SITA BORDER CONTROL SOLUTION

Technical Proposal for 10 ABC Gates to

State Enterprise 'Chisinau International Airport'

Date: 21st August 2025

Company Name and Contact Information

Company Details

Company	SITA Advanced Travel Solutions Limited
Division	Border Management
Website	www.sita.aero

Contact Details

Contact:	Dmitry Taranko
Title:	Senior Business Development Manager, Border Management Solutions
Mobile:	(+375) 29 603 65 52
Email:	Dmitry.Taranko@sita.aero

Correspondence Address

Address

Level 5, Block A-C, Apex,
Forbury Road, Reading,
RG1 1AX, United Kingdom

To the extent permitted under applicable laws or regulations, SITA reserves the right to request confidential treatment of the following: proprietary and confidential information; trades secrets; matters related to sensitive security information; and to national security.

TABLE OF CONTENTS

1. General requirements for the ABC System

1.1 The construction of the general ABC System must be in accordance with the practices recommended by ICAO and IATA as applicable.

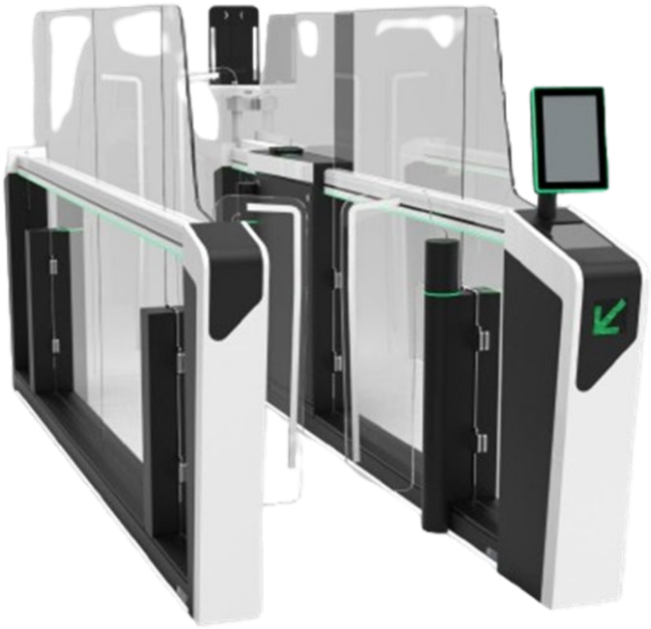
SITA Response: Compliant

The ABC System is fully designed and implemented in accordance with relevant ICAO and IATA guidelines. All applicable international standards and best practices have been followed to ensure compliance, safety, and interoperability.

1.2 The construction of the ABC System must be with 2 barriers/gates (entrance and exit) that perform the person control in two stages. Each stage must include a barrier with double gates.

SITA Response: Compliant

As shown in the image above, a two-stage person control is implemented at entry and exit. Each stage is equipped with a double-gate barrier configuration.



1.3 The construction of the ABC System must include features (including necessary sensors) to ensure that there will be no "tailgating" or "crossovers" during the process of passing through the ABC System.

SITA Response: Compliant

The system uses advanced sensors to detect and prevent tailgating and crossovers. Everyone is monitored to ensure only one person passes per authentication cycle.

1.4 Complete modularity of hardware for gate configuration single-row or multi-row

SITA Response: Compliant

Hardware is fully modular to support both single-row and multi-row gate configurations.

1.5 Sensors must be placed to detect and warn passengers about objects (e.g. luggage, etc.) left in the ABC System control area.

SITA Response: Compliant

Sensors detect objects left behind and trigger alerts within the ABC control area.

1.6 The construction of the ABC System must be an open design that avoids the feeling of imprisonment and claustrophobia and provides optimal visibility for the inspector.

SITA Response: Compliant

The system features an open design to prevent feelings of confinement and ensures clear visibility for inspectors.

1.7 The exit barrier must be of sufficient height so that the passenger who needs to pass the classic border control (at the counter) cannot bypass or jump over it.

SITA Response: Compliant

We confirm compliance: the exit barrier is designed with sufficient height to prevent passengers from bypassing or jumping over it when required to proceed to classic border control at the counter.

1.8 The construction of the ABC System must be safe for passengers, such as avoiding sharp objects/elements, smooth finishes, curved edges, etc.

SITA Response: Compliant

The ABC System is constructed with smooth finishes, curved edges, and safety-rated materials to eliminate sharp elements and ensure passenger safety.

1.9 All materials used in the ABC System must be certified for use in aviation terminals with regard to safety and health standards.

SITA Response: Compliant

All materials in the ABC system are certified for use in aviation terminals, meeting ICAO and IATA safety and health standards.

1.10 All electronic and mechanical components (such as circuit boards, motorized hinges, etc.) must be hidden where possible and kept safe.

SITA Response: Compliant

All electronic and mechanical components in the ABC System such as circuit boards, motorised hinges, and internal fittings, are concealed within vandal-proof metallic encasings and panels to prevent passenger access and ensure safety.

1.11 The construction of the ABC System must be resistant to vandalism, scratches and protected against foreign materials such as chewing gum, drinks, spilled water, cleaning fluids, etc.

SITA Response: Compliant

The ABC System uses scratch-resistant and vandal-proof materials. Exposed surfaces are engineered to withstand foreign substances and can be easily cleaned using soap and cloth.

1.12 In order to protect biometric data and travel documents processed by the ABC System, the Supplier will comply with the following minimum-security requirements:

SITA Response: Compliant-We acknowledge these requirements.

Cybernetics:

a. All communications between the ABC System and the IGPF IT infrastructure (including web services) will be secured through TLS 1.2 or higher protocols, using digital certificates issued by a recognized certification authority

SITA Response: Compliant

The ABC System ensures secure communication with the IGPF IT infrastructure including web services via TLS 1.2 or higher protocols. Digital certificates used for authentication and encryption are issued by trusted Certification Authorities (CAs) compliant with industry standards.

All external integrations (e.g., government systems) are managed through the Administration Portal, which enforces strict security policies, including mutual TLS, certificate validation, and encrypted data flows. The system supports secure APIs and maintains full audit logging of all communications for traceability and compliance.

b. Access to the administration interface and monitoring stations will be protected by multi-factor authentication (MFA) and role-based access control (RBAC) policies

SITA Response: Compliant

Access to both the ABC Administration Portal and Monitoring Client is secured using multi-factor authentication (MFA), requiring username and password as part of the login process.

Role-based access control (RBAC) is enforced, with clearly defined user roles restricting access to system functionalities based on operational responsibilities.

c. **All locally logged and captured data (images, logs, events) must be encrypted at the disk level (AES-256 or equivalent), with the possibility of configuring the retention period.**

SITA Response: Compliant

The ABC Gates system locally logs all audit and event data on the processor disk. The specification allows configurable retention periods for these logs to meet operational needs.

By default, the maximum retention period for locally stored audit and logging data is set to 7 days. Data stored locally at the disk level in compliance with EES and Frontex requirements, which typically mandate AES-256 or equivalent encryption.

d. **The supplier will ensure that all software components comply with "secure-by-design" principles and will be subject to penetration tests and security audits.**

SITA Response: Compliant

The ABC Gates system is developed following secure-by-design principles, with all software components subject to regular penetration testing and security audits. It operates within a secure architecture that integrates with backend risk and movement services.

Device configurations and security policies are centrally managed through the Administration Portal, ensuring compliance with Frontex “Best Practice Technical Guidelines for Automated Border Control (ABC) Systems.” This approach provides robust protection and continuous risk mitigation aligned with industry standards.

e. **The ABC system, including its software and hardware components, must be compliant with the requirements of Regulation (EU) 2016/679 (GDPR).**

SITA Response: Compliant

The ABC System is designed to fully comply with Regulation (EU) 2016/679 (GDPR), ensuring the protection of personal data across all software and hardware components.

f. **The supplier will present proof of compliance with the ISO/IEC 27001 standard for information security management.**

SITA Response: Compliant

We acknowledge this requirement. We confirm that the ABC Gates system is designed in accordance with the Frontex “Best Practice Technical Guidelines for Automated Border Control (ABC) Systems.” These guidelines explicitly incorporate ISO/IEC 27001 principles for information security management

2. General requirements for operating with the ABC System

Citizens of the Republic of Moldova, who have reached the age of 18 and are not accompanying minors, are the basic eligible category to cross the state border through the ABC System. Depending on the evolution of the regulatory framework, the General Inspectorate of the Border Police will decide whose citizens are eligible to use the ABC System. In this regard, the ABC System must provide flexibility and technical possibility to expand the categories of persons who can cross the state border using the ABC System.

SITA Response: Compliant

The ABC Gates system is designed to support flexible eligibility configurations, allowing authorities to define and update the categories of travellers permitted to use the gates.

The ABC System supports the current eligibility rules, allowing citizens of the Republic of Moldova aged 18 and above, who are not accompanying minors, to use the system. It provides the flexibility and technical capability to update and expand the eligible categories of users as defined by the General Inspectorate of the Border Police. Eligibility rules are configurable and managed centrally through the system's administration interface.

2.1 The ABS transition process (steps, actions/processes, information, communication API, information messages, other) will be developed jointly between the Beneficiary and the Bidder, but at the same time the Bidder will describe at least 2 different processes (transition processes used in other implemented projects, good practices)

SITA Response: Compliant

We acknowledge this requirement. The transition process will be developed jointly with the Beneficiary. Two reference transition processes from past projects will be provided during implementation, reflecting best practices**.**

2.2 Communication between the ABC system and the IGPF data and application server must be either through SOAP web services

SITA Response: Compliant

Communication between the ABC system and the IGPF data and application servers is implemented using SOAP web services, ensuring standardized and secure data exchange.

2.3 The information processes (applications) within the ABC System must save audit/logging data for all actions that take place in the border control process. The audit/logging data (in the form of files stored locally on the ABC System processor disk) must be kept for a maximum of 7 days.

SITA Response: Compliant

The ABC Gate system captures and stores audit and event data locally on the processor disk. These logs are retained for a configurable period, with a default maximum retention of 7 days.

2.4 Control/equipment requirements for the ABC System entry process: The first barrier (entry gates) of the ABC System must support the following operations/facilities:

SITA Response: Compliant

We acknowledge all the following requirements.

a. A biometric travel document reader, minimum technical requirements Annex 22

SITA Response: Compliant

The ABC System includes a biometric travel document reader that exceeds the minimum technical requirements specified in Annex 22.

b. A monitor/tablet (small size) intended for viewing information to guide the passenger during the biometric travel document reading process and to display the results (such as eligibility for use of the ABC System, etc.) based on the information received from the ABC System.

SITA Response: Compliant

The ABC System includes a compact tablet designed to guide passengers during the biometric travel document reading process and to display real-time results such as eligibility status based on system data. The entry door screen is positioned directly in front of the gate and functions as a tablet-style interface, providing clear instructions to travellers on passport positioning and displaying real-time notifications regarding entry permission. Likewise, the exit door screen guides travellers through the facial scan and exit procedures.

c. Entrance barrier (2 forward-opening gates) and sensors ensuring that only one person enters the second stage (in the “trap/work” area for people) when entry is permitted. The minimum technical requirements for sensors are described in the “Safety and Security” section.

SITA Response: Compliant

The entrance barrier consists of two forward-opening gates equipped with sensors that ensure only one person proceeds to the second stage (“trap/work” area) upon entry authorization. Sensor specifications comply with the minimum technical requirements outlined in the “Safety and Security” section.

2.5 Control/equipment requirements for the ABC System exit process: The second barrier (exit gates) of the ABC System must support the following operations/ features:

SITA Response: Compliant

The second barrier (exit gates) of the ABC System is designed to support all the following required operations and features.

a. **Hardware-software system for capturing the passenger's face image with the following minimum technical requirements (in accordance with ICAO requirements):**

SITA Response: Compliant

The ABC System complies with the minimum ICAO technical requirements for capturing passenger facial images.

i. **"Active life" detection based on 3D imaging technology.**

SITA Response: Compliant

The ABC System employs active life detection based on advanced 3D imaging technology to accurately verify the liveliness of the traveller during facial recognition.

ii. **Facial image capture must support (automatically adjust) the variable height of the passenger and be able to capture the image when the passenger is standing.**

SITA Response: Compliant

The cameras are fixed with no moving parts, but they feature a wide-angle lens and are positioned to cover a vertical range suitable for passengers between 1.20 m and 2.0 m tall.

iii. **The system must be equipped with a "digital mirror" to assist the passenger during image capture. At the same time, the passenger must receive necessary instructions on a monitor/screen including graphical instructions. All information provided must comply with "user-friendly" practices.**

SITA Response: Compliant

The ABC System includes a digital mirror to assist passengers during facial image capture. Passengers receive clear, step-by-step instructions, including graphical guidance on the integrated screen to ensure proper positioning and successful capture.

All passenger-facing information in the ABC System is designed according to user-friendly principles

iv. **The face capture algorithm shall continuously analyse the video stream from the camera to detect the passenger's face. Once the passenger's face is detected at the correct distance from the camera, a quality assessment algorithm (computer process) shall be run to verify that the facial image meets the minimum criteria based on ISO 39794-5 and ISO/IEC 19794-5:2011 "Face image (eye distance, blur, focus, position, expression)**

SITA Response: Compliant

The system uses real-time video analysis to detect the passenger’s face and automatically triggers image capture when the passenger is at the correct distance (0.8

m to 1.2 m). The ABC System's face capture algorithm continuously analyses the camera video stream to detect the passenger's face in real time. Once proper positioning is confirmed, a built-in quality assessment process verifies that the captured image meets the minimum criteria defined by ISO 39794-5 and ISO/IEC 19794-5:2011, including checks for eye distance, blur, focus, face position, and expression.

v. **The system must be equipped with an identity theft protection system, "Anti-spoofing Control", which will prevent attempts to present facial images, photographs or videos**

SITA Response: Compliant

The ABC System includes an identity theft protection feature with advanced anti-spoofing control. It prevents the use of fraudulent facial images, photographs, or videos by detecting and rejecting non-live presentations.

2.6 The system must have an emergency switch/button that allows the passenger to request assistance from the inspector. The emergency switch must trigger an alarm (audio and visual) but must not automatically release the barriers. The inspector must be able to open the entrance barrier using an "emergency button", which is not accessible to the passenger in the second stage of control.

SITA Response: Compliant

The ABC System includes an emergency switch/button accessible to passengers, which triggers both audio and visual alarms to request inspector assistance. Activation does not automatically release the barriers. Inspectors retain full control and can open the entrance barrier using a separate emergency button, which is not accessible to passengers during the second stage of control.

2.7 Information system intended for managing/operating all IT processes related to border crossing control in the ABC System must provide a large set of configurations for all stages.

SITA Response: Compliant

All ABC Gate device configurations are centrally managed through the Administration Portal, enabling flexible setup, updates, and operational control. The system also supports configurable workflows for verification, exception handling, and manual intervention, ensuring adaptability to various border control scenarios and policy requirements. The admin portal provides a wide range of configuration options, enabling comprehensive management of all IT processes related to border crossing control.

The admin portal provides a wide range of configuration options, enabling comprehensive management of all IT processes related to border crossing control. All ABC Gate device configurations are centrally managed through the Administration Portal, allowing flexible setup, updates, and operational control. It is designed to adapt to diverse operational scenarios and policy requirements.

3. Safety and security

3.1 The ABC system must have sensors that can detect a series of security-related conditions/requirements, including:

SITA Response: Compliant

The ABC System includes integrated sensors to monitor and detect multiple security-related conditions as listed in the following requirements**.**

a. The ability to differentiate between a walking adult or child, plus luggage hand, plus suitcases and bags on wheels (pulling or pushing).

SITA Response: Compliant

The ABC System supports the ability to differentiate between a walking adult or child, as well as recognize whether a passenger is carrying luggage by hand or managing suitcases and bags on wheels, whether pulling or pushing them.

b. The ability to detect multiple people (presence sensors, adult, child, adult with child in arms) entering the security area – tailgating.

SITA Response: Compliant

The ABC System employs presence sensors to identify multiple individuals entering the security area simultaneously, including adults, children, and adults carrying children, effectively preventing tailgating.

c. The ability to fully functionally detect tailgating (without additional overhead camera), based on artificial intelligence integrated into the vision system.

SITA Response: Compliant

The ABC System provides effective tailgating detection through sensors and integrated technologies within the gate infrastructure, ensuring accurate identification of unauthorized multiple entries without the need for additional overhead Camera. Additionally, the biometric camera integrated into the SITA Facepod performs multiple captures as part of the biometric identification and verification process, which reinforces security by incorporating multi-face detection functionality. The same Facepod also has a live streaming capability that provides border officers with an overview of the mantrap. All these features allow for efficient detection of tailgating.

d. The ability to have radar sensors integrated into the bottom for scanning door areas.

SITA Response: Compliant

The ABC System features integrated sensors located at the base of the doors to monitor and scan the passage areas.

e. **Ability to detect multiple passengers inside the ABC System (presence sensors), including adults with minors in their arms.**

SITA Response: Compliant

The ABC System can detect multiple passengers inside the ABC System (presence sensors), including adults with minors in their arms

f. **The ability to detect attempts to forcefully open entrance doors and output.**

SITA Response: Compliant

The ABC system can detect attempts to forcefully open entrance doors and output

g. **Ability to detect a passenger transiting in the wrong direction.**

SITA Response: Compliant

The ABC System can detect when a person attempts to re-enter or move in the wrong direction, effectively identifying transit against the permitted flow.

h. **Ability to detect luggage or other unexpected objects left on the in.**

SITA Response: Compliant

The ABC System can detect luggage or other unexpected objects left on the in. Sensors are configured to identify anomalies such as:

- Forgotten luggage
- Blocked doors
- Crawling or jumping
- Wrong-way fraud (inverse crossing)

3.2 **Optional: The ABC System must be equipped with CCTV cameras to provide the inspector with a clear view of the entire process of passing through the ABC System.**

SITA Response: Compliant

The ABC System uses CCTV cameras to give monitoring station inspectors a clear view of the entire process of passing through the ABC System

3.3 **The system must have a “Visual Signalling” system that provides color-coded visual signalling to display the operational status of the System, such as waiting for the next passenger, busy, inoperative (maintenance mode), alarm, etc. The colour codes must be established in consultation with the Beneficiary. The “Visual Signalling” can be through the use of a monitor/screen (small size) that needs to be installed at the first barrier.**

SITA Response: Compliant

Each ABC Gate is equipped with a visual signalling system, including LED pictograms on the entrance door (first barrier) that change colour to indicate gate status, such as green for available and red for unavailable or inoperative. The colour codes used in the system are configurable and will be defined in consultation with the Beneficiary, as required.

3.4 The ABC system must be designed to provide an average processing time of no more than 20 seconds per passenger.

SITA Response: Compliant

The ABC system provides an average processing time of no more than 15 seconds per passenger

4. Control and monitoring of the ABC System

4.1 The ABC system shall be equipped with a live monitoring station, located in a counter close to the ABC Systems. The monitoring station shall provide a detailed overview of the operational status of each ABC System and its performance data. Optional: the control panel shall include a video monitoring component providing live images from CCTV cameras. installed in/on ABC Systems

SITA Response: Compliant

The ABC System includes a live monitoring station located in a supervision booth near the gates. It provides a comprehensive overview of the operational status and performance of each ABC Gate, including real-time display of passport and biometric verification results. The monitoring station features live video feeds from integrated CCTV cameras installed on the ABC Gates, along with images from Face Pods and document scans under white light, infrared, and ultraviolet. Operators can remotely control gates, respond to alerts, and override gate decisions as required.

4.2 The monitoring station must allow the inspector to monitor and control a group of ABC Systems from a single workstation. A monitoring station must allow the inspector to view and manage up to 5 Systems at the same time.

SITA Response: Compliant

The monitoring station enables border officers to monitor and control a group of ABC Systems from a single workstation. Each station supports the simultaneous supervision of up to 6 gates. In the current solution scope, 2 monitoring stations are deployed to manage 10 ABC Gates.

4.3 The monitoring stations will be provided by the Bidder – 2 sets (system unit, monitor, keyboard, mouse, connection cables, UPS, licensed software).

SITA Response: Compliant

Two fully equipped monitoring stations will be provided by SITA. Each set includes a system unit, monitor, keyboard, mouse, connection cables, UPS, and all necessary licensed software.

4.4 Through the Monitoring Station, the inspector must have full control over the ABC System and be able to open both the entry and exit doors (the door will close automatically when the time expires or after the passenger passes), reset/restart and activate/deactivate the ABC System.

SITA Response: Compliant

The Monitoring Station provides inspectors with full control over the ABC System, including the ability to open and close both entry and exit doors, reset or restart the system, and activate or deactivate individual gates. Doors close automatically after the passenger passes or when the allowed time expires.

4.5 To ensure the efficient operation of the ABC System within the airport ecosystem, the Supplier will detail the following in its technical proposal:

i. how to integrate with existing systems, including:

- DCS (Departure Control System).
- AODB (Airport Operational Database).
- FIDS (Flight Information Display System).
- RMS (Resource Management System).

j. The proposed logical architecture of the integration, including data exchange (format, frequency, protocols) and fallback mechanisms in case of unavailability of external systems.

k. Clarifying responsibilities for connecting and operating the interfaces of the perspectives.

SITA Response: Compliant. SITA can meet this requirement (4.5) if it is required.

Please see below for further explanation on this. The exact arrangements can be agreed between the parties if it is required.

Based on our extensive global experience in deploying Automated Border Control (ABC) solutions, integration with airport operational systems such as Departure Control Systems (DCS), Airport Operational Database(AODB), FIDS (Flight Information Display System), RMS (Resource Management System) or Flight Dispatch Control is not typically implemented, nor is it required to achieve the core objectives of national border security.

In practice, governments maintain a clear separation between national border management systems and airport operational environments, as the latter are operated by airlines and airport authorities and are not part of the secure, government-controlled domain. In our assessment of Moldova’s border management and immigration processes, this approach remains consistent. The focus of the ABC solution is to ensure secure, reliable, and compliant processing of travellers under government control, without reliance on airport-side systems. Similar deployments in other countries confirm that national authorities prioritize independent, sovereign control of border automation, which avoids the risks and complexities of integrating with non-governmental airport systems.

At the same time, as an experienced provider, we always align with the requirements and priorities of our government customers. Should Moldova identify a need for integration with airport systems, our solution is flexible and can be adapted to support such functionality. This would, however, require dedicated design, development, and implementation effort, and can be addressed as part of a separate scope of work in close collaboration with the contracting authority.

4.6 Power on/off function with hidden switch (key).

SITA Response: Compliant.

The ABC System includes a secure power on/off function. A physical switch is located inside a locked cabinet at the exit door, accessible only with a key. The Gate PC can be shut down remotely via the monitoring station using a software control. If the gate is shut down manually or via Windows, it must be restarted using the designated hardware switch.

4.7 The main characteristics of the monitoring workstation must be:

SITA Response: Compliant.

The monitoring station complies with all specified requirements.

a. Viewing data taken from the biometric travel document, including the facial image from the CIP and the visual field (VZ, from the data page).

SITA Response: Compliant.

The workstation displays facial image from the CIP and the visual zone (VZ) from the data page.

b. Viewing, when necessary, images scanned by the travel document reader in all possible light spectra.

SITA Response: Compliant.

Images scanned by the travel document reader are viewable in white light, infrared, and ultraviolet.

c. Monitoring and control of the automatic facial recognition process, including viewing live captured images of the passenger and the possibility of performing manual recognition, if necessary.

SITA Response: Compliant.

The monitoring station allows inspectors to view live facial images captured during the automatic recognition process. In cases where the system is uncertain or a manual check is required, inspectors can intervene and perform manual recognition or override the automated decision.

d. In case of unsuccessful identity verification: possibility of configuring the system behaviour – either the person is forced to leave the gate or is detained until released by an officer.

SITA Response: Compliant.

In the event of unsuccessful identity verification, the ABC System allows configurable responses. The system can be set either to deny passage and prompt the passenger to exit the gate or to hold the passenger inside the gate until an officer intervenes and manually releases them.

e. **Possibility of releasing the person via key switch (separate for each line) or via border control software.**

SITA Response: Compliant.

Possibility of releasing the person can be triggered through the monitoring station software.

f. **Viewing the results of the facial recognition procedure. When the facial recognition score falls below the specified minimum value, the application displays alerts.**

SITA Response: Compliant.

The monitoring station displays the results of the facial recognition procedure in real time. When the recognition score falls below the configured threshold, the system generates alerts containing relevant passenger biographical data, categorized by cause such as biometric mismatch or watchlist hit, enabling prompt operator intervention.

g. **Viewing live video images from the facial camera.**

SITA Response: Compliant.

The monitoring station shows both the image extracted from the passport chip and the live video image captured by the Face Pods. This enables real-time comparison and manual override if needed.

h. **Real-time monitoring of border control processes, including the status of the ABC System.**

SITA Response: Compliant.

Operators can monitor and manage up to six ABC Gates at the same time. The system shows each gate’s operational status, whether active or inactive, as well as the results of ongoing biometric and document verification.

i. **Warning of alarm conditions and other notifications (e.g., tracking, abandoned objects).**

SITA Response: Compliant.

The system detects and alerts operators to exceptional situations, including attempted passage in the wrong direction, forced door opening, abandoned luggage, child protection cases, and excessive passage time.

Alerts are displayed on the supervision station interface, showing gate status and passenger flow. Notifications are categorized by unexpected gate conditions, passport or biometric verification failures, watchlist matches, and time limit breaches.

5. Training

5.1 The Bidder will provide adequate training for the Beneficiary's technical team regarding maintenance, how to detect and eliminate minor errors (software and hardware).

SITA Response: Compliant

We will have available relevant training for teams, focusing on maintenance procedures and the identification and resolution of minor issues through effective troubleshooting and recommendations. This knowledge will empower teams to effectively communicate findings to designated operational groups, ensuring that standard operating procedures are executed efficiently.

5.2 The Bidder will provide user manuals and technical documentation during the implementation of the ABC Systems.

SITA Response: Compliant

In addition to supplying comprehensive user manuals for our software to facilitate smooth onboarding and daily operation, we will provide manufacturer technical documentation to support all hardware components. These resources will be tailored to the deployed system, covering installation guides, configuration instructions, troubleshooting procedures, and maintenance recommendations. Documentation will be made available digitally, ensuring accessibility for technical staff and end-users alike. To further support knowledge transfer, updates to manuals and technical guides will be issued promptly following any system upgrades or modifications, maintaining clarity and accuracy throughout the lifecycle of the ABC Systems.

6. Maintenance and support requirements

6.1 The Bidder must provide a detailed preventive and corrective maintenance plan for the ABC Systems, including regular maintenance intervals and fault diagnosis procedures.

SITA Response: Compliant

Preventive Maintenance

- Execute preventive maintenance in accordance with **SITA or manufacturers' instructions,**
- Periodically inspect the equipment to ensure their working order (e.g., cabling, power),
- The Managed Service Guide (MSG) **specific to the relevant site will be used to identify and resolve issues,**
- Detail of **Preventive maintenance activities shown in table below**

Checklist for Preventive/Corrective Maintenance	
Daily Maintenance	Review previous day's Operations Shift daily status report.
	Review monitoring tool for any alarms (Notifications, Warnings etc.) including performance checks.
	Review operational emails for system alerts and notifications.
	Review ITSM Tool for Incident Creation and Status and update where applicable.
	Validate any alerts raised, relevant emails raised.
	Work on any open incidents, problems, and changes.
	Review previous day's Operations Shift daily status report.
Per Device	Visual inspection: Check for any obvious damage or wear and tear on the gate and surrounding areas. Look for loose or damaged components, obstructions, or unusual noises.
	Sensor check: Verify that all sensors are clean and functioning correctly. This may involve wiping down sensors and ensuring they are not blocked.
	Clearance check: Ensure there is sufficient clearance around the gate for proper operation and to prevent accidental contact.
	General cleaning: Wipe down the gate and surrounding areas to remove dirt, dust, or debris.

Checklist for Preventive/Corrective Maintenance	
	Check and clean physical device(s) surface with Isopropyl Alcohol (min 70%) on a cloth where surfaces are in contact with customer/user.
	As and when required: o Remove foreign objects (gum, paper, coins etc) from physical devices such as reader, camera etc. o Clean outer surfaces with non-chemical liquids, use a damp cloth, do not apply anything liquid direct to surface or equipment.
Daily Maintenance Server Room Where Applicable	Environmental Monitoring Activities (Room Temperature, Humidity, Water Leakage).
	Check server access (Virus Protection, Security Patch Management, System Auditing, Access User Policy Enforcement).
	Server health checks, disk space, memory, CPU, data processing state via monitoring toolsets.
	Database checks (such as table space, any database errors).
	Check backup status.
Document	At end of each activity document in the shift handover document ready for the team to email full daily status report for the morning shift.
Weekly Maintenance	Detailed inspection: Perform a more thorough inspection of all components, including the motor, drive mechanism, and control system.
	Lubrication: Apply appropriate lubricants to moving parts as per manufacturer recommendations.
	Sensor calibration: Calibrate sensors to ensure accurate and reliable operation.
	Software updates: Check for and install any available software updates for the gate's control system.
	Operational testing: Test the gate's functionality under different conditions to ensure it is working as expected.
Document	Record details of checks in Shift Handover document.
Monthly Maintenance	Component replacement: Replace any worn or damaged components, such as belts, rollers, or sensors, as per the maintenance schedule.
	System diagnostics: Run diagnostic tests on the control system to identify any potential issues.
	Emergency stop function test: Test the emergency stop function to ensure it is

Checklist for Preventive/Corrective Maintenance	
	working correctly.
	Have Power supply checked: Verify the power supply is functioning correctly and that all connections are secure.
	Incident review, look for repeated issues and generate associated Problem Ticket in ITSM Tool
	Generate any statistics for monthly reporting (SLA Report)
	Knowledge sharing within the team
	Server/Storage/Network Equipment Firmware/Drive Code Patch Review/Performance Review
	Monthly Operations Review Meeting (Review Incidents, Problems, CRs)
	Validate that monitoring agents are functioning correctly
	Check ABC PC such as fans to make sure clear of dust and dirt, vacuum where appropriate
Document	Record details of checks in Shift Handover document.
Quarterly Maintenance	WAN checks (configuration validation for high availability).
	Capacity review.
	Backup test restores.
	Asset Management Review
	Documentation review
	Review security policies
Document	Record details of checks in Shift Handover document.
Annual Maintenance	Backup media retention/distribution.
	Backup media replacements if applicable.
	Contract review.
	License & Certificate review.
	Service Benchmarking.
	Service Improvement Review

Checklist for Preventive/Corrective Maintenance	
	Production to Standby/DR failover test (Including Business Continuity)
	WAN checks (test resilience)
	Network and Security Policy Review
	Hardware Review
Document	Record details of checks in Shift Handover document.

Preventive Maintenance Check List

6.2 The Bidder will provide spare parts for all essential components of the ABC System throughout the warranty period and for post-warranty maintenance.

SITA Response: Compliant

SITA will supply, as per the supplier recommendations, spares for the warranty period of 3 years, and confirm that spare parts and essential components are made available up to 5 years after commissioning.

After the warranty expires, technical support and maintenance can be provided for a fee, based on these spare parts. The warranty period can be extended through additional negotiation in the maintenance contract.

6.3 If a major defect is identified that affects the normal operation of the ABC System, the Bidder will have to intervene to remedy the defect within a time frame established in the support agreement, usually no more than 72 hours.

SITA Response: Compliant

Here with SITA’s Incident response and Restore Times, along with Incident Priority levels.

Priority Code	Response Time	Update(s) to Customer(s)	MTTR
1	30 min	1hr	4 Hours
2	30 min	1hr	8 Hours
3	30 min	6hrs	1 Business Day
4	30 min	12hrs	2 Business Days
5	30 min	1 Day	5 Business Days

Priority Level	Description & Criteria	Priority Definitions
1	**Critical Impact on Business** Total system failure and interruption of business-critical applications affecting the entire system. Alternative or bypass is unavailable.	**A fault that seriously affects the normal daily operation and needs to be fixed at the earliest opportunity.** **Impact/Urgency: High/High** **For ABC Gates: 100% of devices would be unavailable.**
2	**Serious Impact on Business** Major Business Impact: Complete or partial service interruption of business-critical applications. Acceptable bypass is available.	**A fault seriously affecting the normal daily operation but not yet causing critical impact to the daily operation.** **Impact/Urgency: High/Medium or Medium/High** **For ABC Gates: 75% - <100% of devices would be unavailable.**
3	**Impact on Business Efficiency** Minor Business Impact: Partial service interruption of business-critical applications. Operational impact is minimal with no immediate impact on service operations. Alternative bypass is available.	**An incident which does not seriously affect the day-to-day operation. A workaround exists and/or the problem will be addressed in the next release of the Service Application.** **Impact/Urgency: High/Low or Medium/Medium or Low/High** **For ABC Gates: 50% - <75% of devices would be unavailable.**
4	**Inconvenience to the Business** Minimal Business Impact: Component, procedure, or personal application not critical to a customer is unusable. Alternative is available; deferred maintenance is acceptable (problems reported to suppliers). Impact to service operations minimal; possible minor inconvenience.	**Medium - partial service interruption with no impact on customer's operations.** **Impact/Urgency: Medium/Low or Low/Medium** **For ABC Gates: 0% - <50% of devices would be unavailable.**
5	**No Business Impact** No Business Impact: Non-service affecting faults or request to change. Alternative or bypass is not applicable.	**Low – Non-operational request (for information, request for change - rarely used)** **For ABC Gates: Experiencing intermittent issue(s).**

6.4 The Bidder shall provide ongoing training for the Beneficiary's technicians during the use of the ABC System, to ensure its efficient operation and safety.

SITA Response: Compliant

To ensure the efficient operation and safety of the ABC System, the bidder shall deliver ongoing training for the technical group through a multi-faceted approach. This includes organised shadowing sessions and practical demonstrations by experienced engineers, integrated within a training plan.

All manufacturer hardware documentation and SITA software user guides will be supplied, equipping technicians with essential reference material for both routine use and troubleshooting. In addition, 'train the trainer' guides will be made available, fostering effective knowledge transfer and enabling the beneficiary’s technical group to sustain their expertise over time.

7. Commissioning and periodic validation tests

7.1 Testing the full functionality of the system (document capture, facial identification validation, barrier access control, etc.).

SITA Response: Compliant

SITA will in collaboration with the customer, supply a UAT document that outlines all test cases to be executed, enabling confirmation that the requirements are addressed by the approved test cases.

The format of the test case is shown below and includes sections for detailed descriptions as well as comments from both SITA and the customer.

Example:

E-Gate Normal Workflow

Use Case # WF1	Successful E-Passport Passenger Processing
Scan e-passport. Enter gate. Face matching is successful. (The green LED on Facepod is lit throughout) Passenger exits gate.	
SITA Notes	
Customer Notes	

E-Gate Exception Workflow

Use Case # EW2		Travel document validation Technical Rules
		Scan the blank page on an EU passport. Resulting in no entry to the gate.
SITA Notes		
Customer Notes		

Monitoring Station

Use Case # MS1	Logon/Logoff
Login using credentials.	
SITA Notes	
Customer Notes	

7.2 Performance testing, to verify processing time and passenger throughput per minute.

SITA Response: Compliant

A performance test will be collaboratively planned and included in the UAT document. We need to confirm that the system can be tested both logistically and technically. Live passenger testing requires a fully operational system with appropriate environments, passengers, and passports. Thereafter, performance can be assessed using data from standard reports.

7.3 All tests will be documented in a test report which will be submitted to Beneficiary for validation.

SITA Response: Compliant

All testing activities will be recorded in a UAT document, which will include detailed test cases. Upon completion, after any feedback from both SITA and the customer, the document will be submitted to the beneficiary for validation.

7.4 To validate the interoperability, performance and compatibility of the ABC System with the existing infrastructure:

- **a. the supplier will implement a functional pilot installation for at least 1 ABC gate, including integration with the IGPF infrastructure and testing of biometric capabilities.**
- **b. the testing period will be at least 30 days, with documentation of all the results and any non-conformities.**
- **c. the full commissioning of the other units will be conditional on the formal acceptance of the PoC results by the Beneficiary.**

SITA Response: Compliant

A comprehensive test plan will be collaboratively developed with the customer and relevant stakeholders, encompassing the overall testing strategy, schedules, designated test cases, and required approvals. This plan will address and verify the following elements:

a) Utilisation of a single gate as a Proof of Concept prior to broader implementation, demonstrating both functionality and integration within the IGPF infrastructure.

b) Specification of the testing period, detailing all required tests and criteria necessary for completion, including both environmental and technical considerations; this can be accommodated but we consider this as hyper care if running in production and can be 120 working days. SITA will prepare all other gates for go-live during deployment and UAT signoff to ensure compliance with 120-working days timeline.

c) During acceptance of the single gate, full commissioning and go-live of all remaining gates will proceed in parallel which will allow for compliance of 120-working day timeframe.

8. Compliance requirements

8.1 All components of the ABC System must comply with ICAO (International Civil Aviation Organization) and IATA (International Air Transport Association) regulations.

SITA Response: Compliant

All components of the ABC System are designed and implemented to comply with ICAO and IATA regulations, meeting international standards for identity verification, document handling, and passenger processing.

8.2 The system must be certified for use in airport terminals, complying with safety regulations and fire safety standards.

SITA Response: Compliant

The ABC System is certified for use in airport terminals and complies with all applicable safety and fire safety standards. The equipment meets ISO 9001 quality requirements, and installation is aligned with airport authority approvals. The system can be integrated with fire detection and evacuation systems as defined during the design phase.

8.3 The Supplier will provide complete documentation regarding the API structure used by the ABC System (methods, parameters, responses, error codes, authentication).

SITA Response: Compliant

SITA will provide complete documentation of the API structure used by the ABC System, including detailed specifications for methods, parameters, responses, error codes, and authentication protocols for effective integration.

8.4 Functional and security testing methods applicable to APIs will be specified.

SITA Response: Compliant

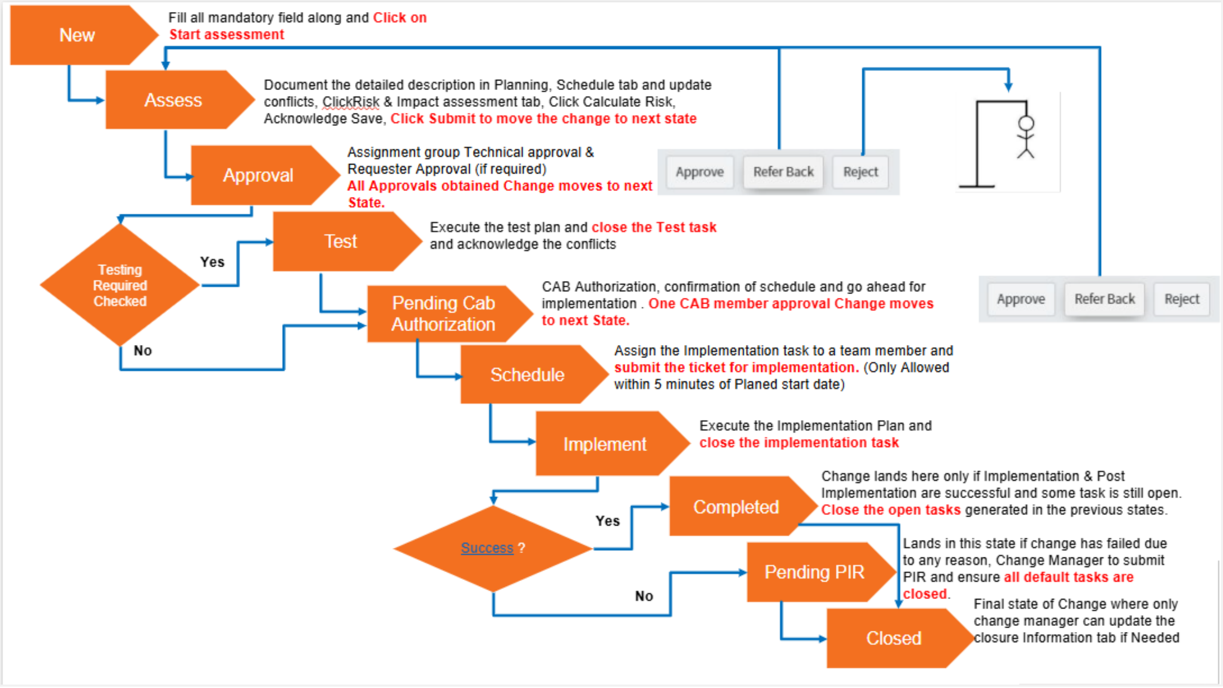
SITA do functional and security tests on our applicable APIs which includes WebInspect scan of all APIs in the solution. Once all API integration is completed for the solution we run in parallel functional testing and security testing. SITA can provide an applicable report from the WebInspect scan and functional tests.

8.5 The Supplier shall present a rollback plan in case of critical failure after an ABC software upgrade (including backups, recovery procedures, estimated duration).

SITA Response: Compliant

This will be part of SITA Change/Release management processes. Below is a detailed description of our processes:

SITA Change Management Process:



Fill all mandatory field along and Click on Start assessment

Document the detailed description in Planning, Schedule tab and update conflicts, ClickRisk & Impact assessment tab, Click Calculate Risk, Acknowledge Save, Click Submit to move the change to next state

Assignment group Technical approval & Requester Approval (if required) All Approvals obtained Change moves to next State.

Execute the test plan and close the Test task and acknowledge the conflicts

CAB Authorization, confirmation of schedule and go ahead for implementation . One CAB member approval Change moves to next State.

Assign the Implementation task to a team member and submit the ticket for implementation. (Only Allowed within 5 minutes of Planed start date)

Execute the Implementation Plan and close the implementation task

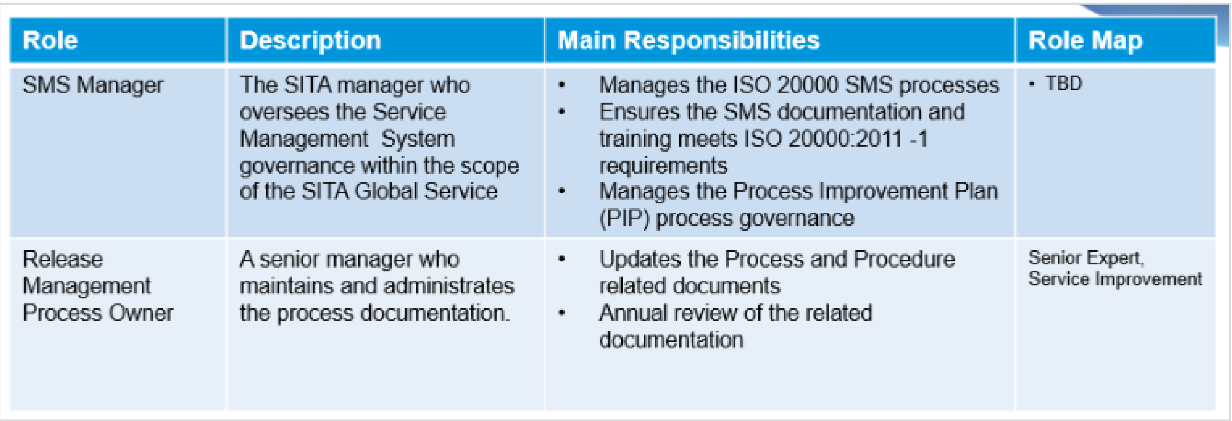
Change lands here only if Implementation & Post Implementation are successful and some task is still open. Close the open tasks generated in the previous states.

Lands in this state if change has failed due to any reason, Change Manager to submit PIR and ensure all default tasks are closed.

Final state of Change where only change manager can update the closure Information tab if Needed

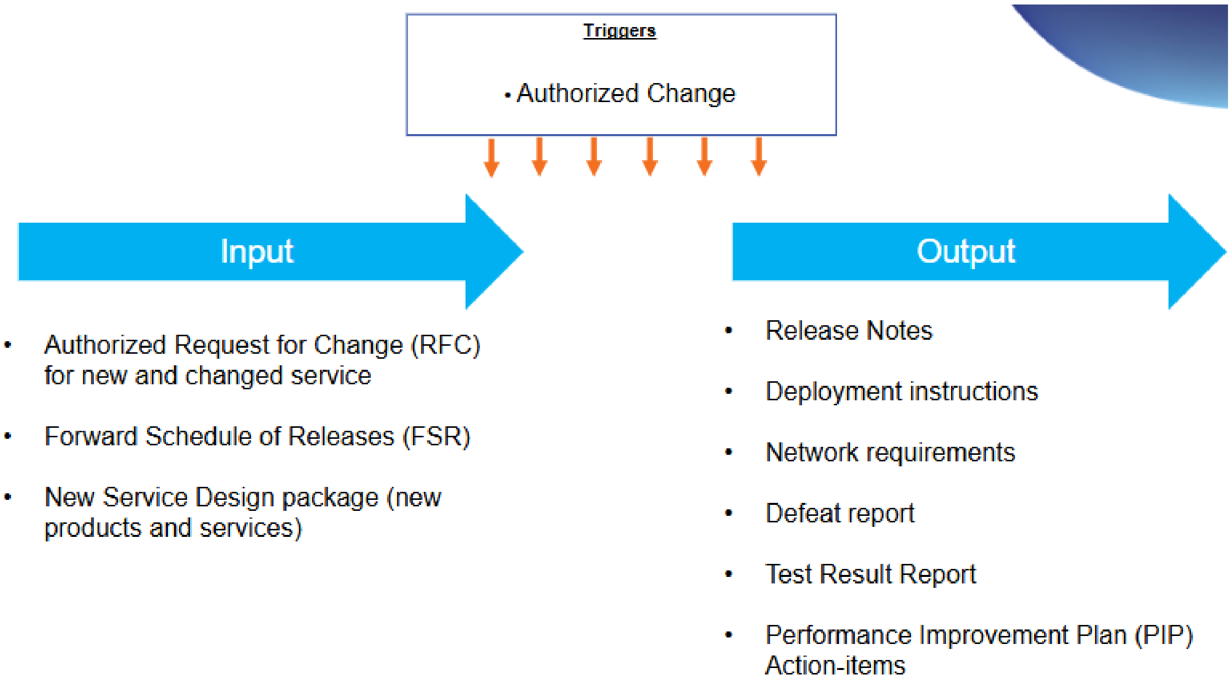
SITA Release Management Process: below figures details SITA's release management roles and responsibilities, triggers, inputs, and outputs, and release management best practice:

Roles and responsibilities:



Role	Description	Main Responsibilities	Role Map
SMS Manager	The SITA manager who oversees the Service Management System governance within the scope of the SITA Global Service	• Manages the ISO 20000 SMS processes • Ensures the SMS documentation and training meets ISO 20000:2011 -1 requirements • Manages the Process Improvement Plan (PIP) process governance	• TBD
Release Management Process Owner	A senior manager who maintains and administrates the process documentation.	• Updates the Process and Procedure related documents • Annual review of the related documentation	Senior Expert, Service Improvement

Triggers, Input, and Output:



Triggers

- Authorized Change

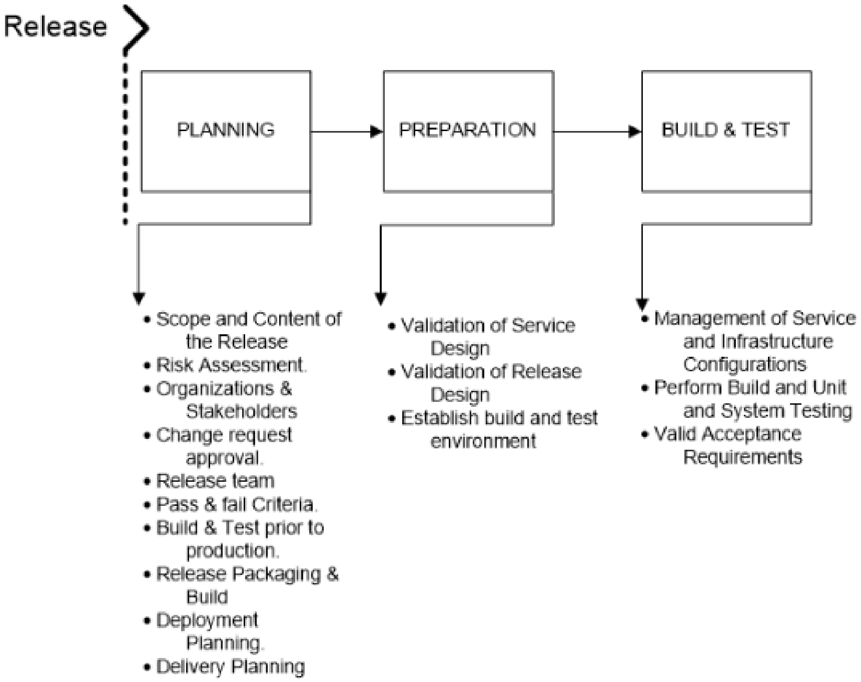
Input

- Authorized Request for Change (RFC) for new and changed service
- Forward Schedule of Releases (FSR)
- New Service Design package (new products and services)

Output

- Release Notes
- Deployment instructions
- Network requirements
- Defeat report
- Test Result Report
- Performance Improvement Plan (PIP) Action-items

Release management best practice:



Release

PLANNING

- Scope and Content of the Release
- Risk Assessment.
- Organizations & Stakeholders
- Change request approval.
- Release team
- Pass & fail Criteria.
- Build & Test prior to production.
- Release Packaging & Build
- Deployment Planning.
- Delivery Planning

PREPARATION

- Validation of Service Design
- Validation of Release Design
- Establish build and test environment

BUILD & TEST

- Management of Service and Infrastructure Configurations
- Perform Build and Unit and System Testing
- Valid Acceptance Requirements

9. Delivery and implementation deadlines

9.1 The Supplier will provide a detailed schedule for the delivery, installation and commissioning of the ABC Systems, which will include key milestones and deadlines for their completion.

SITA Response: Compliant

Please find below a detailed schedule for the delivery, installation and commissioning of the ABC system, including key milestones and deadlines**.**

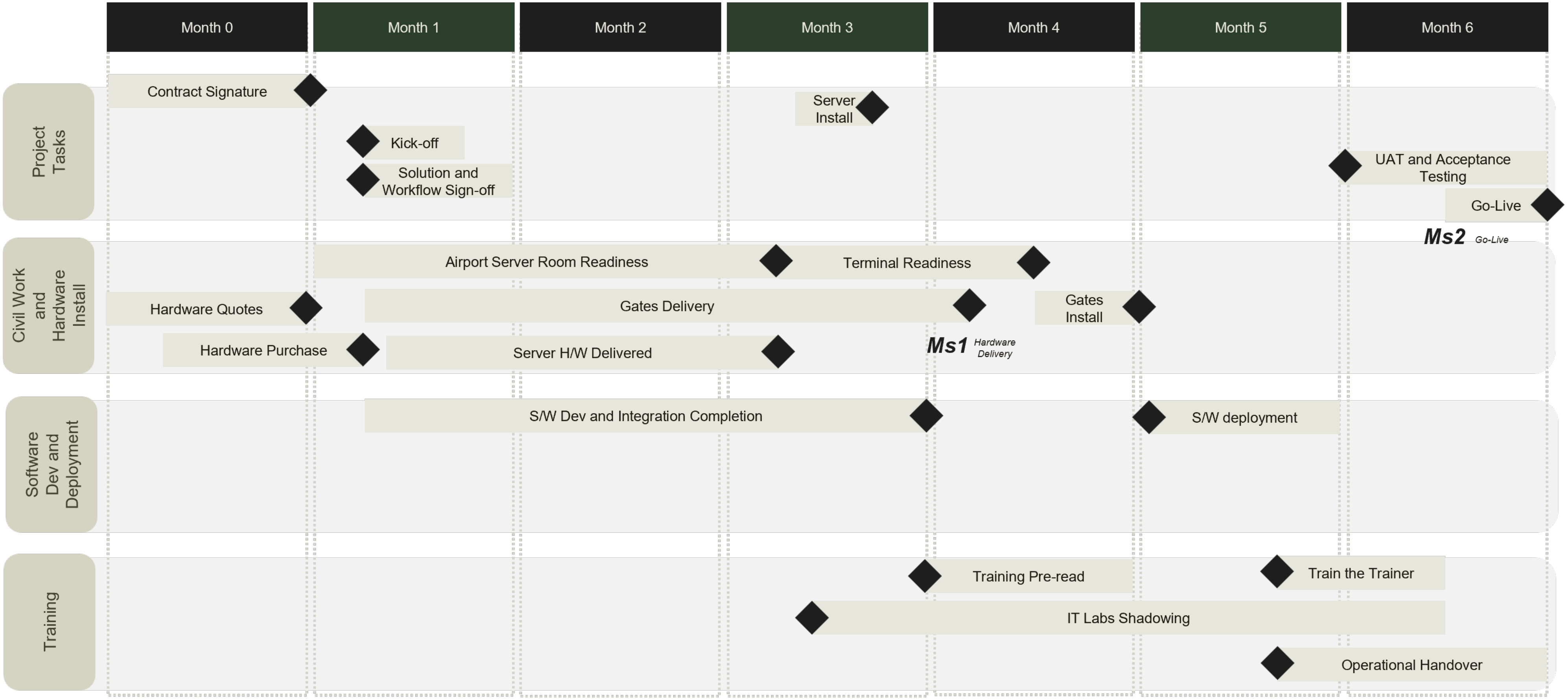
Refer to Section 5 of the proposal document for details on the project management methodology and Section 8.2 for information regarding dependencies and assumptions. The following schedule outlines the delivery timeline, including major milestones, deliverables, activities, and relevant dependencies and assumptions identified in Section 8.2 that may impact successful implementation.

Key Deliverables	Weeks	Activity	Dependencies	Key Assumptions
Signed Contract Project Team Established	W1	Project Kick-off & Contract Sign-off	-	A1 (Scope), A7 (Timely responses)
Detailed Workflow Document Requirement and Test Cases and Solution Design Document Signed-off Interface Control Document Provided from IDGF	W1	Solution & Workflow Sign-off	Customer Workflow & Requirements sign-off (D1)	A1 (Scope), A7 (Timely responses)
Purchase Orders for Hardware	W1	Hardware Purchase	Hardware manufacture and import (D4)	A2 (Logistics), A7 (Timely responses)
Airport Expansion Plan, Cable Diagrams, Gate Locations.	W1-W9	Civil Works Requirements & Planning	Customer Requirements for civil works (D2)	A3 (Civil works)
‘Milestone 1 ‘- Hardware including Servers and Gates delivered to site	W9-W13	Gates Delivery (Manufacturing & Shipping)	Hardware manufacture and import (D4)	A2 (Logistics) A8 (Storage)
Integration and Software Development Completion	W3-W12	Software Development & Integration	Product Development (D6)	A7 (Timely responses)
Server Infrastructure Ready	W9-W11	Server HW Delivered & Server Install	Server room availability for Server install (D3)	A4 (Airport Access), A6 (Server Set-up)

Key Deliverables	Weeks	Activity	Dependencies	Key Assumptions
ABC Gates Physically Installed	W13-W16	Gates Install	Customer Requirements for civil works (D2)	A3 (Civil works), A4 (Airport Access), A8 (Storage and Manoeuvring)
Software Deployment	W16-20	Deployment of gates software	Product Development (D6)	A4 (Airport Access), A5 (Environments), A7 (Timely responses)
Training Materials Reviewed, IT Labs Knowledge Transfer	W9-W24	Training Pre-read & IT Labs Shadowing	Appropriate Training resources (D5)	A4 (Airport Access), A7 (Timely responses)
Trained Border Officers & Trainers	W20-W24	Training Delivery & Train the Trainer	W13-W16 (IT Labs Shadowing)	A4 (Airport Access)
Signed Acceptance Testing Documents	W20-W24	UAT and Acceptance Testing	Acceptance Testing Availability (D4),	A1 (Scope), A5 (Environments), A7 (Timely responses)
‘Milestone 2’ - System Operational	W24 +4 working days.	Go-Live	W20-W24 (UAT and Acceptance Testing)	A1 (Scope), A5 (Environments)

High Level Estimated Delivery Timeline

(Representing 4-weeks per month



Month 0

Month 1

Month 2

Month 3

Month 4

Month 5

Month 6

Project Tasks

Contract Signature

Server Install

Kick-off

Solution and Workflow Sign-off

UAT and Acceptance Testing

Go-Live

Ms2 Go-Live

Civil Work and Hardware Install

Airport Server Room Readiness

Terminal Readiness

Hardware Quotes

Gates Delivery

Gates Install

Hardware Purchase

Server H/W Delivered

Ms1 Hardware Delivery

Software Dev and Deployment

S/W Dev and Integration Completion

S/W deployment

Training

Training Pre-read

Train the Trainer

IT Labs Shadowing

Operational Handover

9.2 Maximum term for the installation and full commissioning of the Systems ABC is 120 days from the signing of the contract.

SITA Response: Compliant

Total Duration: The high-level project plan spans an estimated 24 weeks, culminating in the 'Milestone 2' - System Operational (Go-Live).

Working Days Calculation: When accounting for a standard five-day work week and incorporating known public holidays in Moldova in the expected time period (December 25, 2025; January 1, 2026; January 7, 2026; January 8, 2026) within this period, 24 weeks translates to approximately 116 working days, allowing some contingency.

10. Reporting and documentation requirements

10.1 The Supplier must provide detailed reports on the progress of the project, updates on testing and validation, as well as any delays or problems that may arise during implementation.

SITA Response: Compliant

SITA operates under a strict governance structure with monthly project reviews, risk management methodology and steering committees, the communications plan will specify the frequency and audience of governance meetings and status updates.

The Project Management Plan will outline the baseline schedule, risks, assumptions, and dependencies, all tracked by project teams. Any issues or delays will be addressed collaboratively and transparently to find solutions.

10.2 All documents and reports must be provided in English and Romanian.

SITA Response: Compliant

All required documents and reports will be provided in both English and Romanian.

10.3 Upon completion of the implementation, the supplier will deliver complete documentation regarding the system architecture, operational procedures, user manuals and maintenance guides.

SITA Response: Compliant

We confirm compliance with the requirement to deliver complete documentation regarding the system architecture, operational procedures, user manuals, and maintenance guides upon completion of the implementation.

11. Obligation of the Final Beneficiary

(General Inspectorate of the Romanian Police) Frontier)

11.1 IGPF will publish a set of APIs (SOAP web services) to be consumed/accessed by the ABC System for authorizing the passage of automated border control by the passenger.

SITA Response: Compliant

The ABC System is designed to integrate with external services via SOAP web services. It will consume the set of APIs published by IGPF to authorize passenger passage through automated border control.

12. Log retention policy

12.1 The ABC system will retain logging data (system logs, access logs, captured images) for a minimum period of 30 days, with the possibility of extension or automatic archiving.

SITA Response: Compliant

The ABC System complies with the requirement to retain all relevant logging data, including system logs, access logs, and captured images, for a minimum of 30 days. The system also supports configurable retention settings, allowing for extension of the storage period or automatic archiving based on operational needs and policy requirements.

12.2 Secure deletion policies will be configurable, in accordance with the Beneficiary's internal policies and the provisions of the GDPR

SITA Response: Compliant

The ABC System supports configurable secure deletion policies, aligned with the Beneficiary’s internal regulations and fully compliant with GDPR requirements for data protection and retention.

13. Minimum technical requirements for the biometric travel document reader

Device for automatic reading of the entire data page of the biometric travel document, without removable parts, intended for reading data from: the mechanizable zone (MRZ); the visual zone (VZ); the wireless electronic identification circuit (RFID); the barcode, comparing the read data, verifying the authenticity of the travel document through the possibility of scanning the data page under different light spectra (White, IR, UF, coaxial, OVD, others).

SITA Response: Compliant

The ABC System includes a fully integrated document reader without removable parts, capable of automatically reading the MRZ, VZ, RFID chip, and barcode from biometric travel documents. The reader supports multi-spectrum scanning (white, infrared, ultraviolet, coaxial, OVD, etc.) to verify document authenticity and ensure accurate data extraction. The document reader complies with the minimum technical requirements specified and detailed in Annex 22.

Full technical specification requested by the contracting authority	Full technical specification proposed by the bidder	Standards Reference	SITA Response
Scanning area — the entire passport page; Video sensor type — CMOS; Colour representation — RGB Colour depth — 24 bits	Supports full-page scanning Video Sensor Type: CMOS 10MP Colour Representation: 36-bit RGB Colour depth:36 bits	ICAO 9303	Compliant with all requirements

Full technical specification requested by the contracting authority	Full technical specification proposed by the bidder	Standards Reference	SITA Response
The number of megapixels - 18, with the ability to set values from a list. The list must contain at least 3 values contained in 1..5, 5..10, 10..18; Contactless Identification Electronic Circuit Reader: Standards — ISO 14443: A and B for RFID-electronic circuits; Speed of information exchange — 106, 212, 424, 848 Kbaud Reading of electronic circuits – RFID located in any part of the travel document Anti-collision: detection/reading of the RFID electronic circuit after mechanolyzable area (MRZ) reading Reading and processing the image of format documents: ID-1, ID-2, ID-3 and other documents not exceeding the dimensions of 88x128 mm; Scanning process: Determination of the existence in the document reader device by sensor Automatic scanning of the document after the document has been detected; Removing Lights of reflection (glow) from laminate and holograms for the white and infrared light spectrum; Compensation of outdoor light exposure to image capture (photography) in the ultraviolet light spectrum (Smart UV); Automatic selection of ultraviolet illumination intensity for the type of documents processed; Determining (searching) and selecting images (photo, MRZ area, signature, data fields) from the total image of the document.	Megapixels: 10 MP fixed CMOS sensor; high-resolution capture scalable to 700 dpi Contactless Identification Electronic Circuit Reader: RFID Speed of Information exchange: 106, 212, 424, 848 Kbaud supported. Full-page RFID reading supported (no position restriction mentioned). Anti-collision (Post-MRZ Reading): Supported; the reader accurately detects and reads the correct RFID chip after capturing MRZ data. Reading and processing the image of format documents: Supports ID-1, ID-2, ID-3; documents up to 88×128 mm scannable with proper positioning. The Document Reader supports automatic document detection and initiates scanning immediately upon placement. It removes reflections from laminates and holograms under both white and infrared lighting. The device compensates for outdoor light during UV image capture using built-in UV illumination. Automatic UV intensity adjustment according to document type is supported to an extent. The reader also identifies and extracts key zones such as the photo, MRZ, signature, and data fields from the full document image.	Electronic Circuit Reader: MRZ Reading: Supported per ICAO 9303 RFID Reader Standard: ISO 14443 A & B supported	Compliant with all requirements

Full technical specification requested by the contracting authority	Full technical specification proposed by the bidder	Standards Reference	SITA Response
Mechanolyzable Zone (MRZ) Supported mechanizable area (MRZ) formats in accordance with ICAO 9303s standard. Search for the mechanolyzable area on the document image; Recognition in the white and infrared light spectrum; Verification of the control figures aimed at verifying the correctness of the completion of the mechanizable area in accordance with the requirements of ICAO 9303. Evaluation of correctness and print quality, in accordance with ICAO 9303 и ISO 7501, 1831, 1073-2 standards. Barcode reading: Formats maintained: 1D: Codabar, Code39 (+extended), Code93, Code128, EAN-8, EAN-13, IATA 2 of 5 (Airline), Interleaved 2 of 5 (ITF), Matrix 2 of 5, STF (Industrial), UPC-A, UPC-E 2D: PDF417, Aztec Code, QR Code, Datamatrix Determination automatic a document type Document Type Determination Sequence Country→Type→Series Receive the template from the SDK database Document For further processing: - placement of textual and graphic fields; - the existence of barcodes and protective elements; - verifying its authenticity and parameters; - existence of electronic circuits – RFID. RFID SDK/Functionality	Supports MRZ reading compliant with ICAO 9303 formats. Automatically detects and locates the MRZ area within the document image. Performs MRZ recognition using both white and infrared lighting. Verifies MRZ control digits to ensure data accuracy as per ICAO 9303 requirements. Evaluates MRZ print quality and correctness following ICAO 9303 and relevant ISO standards. Barcode reading: 1D:Supports Code128, Code39, EAN-8, EAN-13, IATA 2 of 5(Airline), Interleaved 2 of 5, Matrix 2 of 5, UPC-A, UPC-E; no explicit mention of Codabar and Code93. Support 2D barcode formats: PDF417, Aztec Code, QR Code, Datamatrix Determination automatic document type Supported via SDK which provides templates and enables placement, barcode and security element detection, and authenticity verification for further processing.	Industry standard 1D barcode formats Industry standard 2D barcode formats	Compliant with all requirements

Full technical specification requested by the contracting authority	Full technical specification proposed by the bidder	Standards Reference	SITA Response
Accepted standards for electronic circuits - RFID: - ISO/IEC 14443-2 (Type A and B) - ISO/IEC 14443-4 Data access regime: Direct, BAC, EAC, PEACE Authentication: Active (AA) Passive (PA) Electronic Circuit (CA v1, CA v2) Terminal (TA v1, TA v2) Application support: ePassport (DG1 – DG16), eID (DG1 – DG21), eSign; Certificate Management: Local storage; Obtaining certificates online through through the software interface; Master List Support, CRL Reading with Extended Length Support Reading of non-contact electronic circuits according to ICAO data formats LDS 1.7, PKI 1.1 Functionality Mandatory required security requirements: - Full tailgating detection functionality (without additional camera on top), based on artificial intelligence integrated into the vision system. - Radar sensors integrated into the bottom for scanning door areas. - Complete modularity of hardware equipment for single-row or multi-row gate configuration. - Power on/off function with hidden switch (key).	Data Access Modes: BAC, EAC v1/v2, PACE-CAM supported Authentication Types: All supported: Passive/Active Auth, CA v1/v2, TA v1/v2 via SDK Application support: Supports ePassport (DG1 – DG16), Supports eID (DG1 – DG16), Partial support for (DG17-DG21) esign: Supported indirectly via OCR and image capture enabling authentication and verification Certificate Management: Supported full certificate management including local storage, online certificate retrieval via software interface, Master List and CRL support, and extended length reading of non-contact electronic circuits. Functionality Mandatory required security requirements: Full Tailgating detection is achieved through integrated sensors within the system. Sensors positioned at the bottom scan the door areas to ensure secure access. The hardware is modular for single-row or multi-row gate configurations. Power on/off is controlled via a hidden key switch for security.	ISO/ICEC 14443-2 (Type A and B) ISO/IEC 14443-4 ePassport: ICAO 9303 LDS 1.7 & 1.8 eID: ISO/IEC 18013 parts 2 & 3 Certificate Management: ICAO LDS 1.7 PKI 1.1 ICAO 9303	Compliant with all requirements
In case of failure of identity verification: the possibility of configuring the behavior of the system – either the person is forced to leave the gate or is detained until release by an officer. The possibility of releasing the person by key switch (distinct for each line) or by means of the border control software. Analysis and comparison of textual information Areas of the document whose data will be analysed (compared): Mechanolyzable area visual area RFID Electronic Circuit Authenticity check luminescence check (UV Dull Paper): bench, MRZ area, photo placement area;	The system allows configurable actions on identity verification failure: either automatic ejection from the gate or detention until officer intervention. -Release can be controlled through the monitoring station software. Analysis and comparison of textual information: All supported via SDK – MRZ, visual area , RFID compared Authenticity check -Supports luminescence checks including UV inspection of the document surface and key areas like MRZ and photo. -Performs MRZ print contrast verification using near-infrared illumination compliant with ICAO 9303.	ICAO 9303 standard (IR B900 Ink)	Compliant with all requirements

Full technical specification requested by the contracting authority	Full technical specification proposed by the bidder	Standards Reference	SITA Response
MRZ print contrast verification according to ICAO 9303 standard (IR B900 Ink) Checks available after determining the document type: checking drawings of certain colours and shapes in the white, infrared and ultraviolet light spectrum (Image Pattern); checking the illumination of fibres of a certain colour and size (UV Protection Fibers) Checking for False Luminescence Checking the photo application method: print or paste (Photo Embedding Type) Infrared Visibility (IR Visibility) check: - blank elements textual data photography (basic and additional) checking for holograms(OVD) Reading text luminescent and comparison with the data read from the area MIZ or VIZ(OCR security Text) - Hidden Image Viewing (IPI) - Retroreflective protection check checking the barcode format.	Checks available after determining the document type: -Supports inspection of specific colour patterns and shapes under white, infrared, and ultraviolet light. -Detects UV protection fibres within documents. -Includes false luminescence detection capabilities. Photo Embedding Type: Print vs. paste detection Supported through image and layer analysis to distinguish print versus paste photo application using the SDK. Security Text: Supported ; OCR and luminescence comparison possible via SDK Infrared Visibility Check: IR visibility of blanks, text, photos, holograms Supported via infrared spectrum imaging and SDK detection of security elements like blanks, text, photos, and holograms. Hidden Image Viewing (IPI): Supported with IR/UV imaging and SDK Retroflective Protection: Supported via co-axial white light illumination Barcode Format Check: Supported for 1D and 2D barcode validation		Compliant with all requirements

14. Addendum: Integration with API/PNR Gateway

The proposed SITA ABC Gates solution is designed with flexibility to support integration with existing government systems. For Moldova, SITA has already deployed the API/PNR Gateway solution for the Moldovan Border Police, providing a strong base for seamless integration between the ABC Gates and the national border management systems.

Although integration with the API/PNR Gateway is not currently included in the proposal, the system architecture fully supports this through secure web services. This capability enables real-time data exchange with IGPF, ensuring compliance with national protocols and enhancing border security operations.

If the Moldovan authorities decide to move forward with this integration, SITA is fully prepared to plan and carry out the necessary development in a future upgrade phase. The ABC solution is designed for integration with the existing SITA API/PNR Gateway.

Digitally signed by Marinescu Mugurel-Costin
Date: 2025.08.22 16:54:57 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

SITA