

IGA QuickStart

Service Description

IGA QuickStart – is a Professional Services Engagement that rapidly enables Identity Governance and Administration (“IGA”) services by enabling the IGA platform’s integration with four (4) Client applications - including the source application - to provide automated Joiner (J) and Leaver (L) processes, access request processes with approval workflows, and access governance processes with access reviews. This Professional Services Engagement ensures that the IGA QuickStart services can be enabled on a maximum of two (2) environments.

Scope of IGA QuickStart

Simeio will:

1. Conduct a requirements verification workshop.
2. Validate the connectivity of the IGA platform in the non-production and production environments and provide information on the privileges required for the service account prior to application integration. (Limited to the OOTB connector applications only.)
3. Configure the automated lifecycle management service for application integration with the IGA platform for the Joiner and Leaver operations using OOTB functionality.
 - a. Joiner:
 - i. attribute generation limited to a maximum of two (2) attributes;
 - ii. process definition limited to a maximum of three (3) user type processes; and
 - iii. birthright rules definition limited to a maximum of ten (10) rules.
 - b. Leaver:
 - i. configure automated termination synchronization;
 - ii. configure deprovisioning process trigger; and
 - iii. configure user notification functionality.
4. Configure the “access request” process for the request-based application, either connected or disconnected, which includes establishing a request process, approval process, and request notifications functionalities using OOTB modules and features.
 - a. For the “request process”, enable the “access request” module; enable required request parameters, request entitlements, and application roles; and enable request access functionality for user accounts and on-behalf of other users.
 - b. For the “approval process”, enable up to two (2) levels of workflow.
 - c. For the “request notifications” functionalities, establish standard request notifications for both the requestor and the approver in the IGA platform.
5. Configure an “access governance” process for connected or disconnected applications using the user manager certification. This review will be enabled for the accounts and access with OOTB certification operations.
6. Closed loop remediation will be enabled for the applications which are connected using the IGA platform.
7. Enable user’s manager certifications to review accounts and review access.
8. Configure the standard certification process, which includes reviewing the scope of applications managed at the application and access levels; enabling an automated review cycle; enabling standard reminders for pending review functionality – limited to a maximum of three (3) reminders; enabling standard review of dates until expiration functionality, based on Client’s requirements and specifications; enabling standard reviewer action functionalities, which includes the capabilities to approve, revoke, or reassign a request, as well as the capability

to consult with another user, i.e., user's manager review; enabling a closed-loop remediation functionality, which includes the automated fulfillment task on connected applications, in case of access revocation, and the manual fulfillment task on disconnected applications.

9. Configure "delegated administration" on functionalities within the IGA platform, which includes the standard functionality to delegate administrative roles capabilities that are enabled with the OOTB IGA platform internal roles.
10. Password management will be enabled for the integrated applications using the OOTB password management capability.
11. Configure end user role functionalities, including self-service access request, view user profile and accounts, and set-up out-of-office (OOO) notifications with default OOTB configuration.
12. Configure manager/supervisor role functionalities, including end user role, 'on-behalf of requests' and certification/reviewer access.
13. Configure certification administrative role functionalities, including certification management.
14. Configure auditor role functionalities, including reports access.
15. Configure help desk role functionalities, including view all profiles and assign and request access.
16. Configure standard OOTB reports and dashboard functionalities, as well as reports modules for Access Request, Certification, LCM (Identity Warehouse) and automated job status in the IGA platform.
17. Configure IGA platform application login with standard options, including native user authentication and SAML based authentication when Client has the SSO product and configuration created.
18. Quality assurance testing of the implementation using Simeio standard tests and share the test results.
19. UAT assistance during the Client UAT cycle with a maximum duration of two (2) weeks.
20. Support Client change management process by developing required deployment document in the standard Simeio format.
21. Onboard the applications in the production environment once the change management is approved.
22. Ready applications to be onboarded in a non-production environment, with required configurations for the production environment, in the event of freezes or other interruptions.

Simeio Team Roles:

Role	Responsibility *
Project Manager	<ul style="list-style-type: none"> Oversee the Simeio project team. Report project progress to both Simeio and Client. Track adherence to in-scope activities. Primary point of contact for Client throughout the Engagement. Manage Deliverables schedule and dependencies. Review Deliverables prior to delivery to Client.
Business Analyst	<ul style="list-style-type: none"> Conduct requirements verification workshop and any additional workshops, as needed. Document requirement changes.
IGA Architect	<ul style="list-style-type: none"> Architecture and design review. Provide domain expertise.
Development team	<ul style="list-style-type: none"> Provide subject matter expertise and lead the overall implementation. Development of Deliverables.

Service Description



Quality Assurance Engineer	<ul style="list-style-type: none"> Integration and functional testing. Documentation and test reports.
-----------------------------------	--

* Simeio will provide support from our Global Delivery Centers, including in the United States, Canada, Costa Rica, United Kingdom, and India.

Deliverables

Deliverables*
Project Delivery: <ul style="list-style-type: none"> Use-case document Requirement document Technical design document Test cases and test reports Deployment document Run book

*Deliverables will be in standard Simeio formats.

Client Team Roles

Role	Responsibilities	Effort*
All stakeholders	<u>Requirement's verification workshop</u> <ul style="list-style-type: none"> The Client team is expected to participate in, discuss and provide direction during the requirements verification workshop. Client team will provide: <ul style="list-style-type: none"> Details of the environments and applications to integrate Trusted user profile attributes to be stored Target application attribute mapping Target application service account connection details based on the connector type used 	4 – 8 hours
Project sponsor	<u>Budget and License</u> <ul style="list-style-type: none"> Client ensures that the IGA platform is active before Simeio commences work on the IGA platform. 	2 – 4 hours
Project Manager	<u>Co-ordination and communication with stakeholders</u> <ul style="list-style-type: none"> Client organizes and engages all required Client teams to perform required changes on dependent services and applications. <u>Change management process</u> <ul style="list-style-type: none"> The Client is responsible for managing all Client processes, including change management and project management. Client is responsible for obtaining internal approvals, as required, from Client's change management team, which aligns with the Engagement Project Plan. 	60 – 80 hours
Datacenter operations + OS administrators	<u>Infrastructure readiness</u> <ul style="list-style-type: none"> IGA platform infrastructure must be made available at the beginning of the Engagement. 	4 – 8 hours

	<ul style="list-style-type: none"> Set up all required access to target and trusted applications, including login credentials for the Simeio team before the start of the Engagement. Client will provide all required SSL certificates. 	
Network engineers	<u>Network configuration</u> <ul style="list-style-type: none"> Must complete all network configuration between the IGA platform services and the Client's applications before the start of the Engagement. 	1 – 2 hours
Application Administrator	<u>Application and service configuration</u> <ul style="list-style-type: none"> Client domain administrator team(s) are expected to perform the required configuration on domain services for AD/domain-based authentication. Client technical team(s) are expected to perform any required changes in existing software, e.g., directory service. Client applications administrative team is expected to perform application side configuration for application integration. 	20 – 25 hours (4 – 5 hours per app)
UI-UX team	<u>Customization and branding</u> <ul style="list-style-type: none"> Client must make all required resources available for UI branding, including images, text messages, labels and so on, at the beginning of the Engagement. 	2 – 4 hours
Datacenter operations	<u>Infrastructure and service monitoring/maintenance</u> <ul style="list-style-type: none"> Client teams must monitor IGA platform's infrastructure throughout development. Report issues, outages, down-time and so on to the IGA platform support team directly. 	Continuous effort

* Indicated effort based on standard application and environment considerations. Level of effort may vary based on complexity of applications and services.

Client Responsibilities

Client will provide a single point of contact to act as Client Project Manager. On their own or in collaboration with other Client teams, the Client Project Manager will:

- Make product licenses available to Simeio at the beginning of the Engagement.
- Make the IGA platform available to Simeio at the beginning of the Engagement.
- Provide required access to the service account, source, and target applications within one (1) weeks' time from the date of request by Simeio.
- Produce system documentation of any current-state system that supports IAM capabilities or dataflow.
- Identify the applications for integration.
- Identify key Client-side internal stakeholders for the Engagement, including application owners, control managers and so on.
- Schedule required meetings with relevant representatives and furnish facilities, as needed.
- Schedule internal stakeholder meetings and workshop meetings with Simeio, as necessary.
- Schedule information gathering sessions and ensure attendance of Client-side personnel.
- Serves as the outreach mechanism for business contacts and executes activities based on the program's priority and at the pace prescribed by the program.
- Allocate support personnel to the project in a capacity for project management, integration support and delivery of Client-side resources.
- Responsible for deprecation of IAM tools and workflow processes, data retention and impact reporting.
- Support remediation effort within two (2) days from when data quality issues are identified.
- Schedule internal program management.

Service Description

- Furnish timely review and sign-off of Deliverables. Not more than two (2) days from the date of the document submission.
- Set up the SSO provider for the IGA platform for the single sign on.
- Facilitate customer-side change management and stakeholder communication on release management.
- Perform UAT of the functionality.
- Ensure the integrity of testing assets required to support the testing phase, including environments, development instances of applications or platforms, test data, obfuscation needs, tooling, and scheduling.

Engagement Pre-requisites:

- Active IGA platform with the latest version deployed.
- IGA platform connectivity to the Client network application, which includes on-premises or SaaS.
- Identify the IGA platform vendor customer success manager ("**CSM**") for any IGA platform related issues.

General Engagement Assumptions:

- Both the non-production and production environments for the IGA platform are available before the Engagement begins.
- All licensing and consents for any product are available/have been purchased.
- Current IAM initiatives not related to the IAM project will be placed on hold; Client IAM activities performed by Simeio take immediate priority over any other work.
- Functional and unit testing will be performed by Simeio using Simeio standard testing tools/processes.
- Deliverable feedback cycles will be limited to one revision cycle, where a cycle is defined as: initial submission, two (2) days for feedback and two (2) days for revisions to the initial submission.
- If required participants do not attend decision-making meetings, then their input will be logged as agreement to any design, process or policy design topic established in their absence.
- In the event there is any disagreement in approach or direction related to the Client effort, the SVP IT Ops/Risk and/or the Chief Information Security Officer (CISO) role-member will make a ruling within two (2) days of notification of such an issue.
- Gate reviews of any component of this effort may be expedited through emergency meetings outside of normally scheduled meeting frequencies.
- Not all design components need to be determined/finalized before initiating build activities.
- Applications and platform teams affected by the effort will support all requests for data or feeds used to input/update tooling for the effort.
- For applications leveraging IGA platform OOTB connectors, functionality is limited to that provided by the unmodified OOTB connector.
- Simeio is not responsible for data quality.
- An IAM leadership group will meet weekly for an initial period to support the effort; once a cadence has been identified and the program is underway a bi-weekly meeting with the IAM leadership may be introduced.
- If required, any level of leadership within the program will support requests from the program within two (2) days of receipt of any request.
- Client branding will be limited to the tool's configurable capabilities.
- Any additional services not contained herein will be subject to evaluation within the change control process.
- Any Client environment change management freeze periods that impact the Engagement timeline will either result in an increase of Fees due to the extension of the Term of the Engagement or any applications that have been configured, onboarded and passed UAT in the non-prod environment(s) will be considered accepted and Client will be billed as complete.

Engagement Exclusions

Everything not explicitly stated as in-scope is out-of-scope for this Engagement.

Definitions & Acronyms

Application	A computer program or software, which is being accessed by the intended users or another application over network (intranet or internet) using a unique web address (URL).
CR	Change Request
IAM	Identity and Access Management
IGA	Identity Governance and Administration
OOTB	Out of the Box – this is used to describe features that are native to an application and are configurable in nature, not features that need programmatic or developer assistance to realize.
SSO	Single Sign On
UAT	User Acceptance Testing
URL	Uniform Resource Locator: Web Address to access an application.
Verification workshop	Capturing the details on the functional requirements document using the workshop session with the Client application team. This meeting will be no more than six (6) hours over the course of two (2) to three (3) days for each application.