTS"

- perform the corrections needed to eliminate any malfunctioning of the WinBank core application which may arise during operation of same.
- release and, if necessary, install any improvement of the Product developed and made available to the market.
- release and, if necessary, install any new version (major release upgrades are not - within the scope) of WinBank made available to the market.
- upgrade the Products (major version upgrades are not within the scope) in accordance with the evolution of the platforms for which their use was licensed, provided that such update is released to the market.
- modify and update the Products as required by law provisions or to adapt them to new international standards. Such updates shall be delivered on or before the effective date of the provisions or regulations they refer to.
- supply specific WinBank Helpdesk and Demand Management service.

The Supplier will create new KPI in according with business priorities.

3.17 Care solution - for New York Branch only

3.17.1 Content of the service

"GTS" provides New York Branch, having accepted the outsourced service and this Service Level Agreement, with a Centralized Customized Automated Rules Engine – Transaction Monitoring system for ISPNY management supplied in conformity with Head Office standard.

3.17.2 Application Management

The AM is managed by NY Information technology through a dedicated SLA contract with the vendor Guidehouse. GTS provides with a support to Guidehouse for their AM services. The FM is under SLA between GTS and New York Branch. ISP is responsible for installation and operational tuning / maintenance of the operating system and database server software as well as the Integration, Analysis and Reporting Services.
The vendor Navigant is responsible for the development, delivery, and maintenance of the SSIS packages.

3.17.3 Server architecture

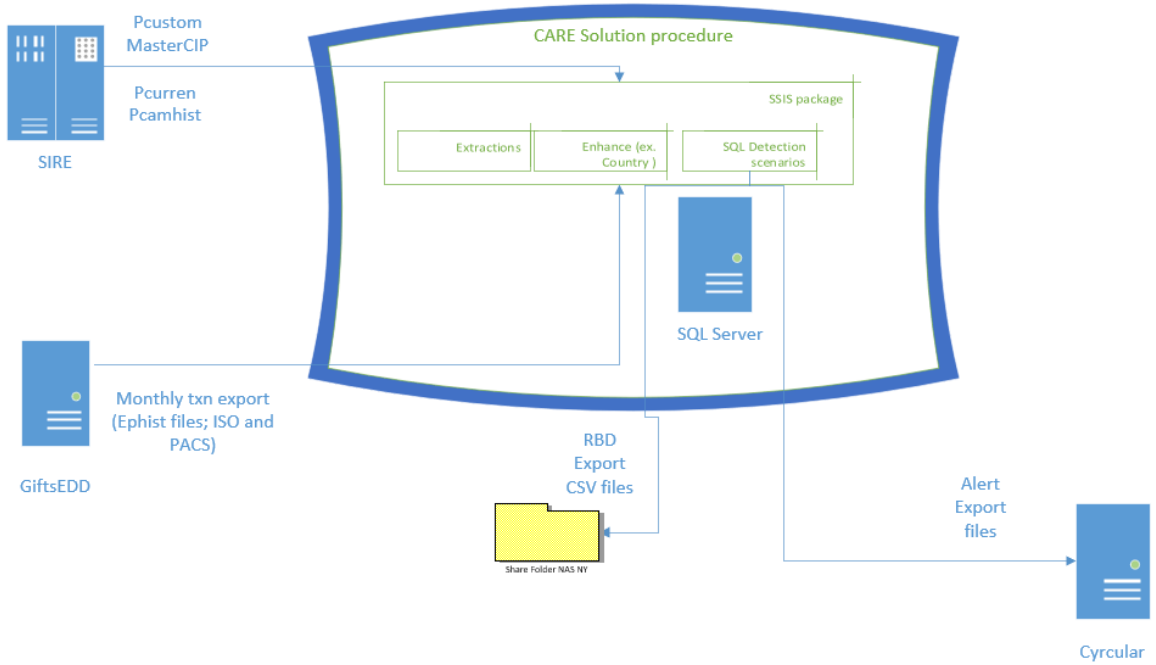
There are four distinct IT environments involved in the processing of the monthly payment files.

- The source Gifts/EDD system is hosted in the ISPNY data center.
- The CARE Solution, SIRE and Cyrcular are hosted in an ISP data center in Moncalieri/Settimo Italy

Overview

CARE Solution encompasses a set of automated processes, system integrations and data flows. On the third business day of each month, CARE Solution receives and loads the prior month's payments from the existing Gifts/EDD data tier into a dedicated SQL Server database.
The rules, defined in the CARE Solution Rulebook document, are then applied the payment data. CARE Solution flags payments that alert based on the rule logic and stores the alerts and related information payment in the database. Subsequently, the alerts and alerting payments are exported to a .csv file compatible with the Cyrcular application. This alert feed is automatically processed by Cyrcular and the alerts are made available to the ISPNY Compliance FIU team.

High-Level Care Solution Diagram
The diagram below outlines the components, inputs, and outputs of the process.



3.17.4 Cyrcular

Cyrcular serves as the user's unique point of access and management for alerts from Transaction Monitoring, both externally generated (i.e., detections generated by CARE Solution), as well as manually generated by users within the application. The management of Transaction Monitoring alerts in Cyrcular pertains to both Customer Monitoring operations, which involve monitoring Client activity, and Non-Customer Monitoring operations, which involve monitoring the activity of non-customer entities.

Cyrcular front end pages are customized in terms of visibility, sections, and functionalities based on the logged-in user authorization, even if cross functional pages/sections are kept the same across users.
In the "Transaction Monitoring" section, the following pages/sections are included:

- Homepage and Notification History section
- Desk (alerts/cases), distinguished among "Customer Monitoring" and "Non Customer Monitoring" sections
- Alert page

• Case page
• Detection page
• Client page
• Counterparty page

A User Handbook is available in “Normativa” at the follow link: Portale Antiriciclaggio Cyrcular NY

To open a ticket, the User’s Branch should use the standard ISP portal “Help4U” - Service Now, following the path “Assistance – Transversal operations – Anti Money Laundering”.

The application has 24-hour coverage (Ticket resolution times and KPIs are governed by the agreements made between GTS and the NY branches)

3.18 Pega – for ISP New York Branch (extension of application use from 2024 for other foreign branches)

3.18.1 Content of the service

“GTS” provides New York Branch, this Service Level Agreement supplied in conformity with Head Office standard.

Pega CIB2B helps address the following key principles:

- Orchestrate and optimize KYC and other due diligence requirements to support entity onboarding decisions.
- Provide simple and rich views of Entity data while providing access complex scenarios.
- Provide Customer Dashboard and Customer Document checklist features.
- Provide ability to incorporate relevant Customer’s related parties onto the Customer onboard processing as well as some other related customer journeys (maintenance, periodic review, …)

3.18.2 Application Management

The FM is under SLA between GTS and New York Branch. ISP is responsible for installation and operational tuning / maintenance Services.
To access the ISP web application, it is necessary to use the "Google Chrome" web browser using the following links and SPIMI profile:

Connection to the Application

The access to the Pega CLM CIB2B Application is done using the Intesa Sanpaolo's intranet through Single Sign On. Enabling codes assignment is necessary to access the tool.
The access to the Pega CLM CIB2B Application is via web browser and the architecture relies on production site:

- Moncalieri (Production Site), Italy

Production environment:
https://onbo0.sede.corp.sanpaoloimi.com:18240/scriptOnbo0/prweb/PRAuth/CIB2B
TEST environment:
https://sonbo0.syssede.systest.sanpaoloimi.com:18240/scriptOnbo0/prweb/PRAuth/CIB2B

3.18.3 Availability of the service – KPI

Availability timeframes of application

Application	Ordinary Hours (with Service Unit presence)	Ordinary Availability	Holiday availability (per disaster/recovery and ordinary activities)
Pega CLM CIB2B	Every working day from 8:30 to 17:30 CET	Every day from 00:00 to 24:00 except maintenance window from Saturday 20:30 to Sunday 23:30 CET	N/A

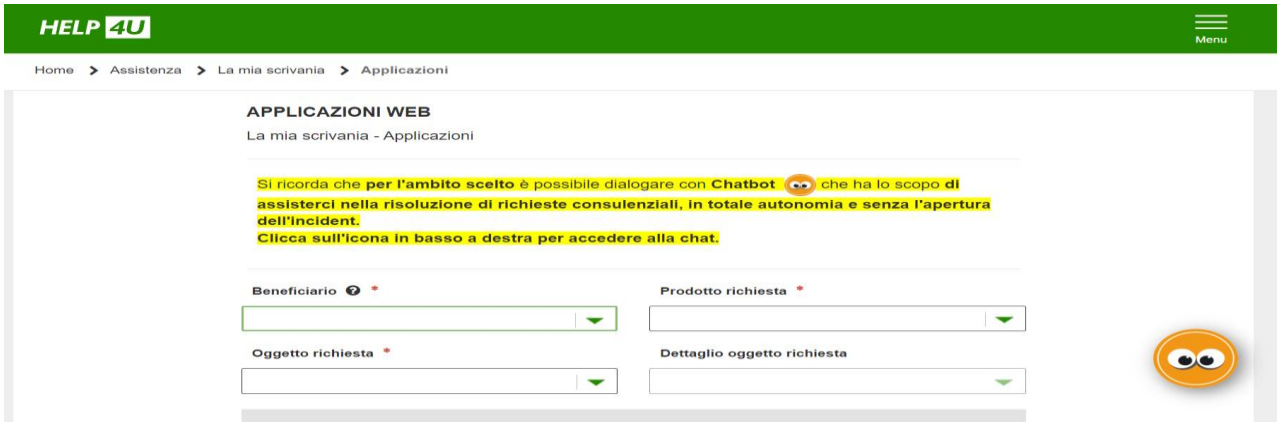
- Incident classification and Resolution time

Priority	Severity	Description	Intervention	Maximum resolution time*	Fraction of delay (for penalties calculation)
1	Major	Emergency Incident	Immediate action to unblock major disruptions in operations	6h	0,5h
2	Severe	Urgent Incident	Urgent intervention to restore partial disruptions in operations	12h	2h
3	Medium	Incident	Intervention to restore limited impacts on functionality, which however affect the regular operations of the company.	54h	8h
4	Low	Incident ASAP	Intervention to be performed as soon as possible	150h	2 days (*)
5 (**)	Residual	Schedulable Incident	intervention to be included in the planned release together with improvement maintenance interventions	Not Expected	Not expected

Quality of provided services (KPI)

Incident requests can be submitted using Help4U tool by the following path:

Home > Assistenza > La mia scrivania > Applicazioni – Applicazioni web (prodotto richiesto =PEGA).



KPI

Description	Value Target
Average time of taking charge of tickets (PIC):	Score > 95% (1)
Average Processing Time (TDL)	Score > 95% (2)

(1) Average ticket handling time (PIC)

• The score is determined by considering the average value of the scoring referred to the timing of taking charge of the individual tickets in the period
• Take charge minimum threshold: 1h
• Take charge maximum threshold: 2h
• Individual ticket scoring is expressed as a percentage based on the distance between the minimum and maximum thresholds.
• If measured time is <= 1h scoring is 100%.
• If measured time is between 1h and 2h scoring is (1-((measured time-min threshold)/(maximum threshold – min threshold))*100
• If measured time is > 2h scoring is 0

(2) Average processing time (TDL)

• The score is determined considering the average value of the scoring referring to the timing of processing of the individual tickets in the period.
• High priority ticket:
  - Processing minimum threshold: 8h
  - Processing maximum threshold: 12h
• Normal priority ticket:
  - Processing minimum threshold: 36h
  - Processing maximum threshold: 54h
• If measured time is <= min threshold scoring is 100%.
• If measured time is between min threshold and max threshold scoring is (1-((measured time-min threshold)/(maximum threshold – min threshold))*100
• If measured time is > max threshold scoring is 0

(3) Tolerance

Incident > 30 days Backlog

4 DECLARATION

We undersigned "**INTESA SANPAOLO S.p.A**" confirm to whom it may concern that the above reported Service Level Agreement is in force and duly integrated in our internal processing procedures.

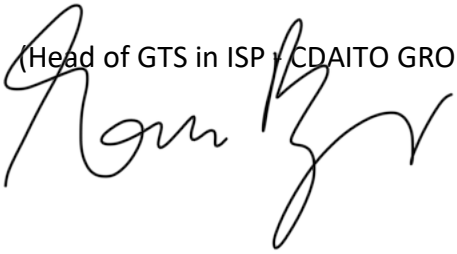
In witness thereof

Moncalieri, 2024

"**INTESA SANPAOLO S.p.A**"

Enrico Bagnasco

(Head of GTS in ISP + CDAITO GROUP TECHNOLOGY & SERVICES)



5 ADDENDUM NEW YORK HUB

Addendum to the Service Level Agreement – International Network
New York Hub - November 2011

A1. Data Confidentiality

A1(a) General

GTS and the New York Branch agree that all information and data provided pursuant to this Agreement by each party to the other party is confidential and proprietary information (**from now on "Confidential Information"**) of the disclosing party. No party shall use Confidential Information provided by the other party for any purpose other than as permitted or required for performance under this Agreement, or as otherwise agreed to between the parties. Each party agrees not to disclose or provide Confidential Information provided by the other party to any third party, without the express written consent of the other party, with the exception of (i) any affiliate or subsidiary with employees required to retain the confidentiality of the Confidential Information. (ii) employees who have a need to know in the course of performing services pursuant to this Agreement, provided that such employees are required to retain the confidentiality of the Confidential Information. (iii) subcontractors as necessary for GTS to deliver services to the New York Branch under this Agreement, provided that employees of such subcontractors are required to retain the confidentiality of the Confidential Information. and (iv) each party agrees to take all reasonable measures, including, but not limited to measures taken by each party to safeguard its own confidential information to prevent disclosure by employees, agents, or contractors.

A1 (b) Exceptions

Nothing provided herein shall prevent GTS or the New York Branch from disclosing Confidential Information to the extent the Confidential Information (i) is or hereafter becomes part of the public domain through no fault of either GTS or the New York Branch. (ii) is rightfully received from a third party without similar restriction of the third party's rights. (iii) is independently developed by either GTS or the New York Branch. (iv) is disclosed pursuant to the requirements of law. or (v) is already known to either GTS or the New York Branch prior to disclosure.

A1(c) Privacy Policy

GTS and the New York Branch shall comply with the terms of their own privacy policies as indicated within the New York Branch Corporate Compliance Manual.

A2 Compliance with Law

The New York Branch is responsible to forward to Head Office relevant U.S. laws, regulations and regulatory guidance pertaining to IT requirements and outsourcing, data protection/privacy, or other related matters set forth by U.S. laws, regulations or other law enforcement agencies that may affect this Service Level Agreement, with the aim to ensure GTS's prompt compliance with such requirements.

For the avoidance of doubt, GTS expressly acknowledges that the New York Branch is a New York-State licensed branch supervised by the Board of Governors of the Federal Reserve System and the New York state department of financial services (NYDFS) and is subject to U.S. laws and regulations. GTS agrees to provide the services set forth in this Agreement in compliance with all applicable U.S. legal and regulatory requirements, including but not limited to, Federal Financial Institution Examination Council (FFIEC) regulatory guidance on information technology and outsourcing matters, Title V of the Gramm-Leach Bliley Act governing the confidentiality of customer data and the Right to Financial Privacy Act governing the U.S. government's access to confidential customer data.

A3 U.S. Regulatory Authorities/Access to Information

GTS expressly acknowledges and agrees that it will provide any U.S. regulatory authority supervising the New York Branch, pursuant to all applicable U.S. laws and regulations, as well as any Internal and External Auditors full access to the databases, operational procedures, programs and logs belonging to the New York Branch and any books and records relating to the arrangements covered by this Agreement, whether such materials are located in Italy or the United States.

A4 Access by Italian Authorities to Customer Data Managed by GTS

Pursuant to Italian law, the Fiscal, Administrative and Criminal Italian Authorities have the power to access all customer data existing in Italy. GTS by executing the outsourcing contract will manage some of the New York Branch's customer data in Italy. GTS will provide the New York Branch with immediate notification of any request from Italian authorities concerning the New York Branch's customer data. The New York Branch will then be entrusted to report the event to its U.S. regulators.

A5 Compliance with Document Retention/Preservation Notices

GTS expressly acknowledges and agrees that the New York Branch has, or may have in the future, document retention or preservation notices or policies in place in connection with regulatory or law enforcement inquiries or litigation that may require different electronic data storing or archiving procedures than those otherwise set forth in this Agreement. GTS will provide its services pursuant to this Agreement in compliance with such document retention or preservation notices upon receipt of written notice from the New York Branch regarding the existence and requirements of such notices.

A6 Duration and Withdrawal Rights

This Agreement is effective from [11th] November 2011 and remains valid and in full force until [10th] November 2012 and it is automatically renewed on a yearly basis, unless either party exercises a withdrawal right upon three months advance written notice to the other party delivered by registered mail with return receipt.

A7 Data Processing Systems Availability During Standard Working Hours

New York Branch staff is enabled to continuously access its front & back-office systems, both for input and enquiry, during customary working hours, for avoidance of doubt: from Sunday from 09:00 pm. to Saturday, 05:00 am Eastern Standard Time.

The New York Branch may request service for extended hours. Whenever possible, any request should be sent in writing two weeks in advance, or as soon as the New York Branch is aware of the need, to DCO – International Network, which is responsible for validating the request and to forwarding it to the relevant GTS Operational Unit. The relevant GTS Operational Unit will either approve the New York Branch's request for the temporary extension of the system availability or will deny the New York Branch's request and set forth in writing the reasons preventing GTS from granting the request.

A8 Data management

During 2024, some evaluations could be carried on regarding:

- GTS management of HO systems that store and transmit NPI data on behalf of NY branch.
- Notification from GTS of data breaches on HO systems that impact NPI data related to NY branch.

We undersigned "**INTESA SANPAOLO SPA - GTS**" and "**INTESA SANPAOLO SPA NEW YORK BRANCH**" confirm to whom it may concern that the above reported Addendum for New York HUB to the Service Level Agreement is in force and duly integrated in our internal processing procedures.

In witness thereof

Moncalieri, 2024

"**INTESA SANPAOLO S.p.A**"

Enrico Bagnasco

(Head of GTS in ISP - COAITO GROUP TECHNOLOGY & SERVICES)

New York, 2024

"**INTESA SANPAOLO SPA NEW YORK BRANCH**"

Paolo Sparano

(General Manager)

6 ADDENDUM ISTANBUL BRANCH

Addendum to the Service Level Agreement – International Network – ITALYA ISTANBUL MERKEZ SUBESI ("Istanbul Branch" or "the Foreign Branch / Bank" or "Bank") – January 2014 - ***RESTRICTIONS ARISING IN CONNECTION WITH THE PROVISION OF THE TURKISH BANKING LAW NO. 5411, THE REGULATION ON BANK'S PROCUREMENT OF SUPPORT SERVICES and THE REGULATION ON INFORMATION SYSTEMS OF BANKS AND ELECTRONIC BANKING SERVICES***

A1. Data Confidentiality

A1(a) General

GTS and the Istanbul Branch agree, acknowledge and undertake that all information and data, including but not limited to any banking and customer-related information, provided pursuant to this Agreement by each party to the other party is confidential and proprietary information (**from now on "Confidential Information"**) of the disclosing party. No party shall use Confidential Information provided by the other party for any purpose other than as permitted or required for performance under this Agreement, or as otherwise agreed to between the parties. Each party agrees not to disclose or provide Confidential Information provided by the other party to any third party, without the express written consent of the other party, with the exception of (i) any affiliate or subsidiary with employees required to retain the confidentiality of the Confidential Information. (ii) employees who have a need to know in the course of performing services pursuant to this Agreement, provided that such employees are required to retain the confidentiality of the Confidential Information. (iii) subcontractors as necessary for GTS to deliver services to the Istanbul Branch under this Agreement, provided that employees of such subcontractors are required to retain the confidentiality of the Confidential Information. and (iv) each party agrees to take all reasonable measures, including, but not limited to measures taken by each party to safeguard the Confidential Information to prevent disclosure by employees, agents, or contractors. GTS further accepts and undertakes that the Istanbul Branch shall only disclose the Confidential Information to GTS only if it is necessary for the execution of the Agreement within the principle of proportionality under Article 73 of the Turkish Banking Law No. 5411 (the ''**Turkish Banking Law**'').

GTS agrees and undertakes to establish and maintain proper security measures and procedures to prevent unauthorized access or use of Confidential Information.
GTS agrees and undertakes to return to the Istanbul Branch, and destroy all copies of, all the Confidential Agreement and other data relating to the Istanbul Branch, its employees, and customers immediately after the Agreement expires or terminated and to keep it.

GTS agrees, acknowledges, and undertakes that any violation of its confidentiality obligation shall also constitute violation of Article 73 of the Turkish Banking Law. In case of any violation of this obligation or failing to show its best efforts to comply with thereof, Istanbul Branch is entitled to unilaterally terminate the agreement. In case of termination of the agreement by Istanbul Branch due to confidentiality violation of GTS, Istanbul Branch or the Banking Regulatory and Supervisory Board shall inform Public Prosecutors Office in writing.

A1 (b) Exceptions

Nothing provided herein shall prevent GTS or the Istanbul Branch from disclosing Confidential Information to the extent the Confidential Information (i) is or hereafter becomes part of the

public domain through no fault of either GTS or the Istanbul Branch. (ii) is rightfully received from a third party without similar restriction of the third party's rights. (iii) is independently developed by either GTS or the Istanbul Branch. (iv) is disclosed pursuant to the requirements of law. or (v) is already known to either GTS or the Istanbul Branch prior to disclosure.

A2 Compliance with Law

The Istanbul Branch is responsible to forward to GTS relevant Turkish laws, regulations and regulatory guidance pertaining to IT requirements and outsourcing, data protection/privacy, or other related matters set forth by Turkish laws, regulations or other law enforcement agencies that may affect this Service Level Agreement, with the aim to ensure GTS's prompt compliance with such requirements.

For the avoidance of doubt, GTS expressly acknowledges that the Istanbul Branch is a Turkish licensed branch supervised by the Turkish Banking Regulatory and Supervisory Board and is subject to Turkish laws and regulations. GTS agrees to provide the services set forth in this Agreement in compliance with all applicable Turkish legal and regulatory requirements, including but not limited to, Turkish Banking Law and Regulation on Bank's Procurement of Support Services (the ''**Support Service Regulation**'') and subject to the supervision of Turkish Banking Regulatory and Supervisory Board.

GTS agrees and undertakes to immediately (i) inform the Istanbul Branch if GTS encounters a security breach or data leakage in any of its systems or infrastructure that it uses to provide the services under the Agreement and (ii) provide the details of its plans to remedy such breach or leakage.

GTS expressly acknowledges, agrees and undertakes that in the event of assignment and transfer of any and/or all of its obligations and liabilities stipulated hereunder to a third party sub-contractor, it will ensure that such sub-contract agrees to be bound by the obligations attributable to GTS hereunder and GTS shall continue to be liable for the performance of such sub-contractor. GTS further acknowledges, agrees, and undertakes that it will enter into a written agreement with the new sub-contractor and such agreement shall expressly specify the subject and scope of the service to be provided, the term, the fees to be paid and the liabilities and obligations of the parties.

To prevent the Istanbul Branch's business continuity from being interreptud GTS agrees and undertakes:

- to ensure that its systems and procedures comply with the Istanbul Branch's risk management, security and customer confidentiality policies and its security principles and implementation is at least as protective as the Istanbul Branch's security principles and implementation.
- to take all necessary measures to prevent and incidents that may jeopardize the business continuity of the Istanbul Branch or otherwise harm the Istanbul Branch and its customers including security breaches and data leaks. and

- that the Istanbul Branch is entitled to (i) audit GTS in respect of the service provided by GTS hereunder and (ii) supervise GTS, to the extent necessary to ensure the compliance of accessibility, performance, and quality of the services with the standards under the

Agreement. and the requirements related to security control, security breach, operational and financial conditions, and any terms of this Agreement.

GTS further accepts and undertakes that GTS meets the requirements set forth for support service providers in the Support Service Regulation.

A3 Turkish Regulatory Authorities/Access to Information

GTS expressly acknowledges and agrees that it is subject to the Turkish Banking Regulatory and Supervisory Board's supervision in relation to the services it provides to the Istanbul Branch and that it will duly and timely provide any Turkish regulatory authority, including but not limited to Turkish Banking Regulatory and Supervisory Board, supervising the Istanbul Branch, pursuant to all applicable Turkish laws and regulations, as well as any internal and external Auditors full access to the databases, operational procedures, programs and logs belonging to the Istanbul Branch and any books and records relating to the arrangements covered by this Agreement, whether such materials are located in Italy or the Turkey.

GTS further agrees and undertakes to keep any and all electronic, magnetic and similarly kept data and any and all systems, passwords and decryptions required to review such data ready and accessible to any Turkish regulatory authority, including but not limited to Turkish Banking Regulatory and Supervisory Board, supervising the Istanbul Branch.

A4 Compliance with Document Retention/Preservation Notices

GTS expressly acknowledges and agrees that the Istanbul Branch has, or may have in the future, document retention or preservation notices or policies in place in connection with regulatory or law enforcement inquiries or litigation that may require different electronic data storing or archiving procedures than those otherwise set forth in this Agreement. GTS will provide its services pursuant to this Agreement in compliance with such document retention or preservation notices upon receipt of written notice from the Istanbul Branch regarding the existence and requirements of such notices.

A5 Audit

GTS expressly acknowledges and agrees that the Istanbul Branch is entitled to audit GTS limited to the scope of the support service provided by GTS under the Agreement, should it be necessary in connection with the banking activities and operations of the Istanbul Branch.

A6 Duration and Withdrawal Rights

This Agreement is effective from the date of acceptance, and it is automatically renewed on a yearly basis, unless either party exercises a withdrawal right upon three months advance written notice to the other party delivered by registered mail with return receipt.
In the event that the Agreement is unilaterally terminated by the Istanbul Branch as per the terms of the Agreement, GTS hereby agrees and undertakes to continue its obligations and responsibilities under the Agreement until the Istanbul Branch makes necessary arrangements to carry out such support services in-house or through a new support service provider and to submit the working papers and all necessary information to the substitute/new support service provider.

A7 Unilateral Termination

GTS expressly acknowledges, agrees and undertakes that should the board of directors of the Istanbul Branch deem that there are issues that hinder auditing or pose a risk as per the evaluation report to be prepared by the audit committee of the Istanbul Branch each year, or the Turkish Banking Regulatory and Supervisory Board restricts or bans procurement of support services, the Istanbul Branch is entitled to unilaterally terminate the Agreement.

A8 Assignment

Any assignment of this Agreement by one of the parties is subject to the prior written approval of the non-assigning party.

GTS expressly acknowledges, agrees and undertakes that in the event of assignment and transfer of any and/or all of its obligations and liabilities stipulated hereunder to a third-party sub-contractor, the provisions provided under this Schedule 1 shall also be accepted and undertaken by the new sub-contractor in writing.

GTS further acknowledges, agrees and undertakes that the written agreement to be executed with the new sub-contractor shall expressly specify the subject and scope of the support service to be provided, the term, the fees to be paid and the responsibilities and obligations of the parties.

A9 Fees

For the services under this Agreement, the Istanbul Branch shall not pay any fee to GTS.

We undersigned "**INTESA SANPAOLO S.p.A**" and **ITALYA ISTANBUL MERKEZ SUBESI** confirm to whom it may concern that the above reported Addendum for Istanbul Branch to the Service Level Agreement is in force and duly integrated in our internal processing procedures.

In witness thereof

Moncalieri, 2024

"**INTESA SANPAOLO S.p.A**"

Enrico Bagnasco

(Head of GTS in ISP - CDAITO GROUP TECHNOLOGY & SERVICES)

Istanbul, 2024

"**INTESA SANPAOLO SpA ITALYA ISTANBUL MERKEZ SUBESI**"

Ufuk Cemal Bali

(General Manager)

7 ADDENDUM SINGAPORE BRANCH

Addendum to the Service Level Agreement – International Network
Singapore Branch – December 2024

A1. Data Confidentiality
A1(a) General
GTS and the Singapore Branch agree that all information and data provided pursuant to this Agreement by each party to the other party is confidential and proprietary information (**from now on "Confidential Information"**) of the disclosing party. No party shall use Confidential Information provided by the other party for any purpose other than as permitted or required for performance under this Agreement, or as otherwise agreed to between the parties. Each party agrees not to disclose or provide Confidential Information provided by the other party to any third party, without the express written consent of the other party, with the exception of (i) any affiliate or subsidiary with employees required to retain the confidentiality of the Confidential Information. (ii) employees who have a need to know in the course of performing services pursuant to this Agreement, provided that such employees are required to retain the confidentiality of the Confidential Information. (iii) subcontractors as necessary for GTS to deliver services to the Singapore Branch under this Agreement, provided that employees of such subcontractors are required to retain the confidentiality of the Confidential Information. and (iv) each party agrees to take all reasonable measures, including, but not limited to measures taken by each party to safeguard its own confidential information to prevent disclosure by employees, agents, or contractors.

A1 (b) Exceptions
Nothing provided herein shall prevent GTS or the Singapore Branch from disclosing Confidential Information to the extent the Confidential Information (i) is or hereafter becomes part of the public domain through no fault of either GTS or the Singapore Branch. (ii) is rightfully received from a third party without similar restriction of the third party's rights. (iii) is independently developed by either GTS or the Singapore Branch. (iv) is disclosed pursuant to the requirements of law. or (v) is already known to either GTS or the Singapore Branch prior to disclosure.

A1(c) Privacy Policy
GTS and the Singapore Branch shall comply with the terms of their own privacy policies as indicated within the Singapore Branch Corporate Compliance Manual.

A2 Compliance with Law
The Singapore Branch is responsible to forward to Head Office relevant Singapore laws, regulations and regulatory guidance pertaining to IT requirements and outsourcing, data protection/privacy, or other related matters set forth by Singapore laws, regulations or other law enforcement agencies that may affect this Service Level Agreement, with the aim to ensure GTS's prompt compliance with such requirements.

A3 Regulatory Authorities/Access to Information
GTS expressly acknowledges and agrees that it will provide any Singapore regulatory authority supervising the Singapore Branch, pursuant to all applicable Singapore laws and regulations, as well as any Internal and External Auditors full access to the databases, operational procedures, programs and logs belonging to the Singapore Branch and any books and records relating to the

arrangements covered by this Agreement, whether such materials are located in Italy or Singapore. The purposes for which the foregoing access may be given, includes, but is not limited to:

(a) ensuring the continuity of the ongoing outsourced service;

(b) safeguarding the confidentiality and integrity of all information in GTS's custody, in relation to the provision of the ongoing outsourced service;

(c) managing Singapore Branch's legal, reputational, technological and operational risks arising from the provision of the ongoing outsourced service; and

(d) assessing the level of compliance of GTS with applicable laws related to the provision of the ongoing outsourced service.

A4 Access by Italian Authorities to Customer Data Managed by GTS

Pursuant to Italian law, the Fiscal, Administrative and Criminal Italian Authorities have the power to access all customer data existing in Italy. GTS by executing the outsourcing contract will manage some of the Singapore Branch's customer data in Italy. GTS will provide the Singapore Branch with three (3) business days' notice of any request from Italian authorities concerning the Singapore Branch's customer data, exception made for special circumstances that may require a faster response. The Singapore Branch will then be entrusted to report the event to its Singapore regulators. Within 14 business days' of such disclosure to the Italian authorities, GTS and/or the Singapore Branch shall also notify the Monetary Authority of Singapore of such disclosure of customer data to the Italian authorities.

A5 Compliance with Document Retention/Preservation Notices

GTS expressly acknowledges and agrees that the Singapore Branch has, or may have in the future, document retention or preservation notices or policies in place in connection with regulatory or law enforcement inquiries or litigation that may require different electronic data storing or archiving procedures than those otherwise set forth in this Agreement. GTS will provide its services pursuant to this Agreement in compliance with such document retention or preservation notices upon receipt of written notice from the Singapore Branch regarding the existence and requirements of such notices.

A6 Liability

In accordance with GTS incident and breaches management policy and provisions, GTS shall be liable for any damages in the event of any breach of security or confidentiality provisions under this Agreement. GTS agrees and undertakes to immediately (i) inform the Singapore Branch if GTS encounters a security breach or data leakage in any of its systems or infrastructure that it uses to provide the services under this Agreement and (ii) provide the details of its plans to remedy such breach or leakage.

A7 Duration and Withdrawal Rights

This Agreement is effective from 1 December 2024 and shall be automatically renewed on a yearly basis, unless either party exercises a withdrawal right upon three months advance written notice to the other party delivered by registered mail with return receipt.

In addition, the Singapore Branch may also terminate:

(i) if directed by its regulatory authority to terminate the outsourcing agreement or to stop receiving the outsourced service from GTS;

(ii) if GTS has failed to safeguard the confidentiality or integrity of customer information of the Singapore branch that is in the custody of GTS in relation to the provision of the outsourced service;

(iii) if there has been a demonstrable deterioration in the ability of GTS to safeguard the confidentiality or integrity of the customer information in its custody.

If the Singapore Branch terminates the outsourcing agreement or stops receiving the outsourced service provided by GTS, GTS shall ensure that all customer information given to GTS is deleted, destroyed or rendered unusable as soon as possible except where:

(i) GTS is prohibited from doing so by applicable laws, in the case where the outsourced service is performed overseas; or

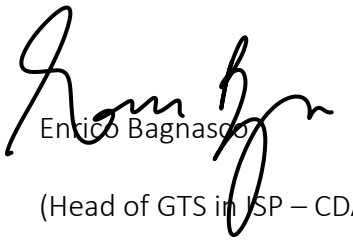
(ii) if (i) is not applicable, the record, document or information is stored in a system of GTS which, upon the termination of the outsourcing agreement, can only be accessed by the Singapore Branch.

We undersigned "INTESA SANPAOLO SPA - GTS" and "INTESA SANPAOLO S.P.A., SINGAPORE BRANCH" confirm to whom it may concern that the above reported Addendum for the Singapore Branch to the Service Level Agreement is in force and duly integrated in our internal processing procedures.

In witness thereof :

Moncalieri, 2024

"INTESA SANPAOLO S.P.A."



Enrico Bagnasco

(Head of GTS in ISP – CDAITO GROUP TECHNOLOGY & SERVICES)

Singapore, 2024

"INTESA SANPAOLO S.P.A., Singapore Branch"

Novella Burioli

(Chief Executive & General Manager)