Prerequisites for Installing and/or upgrading to release 5.2.13

compliance NOW

Content

Introduction

This guide outlines the prerequisites and key preparations required before upgrading ComplianceNow Suite from a olde release to the newest release 5.2.13. It is intended to help administrators gain a task overview and to ensure that all necessary conditions are met for a smooth and successful system upgrade.

For support, contact ComplianceNow at +45 4041 4401 or support@compliancenow.eu.

System overview and landscape assessment

Before initiating the upgrade, an overview of the system landscape must be established. This includes identifying which SAP systems are connected to which ComplianceNow web application server(s).

The ComplianceNow Suite consists of:

- An ABAP add-on installed in each SAP system where ComplianceNow functionality is required.
- One or more external web application servers to which the SAP add-on components connect.

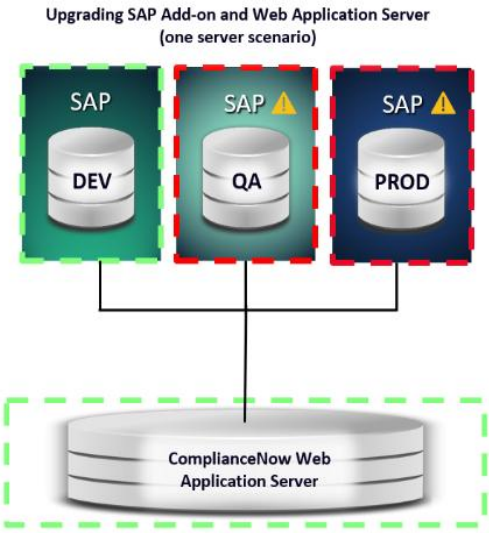
Although the ComplianceNow web application server supports backward compatibility, full functional compatibility cannot be guaranteed. Therefore, it is recommended to operate:

- One dedicated web application server for non-productive SAP systems (DEV/QA).
- One dedicated web application server for productive SAP systems.

This segregation establishes technical isolation between environments and ensures that maintenance, upgrades, configuration changes, and functional testing in non-productive systems can be performed without impacting the productive environment.

If a single ComplianceNow web application server is shared between non-productive and productive SAP systems, any upgrade of the web application server will affect all connected ComplianceNow SAP add-on installations.

Although the ComplianceNow web application server supports backward compatibility, full functional compatibility cannot be guaranteed. If an upgrade is performed in the non-productive environments, the productive SAP system may continue to run an older ComplianceNow add-on version while being required to interact with an upgraded web application server, resulting in a version mismatch and potential functional instability.



As a result, when a single web application server is used for both non-productive and productive SAP systems, the upgrade process introduces a period during in which ComplianceNow in the productive environment may be disrupted while validation and testing are performed in the non-productive environments.

Impact assessment

The impact of version mismatches between the SAP ComplianceNow add-on and the web application server depends on which ComplianceNow components are in use and the version gap between the installed add-on and the connected web application server.

Potential issues range from:

- Disruption of essential core features in the ComplianceNow components.
- Errors in master data.
- Partial loss of functionality.

Upgrade planning and coordination

The following activities must be planned and coordinated in advance:

- Overview over dependencies between SAP systems where the ComplianceNow ABAB Add-on is installed and the ComplianceNow web application server(s)
- Assessment of impact related to business operations.
- Overview over the upgrade requirements of components on the web application server e.g. Apache, MySQL, PHP, Microsoft Java and SourceGuardian.
- Deployment of the new ComplianceNow SAP add-on software.
- Import of any additional SAP transports required for the upgrade.
- Allocation of technical and functional resources throughout the upgrade process.

- Validation of ComplianceNow components post upgrade installation
- Coordination of task utilization, including internal planning and execution by the customer.
- If extended billable support is required from third parties (e.g. Nagarro, third-party basis team, etc.).

All documentation related to the upgrade, including installation manuals, are provided and covered under the general support agreement.

General support is limited to assistance with general questions and similar inquiries and does not include project planning, coordination of installation activities, or execution of upgrade processes unless explicitly agreed.

SAP SPAM

SPAM version at least 55 must be installed on the SAP system before installing

Access Control

Pending workflow

Before upgrading to ComplianceNow Suite release version 5.2.13, it is strongly recommended to complete all pending CN Access Control approval workflows. This precaution ensures a smooth transition, as the logic behind the approval process has been significantly updated in this release.

In previous versions, when assigning one or more roles to a user triggered multiple risks for different approvers, all risks were grouped into a single work task. This meant that all approvers had to approve the same task before any of the role assignments could be completed.

From version 5.2.13 onwards, each risk is handled and approved individually. This allows roles linked to approved risks to be assigned without waiting for other approvers to complete their tasks.

To prevent unintended actions or misunderstandings related to workflow handling, it is strongly recommended to complete all pending approval workflows before upgrading.

If the upgrade is performed while workflows are still pending, the following occurs:

- Existing approval workflow tasks will be split into separate tasks.
    - For example, if three role assignments involving three different approvers were previously grouped in one workflow task, they will now appear as three individual work tasks after the upgrade.
- Any existing workflow task with partial approvals will be reset, meaning that all approvals must be re-submitted after the upgrade.

Before version 5.2.13

User	Assigned Roles	Triggered Risks	Approvers	Workflow Structure
USER001	Role A, Role B, Role C	Risk 1 Risk 2 Risk 3	Approver 1 Approver 2 Approver 3	Single combined Work Task (All roles and risks included in one approval process. All approvers must approve before any role is assigned.)

From version 5.2.13

User	Assigned Roles	Triggered Risks	Approvers	Workflow Structure
USER001	Role A	Risk 1	Approver 1	Separate Work Task 1
USER001	Role B	Risk 2	Approver 2	Separate Work Task 2
USER001	Role C	Risk 3	Approver 3	Separate Work Task 3

Privileged Access Management

Privileged Access Management (previous EUA) transactions

From ComplianceNow Suite release version 5.2.12 and onwards, the application previously named *Emergency User Access(EUA)* has been renamed to *Privileged Access Management (PAM)*.

This change impacts the SAP transactions associated with the component. As a result, new transactions are introduced and must be considered in connection with role design and authorization assignments.

Below is an overview of the new transactions related to the Privileged Access Management (PAM) application.

Transaction	Description
/APPLISOL/EMERGENCY (same as before)	**Open / Close Privileged Access User**
/APPLISOL/PAM_ADMIN	**PAM administrator**
/APPLISOL/PAM_AUDIT	**PAM Auditor**
/APPLISOL/PAM_CUST	**PAM: User Class Customizing**
/APPLISOL/PAM_REORG	**Privileged Access User: REORG**
/APPLISOL/PAM_USAGE	**Usage of Privileged Access Users**

Change to Privileged Access Management (previous EUA) roles

Overview of new roles for the Privileged Access Management (PAM) application.

Role	Description
/APPLISOL/PAM_ADMIN	**PAM administrator**
/APPLISOL/PAM_AUDIT	**PAM Auditor**
/APPLISOL/PAM_USER_GRP_ALL	**Privileged Access role to use group ALL users**
/APPLISOL/PAM_EMERGENCY_USER	**Privileged Access role for minimum PA-user authorizations**
/APPLISOL/PAM_USER_MASTER	**Privileged Access role to use groups - Master role**

Internal Control

Start date and frequency

From ComplianceNow Suite release 5.2.13 and onwards, the logic for *Start Date* and *Frequency* for control checks has been changed.

Previously, frequencies were based on predefined calendar periods.

For example, yearly controls were always triggered in January, and quarterly controls were triggered in fixed months regardless of the configured start date.

From release 5.2.13 and onwards, the *Start Date* is used as the reference point for all frequency and period calculations.

Controls are now scheduled dynamically based on the defined start date rather than fixed calendar periods.

As a result of this change, it is recommended to review and reconfigure the start date and frequency for all active controls after upgrading to ensure that executions occur on the expected dates.

Example 1

If a yearly control should be executed in January each year, set the start date to January in the upcoming year and select Yearly as the frequency.

Example 2

If a yearly control should be executed in August each year, set the start date to August in the upcoming year and select Yearly as the frequency.