

Managed SAP Security

1 Overview of Service

NTT will provide Managed SAP Security Services for Client's SAP security and controls environment. Delivery of Managed SAP Security Services is structured on a regular periodic basis. Services are generally provided in the following areas:

- (a) User Administration
- (b) Role Construction and Maintenance
- (c) Security Monitoring
- (d) Security Audit and Compliance Reporting

If Client incorporates NTT ControlPanel^{GRC®} into their Managed SAP Security solution, additional services are provided in the following areas if selected as In Scope in the SOW:

- (e) Risk Analysis and Remediation
- (f) Emergency Access Management
- (g) User and Role Change Management




1.2 Service Levels

NTT offers the following three types of service for Managed SAP Security, one of the following levels must be selected as in scope in the SOW or none shall be included:

- (a) SAP Security SafetyNet - Includes all Managed SAP Security services based on Client request, up to a predefined number of hours per month.
- (b) SAP Security Complete - Includes all Managed SAP Security services for a fixed monthly charge, and if applicable, leverages Client's governance, risk and compliance (GRC) tool to automate processes and provide compliance reporting.
- (c) SAP Security Complete PlusGRC - Includes all Managed SAP Security services for a fixed monthly charge, along with licensing of additional ControlPanelGRC software components to automate routine processes. NTT will:
 - (i) Provide a subscription to selected components of ControlPanelGRC Access Controls. The software license and use of these components is permitted for the duration of the agreement.
 - (ii) Install and configure ControlPanelGRC Access Controls in accordance with best practices and Client-specific processes within the current ControlPanelGRC .
 - (iii) Provide software maintenance for ControlPanelGRC, which entitles Client to technical support, bug fixes, and version upgrades. Additional training or consulting services are not part of software maintenance and are subject to additional charges.
- (d) Client must have an active license of ControlPanelGRC, have this option selected in scope in the SOW, and have an active SLMA or EULA with current maintenance agreement.

2 Service Design

Tasks legend:

- (a) Tasks marked as  are included in the service for the specified level.
- (b) Tasks marked as  are not included in the service for the specified level.
- (c) Tasks marked as  are available at Client Request. Assistance will be debited from Client's available block of SAP Security SafetyNet hours.

| Services | | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|---------------------|-------------------------------|---|------------------------|-----------------------|---|
| User Administration | End-User Logon Administration | Construct logons and distribute secure passwords to end-users. | ★ | ✓ | ✓ |
| | | Maintain Role assignments based on data owner approvals. | ★ | ✓ | ✓ |
| | | Execute Client change management logging process to provide audit ability of user master record changes | ★ | ✓ | ✓ |
| | | Troubleshoot end user authorization issues. | ★ | ✓ | ✓ |
| | | Provide secure password resets and lock or unlock user master records. | ★ | ✓ | ✓ |
| | | Classify users for evaluation in SAP System Measurement Report. | ★ | ✓ | ✓ |
| | | Delete inactive and unused logons to reduce SAP licensing costs. | ★ | ✓ | ✓ |
| | Support Logon Administration | Construct and maintain logons for Client's SAP Team Members in non-Production systems. | ★ | ✓ | ✓ |
| | | Manage emergency (that is, firefighter) access for Client's SAP Team Members in Production systems. | ★ | ✓ | ✓ |

| Services | | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|-----------------------------------|--|--|------------------------|-----------------------|---|
| Role Construction and Maintenance | Role Creation | Execute Client change control process to ensure approval by data owners. | ★ | ✓ | ✓ |
| | | Design and construct Roles based on business and audit requirements. | ★ | ✓ | ✓ |
| | Role Modifications | Execute Client change control process to ensure approval by data owners. | ★ | ✓ | ✓ |
| | | Maintain existing Roles based on business and audit requirements | ★ | ✓ | ✓ |
| | Role Validation | Construct test logons to permit validation of Role changes in appropriate test system. | ★ | ✓ | ✓ |
| | | Resolve security defects identified during Role testing. | ★ | ✓ | ✓ |
| | Role Documentation and Migration | Execute Client change management and audit history process for Role maintenance. | ★ | ✓ | ✓ |
| | | Execute Client transport management process for Role maintenance. | ★ | ✓ | ✓ |
| | Authorization Troubleshooting | Provide technical troubleshooting for complex authorization issues. | ★ | ✓ | ✓ |
| Security Monitoring | User Monitoring | Monitor and analyze relevant user activities. | ★ | ✓ | ✓ |
| | | Identify inactive logons and unused passwords. | ★ | ✓ | ✓ |
| | | Report system usage statistics based on Client procedures and requirements. | ★ | ✓ | ✓ |
| | | Validate system user passwords are not easily identified. | ★ | ✓ | ✓ |
| | Intrusion and Inappropriate User Detection | Detect and report unusual security violations as captured by the SAP Security Audit Log. | ★ | ✓ | ✓ |

| Services | | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|---|---|--|------------------------|-----------------------|---|
| | | Report transaction usage based on Client procedures and requirements. | ★ | ✓ | ✓ |
| | Authorization Monitoring | Monitor Transaction Start failures to identify both authorization and training issues. | ★ | ✓ | ✓ |
| | | Identify Remote Function Call execution failures. | ★ | ✓ | ✓ |
| Security Audit and Compliance Reporting | Periodic and Ad-hoc Authorization Reporting | Provide summary report of SAP Security administration activities using Client change log procedures. | ★ | ✓ | ✓ |
| | | Generate ad-hoc reports based on Client requests and queries. | ★ | ✓ | ✓ |
| | | Generate SAP System Measurement reports. | ★ | ✓ | ✓ |
| | Yearly Compliance Reporting | Provide reports to data owners detailing Role assignments to Users and Transaction assignment to Roles. | ★ | ✓ | ✓ |
| | | Execute Segregation of Duty (SoD) report based on Client's internal control structure. | ★ | ✓ | ✓ |
| | | Execute queries to determine Users or Roles with selected authorizations. | ★ | ✓ | ✓ |
| | Audit Advocacy and Support | Provide reports to authorized third parties (internal and external auditors). | ★ | ✓ | ✓ |
| | | Review and respond to Management Letter findings. | ★ | ✓ | ✓ |
| | Risk Analysis And Remediation | Install and configure software and related workflows. | ✗ | ✗ | ✓ |
| | | Execute monthly SoD report detailing risk changes during previous period and distribute to system and User Group owners for signoff in workflow. | ✗ | ✗ | ✓ |

| Services | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|----------|---|------------------------|-----------------------|---|
| | Review Client settings to identify instances where productive Client might be incorrectly unlocked for modification. | ✗ | ✗ | ✓ |
| | Automatically integrate risk analysis as Client makes changes to the security model (User changes in SU01 or Role changes in PFCG). | ✗ | ✗ | ✓ |
| | Execute monthly reports for Sensitive Role and Profile, Baseline Profile Parameter, and Passwords for Delivered User, and distribute to system owners for signoff in workflow. | ✗ | ✗ | ✓ |
| | Execute quarterly reports for Unused Role Assignment, Unused Transactions in Roles, and Unused Single Roles in Composite Roles, and distribute to system owners via workflow. | ✗ | ✗ | ✓ |
| | Change SoD Rulebook, Risk Owners, or User Group Owners per Client's request. | ✗ | ✗ | ✓ |
| | Change compensating controls to mitigate user risks per Client's request | ✗ | ✗ | ✓ |
| | Implement changes to SoD Risk Definitions (including Risk Owners), baseline Profile Parameters, Sensitive Roles and Profiles, and Compensating Controls based on Client's yearly review and stated requirements for changes, and set compliance calendar. | ✗ | ✗ | ✓ |
| | Send compensating control re-affirmation to control owners via workflow on a yearly basis to validate that controls are still active and effective | ✗ | ✗ | ✓ |
| | Execute License Optimization based on yearly review with Client and distribute to system owners via workflow. | ✗ | ✗ | ✓ |

| Services | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|---------------------------------|--|------------------------|-----------------------|---|
| Emergency Access Management | Install and configure software and related workflows. | ✗ | ✗ | ✓ |
| | Provision and de-provision elevated privileges automatically during emergency access periods. | ✗ | ✗ | ✓ |
| | Execute Emergency Access Session report per Client's request and distribute to appropriate monitors for signoff in workflow. | ✗ | ✗ | ✓ |
| | Combine all Emergency Access Session reports monthly and distribute to system owners for signoff in workflow. | ✗ | ✗ | ✓ |
| | Implement changes to emergency access configuration based on Client's yearly review of procedures and stated requirements for changes. | ✗ | ✗ | ✓ |
| User and Role Change Management | Install and configure software and related workflows. | ✗ | ✗ | ✓ |
| | Provision and de-provision per user change requests made via the ControlPanel ^{GRC} web-based self-service request system, which includes automatic integration to check for SoD risks. | ✗ | ✗ | ✓ |
| | Reset passwords per user change request made via the ControlPanel ^{GRC} web-based self-service request system. | ✗ | ✗ | ✓ |
| | Configure Role Owners for workflow approval purposes based on Client's request. | ✗ | ✗ | ✓ |
| | De-provision users on a weekly basis based on a predefined period of inactivity in Production systems. | ✗ | ✗ | ✓ |
| | Execute User Change and Role Change reports on a periodic basis, and submit to system owners for signoff in workflow. | ✗ | ✗ | ✓ |

| Services | Tasks | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|----------|--|------------------------|-----------------------|---|
| | Execute User and Role Re-Certification reports on a yearly basis, and submit to system owners for signoff in workflow. | ✗ | ✗ | ✓ |
| | De-provision users based on Client's yearly review of User and Role Re-Certification processes and stated requirements for change. | ✗ | ✗ | ✓ |
| | Make changes to Role Transactions or Single Roles (in Composite Roles) based on Client's yearly review of User and Role Re-Certification processes and stated requirements for change. | ✗ | ✗ | ✓ |
| | Provide list of Roles assigned in Production system on a yearly basis and based on Client's review and stated requirements for change, configure the Roles for use in workflow engine. | ✗ | ✗ | ✓ |
| | Update User and Role change management workflows on a yearly basis per Client's review and stated requirements. | ✗ | ✗ | ✓ |

3 Operational Parameters

For SAP Security services, Client must define the operational parameters included in the table below for the selected in scope service level:

| Service Level | Operational Parameters |
|------------------------|---|
| SAP Security SafetyNet | Authorized approvers for change requests. |
| | Monthly reporting requirements for Security Monitoring, including desired recipients and reasonable Client-specific input where required. |
| SAP Security Complete | Authorized approvers for change requests based on Roles or Business Locations. |
| | Change management processes for User and Role Changes. |
| | Monthly reporting requirements for Security Monitoring, including desired recipients and reasonable Client-specific input where required. |
| | Elevated Access processes for Support Logons, including specific logging requirements and access to be assigned as part of emergency access processing. |
| | SoD report/GRC tool for execution of yearly compliance reporting, including desired data owners and specific query input requirements. |

| | |
|---|--|
| SAP Security Complete Plus ^{GRC} | Authorized approvers for change requests based on Roles or Business Locations. |
| | Change management processes for User and Role Changes. |
| | Monthly reporting requirements for Security Monitoring, including desired recipients and reasonable Client-specific input where required. |
| | Elevated access rights and approvers for Support Logons (managed in Emergency Access Manager), including specific logging requirements and access to be assigned as part of emergency access processing. |
| | SoD rules required to be checked within ControlPanel ^{GRC} Risk Analyzer SM . |

4 Out of Scope

Managed SAP Security services do not include projects, such as additional implementations, upgrades, and compliance remediation efforts.

- (a) Additional SAP Security Implementations or Deployments - Security consulting support to implement SAP Security in new SAP environments, redesign SAP Security in existing SAP environments, or rollout SAP Security for new company locations.
- (b) SAP Security Upgrades - Security consulting support for Client's SAP upgrade.
- (c) Compliance Remediation for SAP Security - Consulting activities to assist Client in remediation of SAP Security and controls issues, as may be identified in an NTT assessment report, Management Letter Findings of an internal/external auditor, or other SAP Security issues document.

5 Client Responsibilities

- 5.1 Client failure to fulfill its responsibilities may delay or prevent NTT from providing the service.

| Service Level | Client Responsibilities |
|------------------------|--|
| SAP Security SafetyNet | Client will establish an IPSEC VPN tunnel between NTT and the location where Client systems reside, to allow for reliable systems monitoring and rapid response to automated alerts and Client requests. |
| | Client will provide three (3) privileged access accounts (one each for SAP Security, Service Desk, and Systems), to allow for system access by NTT consultants. |
| | Client will provide adequate advance notice of requested changes, and if contracted for, project work, to allow for efficient scheduling of resources. |
| | Client will submit change requests to NTT Support Services by creating an incident or request 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. |
| | Client will provide NTT consultants with appropriate access to maintain security model in Development systems and maintain users in other relevant system. |
| SAP Security Complete | Client will provide documented processes and/or tools required for all services, such as provisioning, SoD checking, and emergency access. |
| | Client will establish an IPSEC VPN tunnel between NTT and the location where Client systems reside, to allow for reliable systems monitoring and rapid response to automated alerts and Client requests. |

| | |
|---|--|
| | Client will provide three (3) privileged access accounts (one each for SAP Security, Service Desk, and Systems), to allow for system access by NTT consultants. |
| | Client will provide NTT consultants with appropriate access to maintain security model in Development systems and maintain users in other relevant systems. |
| | Client will provide adequate advance notice of requested changes, and if contracted for, project work, to allow for efficient scheduling of resources. |
| | Client will submit change requests to NTT Support Services by creating an incident or request 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. |
| SAP Security Complete Plus ^{GRC} | Client will provide documented processes and/or tools required for all services, such as provisioning, SoD checking, and emergency access. |
| | Client will establish an IPSEC VPN tunnel between NTT and the location where Client systems reside, to allow for reliable systems monitoring and rapid response to automated alerts and Client requests. |
| | Client will provide three (3) privileged access accounts (one each for SAP Security, Service Desk, and Systems), to allow for system access by NTT consultants. |
| | Client will provide adequate advance notice of requested changes, and if contracted for, project work, to allow for efficient scheduling of resources. |
| | Client will submit ninety percent (90%) of all security requests via ControlPanel ^{GRC} within sixty (60) calendar days of start of service delivery |
| | Client will provide NTT consultants with appropriate access to maintain security model and ControlPanel ^{GRC} in Development systems and maintain users in other relevant systems |
| | Client will submit service requests to NTT Support Services using ControlPanel ^{GRC} or by creating an incident or request 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. Symmetry is not responsible for gathering additional approvals for service requests |

6

Charges

| Charges | SAP Security SafetyNet | SAP Security Complete | SAP Security Complete Plus ^{GRC} |
|-------------------|--|--|---|
| Monthly Recurring | Client will subscribe to a set amount of hours per month specified in the SOW. These hours must be consumed within the month and cannot be carried over to future months. If Client consumes more than 125% of | Client will subscribe to services based on a predefined number of managed users as specified in the SOW. Managed users are calculated based on the sum of named user counts in each Production system. | Client will subscribe to services based on a predefined number of managed users as specified in the SOW. Managed users are calculated based on the sum of named user counts in each Production system. Monthly charges will be adjusted automatically (based on the additional percentage of users) when Client exceeds 110% of the subscribed number of users. |

| | | | |
|---------------|--|--|---|
| | their monthly hours for three (3) consecutive months, monthly charges will be increased equal to the average hours used over the three (3)-month overuse period. | Monthly charges will be adjusted automatically (based on the additional percentage of users) when Client exceeds 110% of the subscribed number of users. | Client will submit 90% of all security requests via ControlPanel ^{GRC} within sixty (60) calendar days of start of service delivery. If Client is unable or unwilling to submit access requests in ControlPanel ^{GRC} after this date, NTT reserves the right to increase monthly charges by 100% or its then current pricing at NTT's sole discretion. |
| Non-Recurring | Client requested expedites are subjected to charge at NTT's sole discretion. | Client requested expedites are subjected to charge at NTT's sole discretion. | Client requested expedites are subjected to charge at NTT's sole discretion. There may be an NRC for SAP Security Complete Plus ^{GRC} initial setup and configuration of Client's Managed SAP Security services. This will be detailed on the applicable SOW |