ControlPanelGRC

ControlPanelGRC Commercial Framework

ControlPanelGRC is NOT a Managed Service, and requires its own legal framework. Do not use the Client Service Description or standard Statement of Work documents when contracting this service.
This section will be updated as soon as details are available. For now contact Barbara Davis with any questions.

1 Overview of Service

ControlPanel[GRC®] is a software platform that provides a compliance automation solution for SAP environments. NTT offers the following ControlPanel[GRC] suites, one or more of which must be selected as in scope in the SOW, that enable Clients to execute and enforce a continuous compliance regimen while accelerating day-to-day tasks:

(a) Access Control Suite

(b) Security Accelerator Suite

(c) Basis Control Suite

(d) Process Control Suite

The specifics of the quantity of licensees and specific modules ordered must be specified in the SOW, and Client must agree to any required end user, software license and maintenance agreement.

2 System Design

One or more of the following Modules must be selected as in scope in the SOW, otherwise they are out of scope. A suite may be a collection of modules, and all modules must be ordered in order to obtain a suite.

2.1 ControlPanelGRC Access Control Suite

The ControlPanel[GRC] Access Control Suite detects and prevents potential segregation of duty (SoD) risks, provides SoD remediation options, manages elevated rights, provides compliant User provisioning and Role management, and manages periodic access reviews.

Modules	Features
Risk Analyzer[SM]	Real-time detective and preventive risk analysis and mitigation for SoD, critical transaction, and sensitive authorization risks.
	Root cause analysis for risks to help identify related transactions and authorizations and provide remediation options based on transaction usage.
	Best practices rulebooks that can be extended based on business or auditor requirements.
	Mitigating controls that filter accepted risks and push select compliance reporting to reviewers for signoff in the self-documenting workflow.
	Monitoring of select system risks, such as modifiable Clients, passwords of delivered SAP users, and profile parameters.
	Graphical dashboards for control owners to review risk trends and drill-down into changes in risk between periods.
Usage Analyzer[SM]	Collection of transaction execution history by user for use in SoD remediation or user monitoring.
	Analysis of usage instances, such as: • Roles assigned to Users are seldom or never used. • Transactions assigned to roles are seldom or never used by role users. • Single roles assigned to composite roles are seldom or never used by role users. • Roles are no longer assigned or used.
	Automated SAP license optimization based on Client rules within the limitations of the environment.
	Notification and tracking of users executing sensitive transactions.
	Accelerated security redesign by reviewing transaction executions by groups of users.
	Graphical dashboards for system owners to analyze system usage by User or User Group.

Emergency Access Manager℠	Provides elevated rights on a temporary basis for troubleshooting issues or backing up absent employees.
	Automatic provisioning and tracking of elevated access rights.
	Closed loop workflow approvals assist signoff after session completion and can be configured to require signoff before sensitive emergency access is granted.
	Automatic termination of emergency access based on time limits or system signoff.
	Notification of emergency access sent via email or routed for review in workflow, including executed transactions, captured screenshots, statistical records, table change logs, and change documents.
	Graphical dashboards for system owners to analyze emergency access usage and drill-down into details for simplified audit reporting.
User and Role Manager℠	Workflow-based access request engine that provides compliant user provisioning and compliant role management.
	Configurable workflow approvals available for combinations of employee supervisor, business owner, role owner, risk/control owner, and security to review changes before provisioning.
	Integrated risk analysis to identify SoD risks as part of the access request workflow.
	Automated provisioning of user change requests and accelerated processing for role change requests.
	Available web services allow integration with identity management and help desk platforms to simplify access request submission.
	Graphical dashboards for system owners to analyze user and role change requests and drill-down into details for simplified audit reporting.
Access Certification Manager℠	Automatic generation of periodic access reporting that is pushed to appropriate business owners for review in the self-documenting workflow.
	Configurable access analysis where user owners can review roles assigned to their users and/or role owners to review users assigned to their roles.
	Configurable messaging to business owners to help communicate the purpose and scope of periodic access reviews.
	Provides information that business owners may require to determine if current access is appropriate or should be removed, such as Role/User details and usage history.
	Automatic de-provisioning of access based on business owner feedback.
	Audit reporting shows the status of the periodic access review and identifies changes requested by business owners.
HR Analyzer℠	Analysis of non-sensitive human resources (HR) data (for example, location, supervisor, position, and direct reports) for use by system administrators.
	Automatic provisioning and de-provisioning based on HR activity, such as new hires, job changes, and terminations.
	Configurable Role and User Parameter assignments can be driven from employee attributes, such as personnel area, organization, position, and employee group, to simplify manual SAP security reconciliation with HR master data
	Reconciliation of HR master data with selected User master data fields.
	Monitoring of usage of sensitive HR master data.
	Built-in data scrambling routine to protect information used outside of Production systems.

Workflow[SM] and AutoAuditor[SM]	Flexible, configurable workflows enabling self-documenting approvals for compliance activities.
	Robust reporting on workflow approvals, documentation, and history.
	Compliance reporting that is automatically pushed to reviewers in the self-documenting workflow.

2.2 ControlPanelGRC Access Control Suite Module Dependencies

The following dependencies exist for the Modules that comprise the Access Control Suite and must be included as in scope in the SOW:

Module	Dependency
Risk Analyzer	Usage Analyzer
User and Role Manager	Risk Analyzer
Access Certification Manager	User and Role Manager
HR Analyzer	User and Role Manager

2.3 ControlPanelGRC Security Acceleration Suite

The ControlPanel[GRC] Security Acceleration Suite provides information to recreate and troubleshoot security issues, automated security testing, password resets and synchronization, and user and SAP role version management and change acceleration.

Module	Features
Password Manager[SM]	Synchronization of SAP password across complex SAP landscapes with multiple systems and Clients.
	Password self-service functionality enables users to request an automatic password reset without having to involve the help desk.
	Configuration allows password synchronization and self-service to be enabled for specific SAP systems or all systems.
	Capability to ask a security question with validation prior to granting a password reset.
	Available Web Services allow integration with help desk platforms to simplify password reset request submission.
	Graphical dashboards for system owners to analyze password reset usage and with detailed reporting.
Security Troubleshooter[SM]	Simplified and accelerated resolution of SAP security issues.
	Automatic capture of description and details to recreate SAP security issues.
	Optional automatic screenshot provides all information necessary to recreate and resolve issues.
	Significantly enhanced authorization details help troubleshoot security issues instead of relying on SU53.
	Automatic delivery of issue to security team for processing and resolution.
	Configurable delivery of issues to decentralized security teams based on user location.
Security Quality Assurance[SM]	Automated initial unit testing for roles ensuring that all transactions within a role can be started without authorization failures.
	Automated testing of SU24 defaults ensuring that appropriate authorizations are configured to allow transactions to be started without authorization failures.

	Automated creation of test logons for roles with recurring batch process to identify new roles.
	Simplified interface for role owners to easily activate test logons without having to sign in and out of multiple logons.
	Test user launch pad shows all transactions available for testing and date of last test.
	Monitoring of validation processes to identify completeness of testing.
User and Role Change Analyzer℠	Automated versioning of roles enable easy comparison and/or ability to revert to previous Role versions.
	Cross-system analysis of roles to ensure synchronization across landscapes.
	Mass changes to users, such as download/upload between Clients, data conversions for user creation, upload of role assignments from flat file, and mass password reset with user notification.
	Mass changes to roles, such as adding/removing transactions or single roles to/from multiple roles and synchronizing role organizational values based on templates.
	Mass creation of roles, including upload from flat file and mass copy from parent to derived role.
	Mass changes to SU24 defaults to reduce open activity fields, unnecessary Basis and HR access, and include any missing objects identified during testing.

2.4 ControlPanelGRC Basis Control Suite

The ControlPanel℠ Basis Control Suite automates SAP change request processing and batch job monitoring. The suite includes a powerful workflow engine with embedded compliance to eliminate repetitive daily tasks.

Module	Features
Transport Manager℠	Self-documenting workflow engine for change request management that includes integrated tracking and recording.
	Integration with transport release processing to simplify approval request submission.
	Predefined migration model determines appropriate approvers and target systems.
	Automatic migration of SAP transports based on approval and migration schedule.
	Testing details captured in documentation, including testing plans, results, and relevant screenshots.
	Graphical dashboards for system owners to analyze change requests and drill-down into details for simplified audit reporting.
Batch Manager℠	Compliant management, approval, documentation, and monitoring of cross-system SAP batch Jobs.
	Centralized infrastructure for job scheduling and monitoring.
	Mass monitoring of batch jobs with notifications sent to appropriate owners to review failures or long running jobs.
	Cross-system job definitions that can execute steps in differing target systems.
	Workflow notifications identifying long running jobs or routing failed jobs (and related logs) to appropriate owners for review.
	Routing of output from successful jobs to appropriate owners for review.

Workflow[SM]	Flexible, configurable workflows enabling self-documenting approvals for compliance activities.
	Robust reporting on workflow approvals, documentation, and history.

2.5 ControlPanelGRC Process Control Suite

The ControlPanel[GRC] Process Control Suite provides enterprise risk management with exception-based reporting for configuration, master data, and transactional activity.

Module	Features
Enterprise Risk Management[SM]	Configurable library to document enterprise control structure for specific compliance regimes.
	Control definitions capture, such as risk documentation, control framework categorization, business and risk owners, and location specific controls.
	Risk and control matrix generation to document controls for specific compliance regimes.
	Automated SAP-based reporting, for which control reports are automatically executed in appropriate systems and routed to control monitors within the self-documenting workflow engine.
	Automated audit plans utilize workflow to capture signoff on control reaffirmation, audit preparation tasks, and control testing.
	Easy-to-use reporting to identify exceptions in control monitoring and audit testing.
Order to Cash[SM]	Sample queries to address potential order to cash business risks that can be adjusted based on Client requirements.
	Monitoring of risks related to key configurable controls.
	Monitoring of risks related to key master data controls.
	Monitoring of risks related to key transactional data controls.
	Documented workflow to approve potential risks as they are identified.
Procure to Pay[SM]	The ControlPanel[GRC] Process Controls – Procure to PaySM is a module of the ControlPanelGRC Suite for Compliance Automation that provides: • Sample queries to address potential procure to pay business risks that can be adjusted based on Client requirements. • Monitoring of risks related to key configurable controls. • Monitoring of risks related to key master data controls. • Monitoring of risks related to key master data controls. • Documented workflow to approve potential risks as they are identified.
Workflow[SM] and AutoAuditor[SM]	Flexible, configurable workflows enabling self-documenting approvals for compliance activities.
	Robust reporting on workflow approvals, documentation, and history.
	Compliance reporting is automatically pushed to reviewers in the self-documenting workflow.

3 ControlPanelGRC Services

The following ControlPanelGRC Services must be selected as in scope in the SOW and are required, and will be charged as long as the license is in use.

3.1 Software Maintenance

NTT provides ControlPanel[GRC] software maintenance with a current subscription the software maintenance agreement provided by NTT to Client, which consists of the following:

(a) Software bug fixes, updates, enhancements, and version upgrades.

(b) Incident management system for logging issues.

(c) Issue review and resolution by qualified consultants for the Client environment.

(d) Hands-on technical support to help troubleshoot issues via screen sharing.

(e) Bug fixes addressed with urgency.

(f) Software enhancements driven by Client feedback.

(g) Simple upgrade path and release strategy that ensures backward compatibility.

(h) Option to attend annual ControlPanelGRC User Summit.

3.2 JumpStart Implementation Services

NTT provides JumpStart Implementation Services to Client to assist in the ControlPanel[GRC] go-live process. These services are performed by a ControlPanel[GRC] implementation consultant. Several service options are offered and are recommended to Client based on the complexity of the Client's environment and scope of the ControlPanel[GRC] implementation. These services last for a fixed duration and delivered remotely and/or onsite (onsite requires additional fee and travel costs). The specific amount of JumpStart implementation included must be specified in the SOW, otherwise none are included.

Training sessions are led by certified ControlPanel[GRC] implementation consultants, Client personnel are "hands on keyboard" with guidance from the instructor, leveraging a "train-the-trainer" approach. JumpStart Implementation Services are used for both new implementations and refresher training, or consulting, and the specific amount of JumpStart implementation included must be specified in the SOW, otherwise none are included.

JumpStart Implementation Services consist of the following, which the total JumpStart service commitment is specified in the SOW:

(a) Pre-implementation planning and kick-off call to establish software install prerequisites, project timelines, scope, and the agenda for training.

(b) Training and/or consulting, with hands-on learning for key Client personnel.

(c) Instruction and guidance for Client personnel to configure ControlPanelGRC based on Client use cases.

(d) Remote support and/or consulting.

JumpStart Implementation Services are hour based starting on the first day training/consulting and ending based on the predefined timeline specified in the SOW. Specific timeline, work to be performed and actual details for JumpStart Implementations is in the SOW, otherwise none are included.

4 Operational Parameters

ControlPanel[GRC] runs on the existing SAP infrastructure and is imported via a transport. ControlPanel[GRC] is compatible with all SAP releases from 4.6C and above. ControlPanel[GRC] does require approximately twenty to forty (20–40) GB of storage available. Future releases and updates may have additional hardware requirements.

Client must define and implement the operational parameters specific to the services purchased, as outlined in the table below:

ControlPanel[GRC] Services	Operational Parameters
ControlPanel[GRC] Implementations	Current policies for related ControlPanel[GRC] software (for example, SoD risks, emergency access rights, periodic access reviews, and change management strategy).
	Current manual processes (for example, existing workflows and approvers).
JumpStart Implementation Services	Client is responsible for all configuration and deployment tasks related to ControlPanel[GRC].

5 Cloud Platform Integration Services

NTT provides Cloud Platform Integration Services to Client to provide ControlPanelGRC with non-ABAP platforms. These services are performed by a ControlPanelGRC implementation consultant and a ControlPanelGRC developer. These services last for a fixed duration and are delivered remotely and/or onsite (onsite requires additional fee and travel costs). The specific amount of Cloud Platform Integration Services must be specified in the SOW, otherwise none are included. Client is responsible for providing user access field mappings, mapping of cloud platform activities to ControlPanelGRC Rulebook Functions, and documentation on available web service APIs to extract access data and complete provisioning tasks. Using this data, NTT configures external adapters within ControlPanelGRC to call the cloud platform, extract relevant data, and map it into ControlPanelGRC structure for risk analysis and provisioning tasks. NTT will also update any existing Rulebook Functions based on the provided activity mappings.

Cloud Platform Integration Services consist of the following, which the total service commitment is specified in the SOW:

(a) Pre-implementation planning and kick-off call to discuss client prerequisites, project timelines, and scope.

(b) Configuration of external adapters to Cloud Platform and mapping into ControlPanelGRC structures.

(c) Instruction and guidance for Client personnel to validate ControlPanelGRC integration based on Client use cases.

(d) Remote support and/or consulting.

Cloud Platform Integration Services are hour based starting on the first day training/consulting and ending based on the predefined timeline specified in the SOW. Specific timeline, work to be performed and actual details for Cloud Platform Integration Services is in the SOW, otherwise none are included.

6 Out of Scope

6.1 SAP Releases

ControlPanel[GRC] is designed to run on all SAP releases starting with 4.6C. However, there are some features of ControlPanel[GRC] that are only available in newer releases of SAP. Examples of these features include, but are not limited to, use of Fiori Apps and use of ZIP functionality to reduce attachment size. Each new release of ControlPanel[GRC] may not be compatible will all SAP releases or may be different than the current supported SAP releases by the previous ControlPanel[GRC] release.

6.2 Software Maintenance

Software maintenance provides for bug fixes, software upgrades, technical support, and other updates to the software, as specified in the SLMA and as long as it is in scope in the SOW as required above. It does not provide for continued education, training, or additional consulting services.

6.3 Software Enhancements

Client requested enhancements and suggestions to ControlPanel[GRC] are may be included in upcoming software releases at NTT's discretion. Development and delivery of Client-requested enhancements is not part of software maintenance and require a separate SOW and are out of scope. Client grants the irrevocable, worldwide, royalty free licenses for any improvements suggestions, or otherwise to NTT.

6.4 JumpStart Implementation Services

NTT is providing consulting services to train Client personnel on how to implement, configure, and use ControlPanel[GRC]. NTT uses a “train the trainer” approach where the Client establishes a ControlPanel[GRC] subject matter expert (or experts) and Client ultimately responsible for deploying ControlPanel[GRC] per their use cases and training other Client end-users.

JumpStart Implementation Services are not intended to help Clients define security policies like IT general controls or SoD requirements. Client is responsible for establishing control requirements in advance and can use NTT to translate requirements in ControlPanel[GRC] automation.

JumpStart Implementation Services are sold, and NTT resources are made available, based on a predefined project duration. Client is responsible for managing project timelines and ControlPanel[GRC] deployment using NTT as a technical resource.

7 Client Responsibilities

Client failure to fulfil its responsibilities may delay or prevent NTT from providing the service.

ControlPanel[GRC] Services	Client Responsibilities
JumpStart Implementation Services	Client will perform project management tasks related to implementation of ControlPanel[GRC].
	Client will import ControlPanel[GRC] software transport into appropriate SAP systems.
	Client will provide resources to attend JumpStart sessions and become internal subject matter experts for ControlPanel[GRC].
	Client will define and establish internal control processes for implementation in ControlPanel[GRC].
	Client will configure ControlPanel[GRC] based on Client use cases.
	Client will adjust ControlPanel[GRC] risk rulebooks (if necessary) based on unique Client processes, custom transactions, and/or document types.
	Client will deploy ControlPanel[GRC] in Client Production systems.

	Client will conduct end-user training and/or develop use case specific documentation for access requestors and/or approvers.

8 Support

This section outlines the support expectations as it relates to software maintenance, including a general description of incident types, a matrix of common tasks, and an explanation of how to submit support requests.

8.1 Incident Types

(a) Severity 1- An incident is classified as a SEV1 when users are experiencing major loss of ControlPanelGRC functionality, or the ControlPanelGRC subscribed service has been rendered unusable for its intended purpose.

(b) Severity 2 - An incident is classified as a SEV2 when a major component of ControlPanelGRC is substantially not performing in accordance with the Documentation and there is no practical work around.

(c) Severity 3 - An incident is classified as a SEV3 when a major component of ControlPanelGRC is substantially not performing in accordance with the Documentation.

(d) Severity 4 - An incident is classified as a SEV4 when a Client requests an enhancement to existing ControlPanelGRC

8.2 Task Matrix

The tasks listed in the following matrix are examples of typical support requests that may be submitted related to ControlPanel[GRC]. The list is not meant to be all-inclusive, but rather to provide a framework for understanding the response typically given to support tasks. It is Client's responsibility to include the classification and pertinent details that explain the impact that the request has on their business/service under the guidelines detailed below. NTT may adjust the the Severity level in its reasonable discretion based on the information included.

The time frames reflected in the table are typical times to respond to the request, expressed in Minutes (M), Hours (H), or Business Days (D) but is not a guarantee, promise, or binding commitment and are only provided as an example. Response times for SEV2–SEV4 tasks are calculated during standard continental U.S. business hours only, defined as Monday through Friday, 8am to 5pm CST, excluding public and bank holidays. Some tasks may require additional validation or information to commence work and/or an update to the SOW in order to be processed. Some tasks may also require a Client Information Form to be completed by Client and returned to the Project Manager, detailing how the options for the service are to be configured. For these tasks, the time frame described begins once a signed SOW or completed Client Information Form is received by NTT.

Severity Level	Task	Typical Response Time	New SOW Required	Task Description
SEV1	Troubleshoot Issue	4H	N	Begin investigation of why all or most users are experiencing a significant outage related to ControlPanel[GRC].
	Escalate Unresolved Issue	2D	N	Escalate the issue to a higher level of support until it is resolved.
SEV2	Troubleshoot Issue	1D	N	Begin investigation of why a large number of critical users are experiencing a significant outage related to ControlPanel[GRC]
	Escalate Unresolved Issue	4D	N	Escalate the issue to a higher level of support until it is resolved.
SEV3	Troubleshoot Issue	2D	N	Begin investigation of ControlPanel[GRC] issues.
	Escalate Unresolved Issue	4D	N	Escalate the issue to a higher level of support until it is resolved.
SEV4	Review Issue	4D	N	Respond to request to enhance ControlPanel[GRC] based on Client request.
	Deliver ControlPanel[GRC] enhancement to Client	N/A	Y	Enhance ControlPanel[GRC] software based on Client request.

8.3 Support Requests

Client must report incidents and requests to NTT using the Services Portal, and must properly classify the severity level upon submission. If Client is experiencing a SEV1 incident, after submitting the incident, Client

must immediately call the NTT Integrated Operations Center (IOC). Support requests may require additional validation and/or information from Client before a task is initiated.