SAP Security Implementation and Redesign

1 Overview of Service

NTT will provide security consulting support to implement SAP Security in new SAP environments, redesign SAP Security in existing SAP environments, or roll out SAP Security for new company locations that are specified as in scope in the SOW and the specific service in System Design below must be elected in the SOW or will be considered out of scope.

2 System Design

2.1 Blueprints: Role Definitions

NTT consultants will work with Client functional team to create technical Role definitions, for which Client will be responsible for defining Role requirements. NTT will provide design workbooks and facilitate discussions as necessary in NTT's sole discretion. The design workbooks capture the following information:

(a) Baseline Role Definitions – Includes descriptions, owners, estimated number of users, and location-based restriction requirements.

(b) Restricted Data Requirements – Includes fields or screens containing data that is considered sensitive and requires restriction beyond the transaction level.

(c) Functional Mapping – Details what is mapped to each Role, including Transactions, Reports, SAP Fiori® Apps, and Web Services.

(d) Organizational Restrictions – Lists those fields that require restriction by location in Derived Roles and provides the set of restricted values for each location.

2.2 Additional Services for Security Redesign

If Client is licensed for NTT ControlPanel[GRC®] (CPGRC) Usage Analyzer[SM], NTT can assist in the functional mapping of Transactions to Roles. NTT will provide Client with an additional design workbook to map a sample set of existing users to Baseline Role definitions. NTT will use CPGRC Usage Analyzer data to identify the collective Transaction executions of these example users to propose a mapping of Transactions to Roles.

2.3 Segregation of Duty Analysis

If Client is licensed for CPGRC Risk Analyzer[SM], NTT will perform Segregation of Duty (SoD) validation on the security design before constructing Roles. This allows Client to review potential SoD risks and adjust functional mapping within Roles before development begins.

2.4 Realization: Role Construction and Validation

(a) Role Construction

The NTT consultants will construct Baseline Roles and Authorizations according to industry best practices. Baseline Roles are constructed as Single Roles and do not have Organizational restrictions.

(b) Initial Unit Testing

NTT will perform initial Role testing to ensure that Transactions within a Role can be started without encountering authorization defects. NTT will resolve defects that are identified or escalate to Client.

(c) Critical Transaction Testing

NTT will create test logons and deliver them to Client for Baseline Role testing. During testing, Client will perform positive and negative testing of critical transactions. NTT will resolve any defects that are identified during testing.

(d) Derived Role Construction and Testing

NTT will construct Organization-specific Derived Roles using the Baseline Roles as a template. NTT will create test logons and deliver them to Client for final positive and negative testing of Organizational restrictions. NTT will resolve any defects that are identified during testing.

(e) Cutover and Support

NTT will provide design workbooks for Client to complete final mapping of Roles to Users.

(f) Segregation of Duty Analysis

If Client is licensed for CPGRC Risk Analyzer, NTT will perform SoD validation on the final mapping of Roles to Users. This allows Client to see potential SoD risks and adjust Role mapping to Users before Role assignment begins.

(g) Additional Services for Security Redesign

If Client is licensed for CPGRC Emergency Access Manager[SM] (EAM), NTT will configure CPGRC EAM to allow users to restore their previous access in the event of a security issue after cutover. The use of CPGRC EAM reduces the risk during cutover and ensures that users can continue job responsibilities while any authorization issues are addressed.

(h) User Maintenance

NTT will create Users, assign Roles to Users, and/or remove existing Roles from Users based on the mapping workbook provided by Client.

(i) Go-Live Support

NTT will provide go-live support and troubleshooting for cutover weekend and up to one (1) week after cutover.

3 Operational Parameters

For all SAP Security Implementation and Redesigns services, Client must define the following:

(a) Baseline Role Definitions

(b) Restricted Data Requirements

(c) Functional Mapping

(d) Organizational Restrictions

(e) User/Role Mapping

4 Out of Scope

For every Role creation there is a maximum of four (4) revisions to the Role during the project. Additional revisions will be charged as a Role Modification. For more details on Role Modification revisions and charges, see Non Recurring charges.

5 Client Responsibilities

The SAP Security Implementation and Redesign services have certain roles and responsibilities defined as part of this Service Description. Client failure to fulfill its responsibilities may delay or prevent NTT from providing the service.

Client Responsibilities:

(a) Client must define Role requirements.

(b) Client must provide NTT consultants with appropriate access to maintain security model in Development systems and maintain users in other relevant systems.

(c) Client must provide NTT Security Consultant a Developer Key (if necessary).

(d) Client must perform their own SoD analysis on Role design and assignment of Users to Roles if the Client is not licensed for CPGRC Risk Analyzer.

(e) Client must validate Role modifications/creations via test logons and report any defects to NTT Security Consultant for resolution within thirty (30) days of delivery.

(f) Client must provide adequate advance notice of requested changes to allow for efficient scheduling of resources.

(g) Client must submit change requests to NTT Support Services by creating an incident using the CloudLink portal. These requests must include all pertinent details and are subject to standard NTT Support SLAs, applicable to the criticality of the request as defined by the NTT incident escalation/prioritization guidelines. All service requests are considered approved upon receipt. NTT is not responsible for gathering additional approvals for service requests.

6 Billing Parameters

All Monthly Recurring Charges (MRC) and Non-Recurring Charges (NRC) will be detailed in the applicable SOW. MRC does not begin until the services detailed on the applicable SOW have been provisioned and the environment is turned over to Client to begin using, sometimes referred to as Go Live, Handoff, Turnover, Ready Date, or Commencement Date. Client is not billed for implementation time, but may be billed for partial months after implementation is complete.

Monthly Recurring Charges	Non Recurring Charges
No MRCs are applicable for the SAP Security Implementation and Redesign Service.	SAP Security Implementation and Redesign Services are billed as a fixed price per Role specified in the SOW. Client is ultimately responsible for the number of Roles and therefore has control over the total cost of the project.

The following parameters are used to determine the total number of Roles billed to Client:

(a) Non-Organizational Baseline Roles that are constructed are billed separately for each production landscape where Roles are created. As an example, a “Buyer” Role constructed in ECC or S/4 is counted as a Role for billing. If a “Buyer” Role is also created in SRM, it is counted as a second Role for billing.

(b) Organizational Derived Roles that are linked copies of Baseline Roles are not subjected to Role construction billing.

(c) User Experience (UX) Roles that are created in Fiori/SAP NetWeaver® Gateway systems that are linked to a single Baseline Role are not subjected to Role creation billing.

Roles that are created with this service come with up to four (4) changes to the Role after construction is complete. These changes allow for Client to identify required modifications to Roles during various testing phases or after go-live. Role changes are calculated by counting the total number of Role modifications after Role construction.

The following parameters are used to determine the total number of Role changes.

(d) A request to change a Non-Organizational Baseline Role is considered to be one (1) change. Automatic changes to the linked Organizational Derived Roles are not counted.

(e) A request to change organizational values of a Derived Role is considered to be one (1) change.

(f) A request to change a User Experience (UX) Role in Fiori/Gateway system is considered to be one (1) change.

Client requested expedites are subjected to a charge.

Overage of Role Changes will be billed at the Role Modification rate outlined in the SOW.