nagarro

Compliance
Now

Top 50 Core SAP Controls

to help you ensure the next level of compliance for your SAP processes

nagarro.com
Fluidic Enterprise

Introduction

This document provides a list of the top 50 SAP core mitigating controls to improve compliance in your SAP processes, a critical resource for organizations seeking advanced risk management. Before delving into this list, it's essential to understand the journey and the synergies between the various risk management processes in SAP.

In the quest for advanced risk management and compliance in SAP environments, organizations typically take the first major step on this journey with the implementation of a Segregation of Duties (SoD) tool. This major improvement can serve as the foundation, but what comes after establishing SoD? This document delves into the subsequent critical phase of integrating mitigating controls. It highlights the natural progression from SoD to mitigating controls and illustrates how they complement each other to form a holistic risk management strategy. This synergy between SoD and mitigating controls is essential for organizations seeking to achieve not just compliance, but excellence in risk management.

Following this exploration, we present the essential top 50 core mitigating controls that are common across all organizations, and therefore instrumental in advancing your organization's compliance and risk management in SAP.

About SAP Risk Management

SAP Risk Management is often not part of the implementation roadmap for many companies. SAP ERP systems are complex and often businesses cannot see the full roadmap for implementing risk management as part of an ERP project at the time of implementation. Taking European companies as an example, there is often tendency for small to mid-sized companies to generally lag in implementing the SAP risk management measures compared to the US companies which are heavily regulated by SOX requirements, leading to greater focus on risk management.

Trend indicates a growing emphasis on Segregation of Duties (SoD) in Europe

We now see indicators that the trend is changing and more European companies are exploring what a roadmap might look like if they were to implement Segregation of Duties (SoD). Implementing SoD is an important step towards a more mature risk management set-up.

Implementing SoD will provide you support with two tasks.

I. Firstly, helping to identify and/or prevent the combination of risks built into the same role – often referred to as SoD-Free roles.

II. Secondly, SoD supports the identification of SoD's and critical access in the user provisioning process for approval prior to assignment.

Implementing SoD is the final step of Risk Management in SAP – or is it?

Now that you have implemented an SoD tool to protect important processes, sensitive data, and critical SAP infrastructure, are you then done for good?

Implementing SoD is a big step from just being covered by the ordinary access management in SAP. Based on a dedicated SAP risk library, you have a clear picture of who in the organization has a risk and you may have even delegated the approval of risks away from the IT-department to the relevant risk owners in the business instead.

You are at a point where the risk owners have approved the relevant users with privileged access and (hopefully) rejected the ones not needing the access (or are not to be trusted with the risk associated with the access).

As mentioned, implementing SoD is an important milestone toward protecting your SAP environment. But SoD is not a 100% safety net – you will potentially still have a lot of people with powerful and critical access. However, there is a big difference after implementing SoD – you now get the visibility of everyone who has the access. And perhaps more importantly you know someone in your organization has explicitly given consent, allowing the privileged access.

Why do we need controls as part of our ERP Risk Management strategy?

One might ask **why the controls are necessary as part of an effective ERP Risk Management strategy?**

Well, since SoD is a big step up on the risk management maturity ladder, implementing SAP controls is the next natural step in protecting against risks and securing your SAP environment. Essentially, controls take over the process of identifying and remediating risks where SoD left off. While the SoD process is focusing on access risks, the controls are an audit process that detects and prevents oversights in the previous control measures.

In summary, while the SoD tool concentrates on determining your access permissions and whether they can be approved, controls act as an audit mechanism to detect and avert errors after privileged access has been approved.

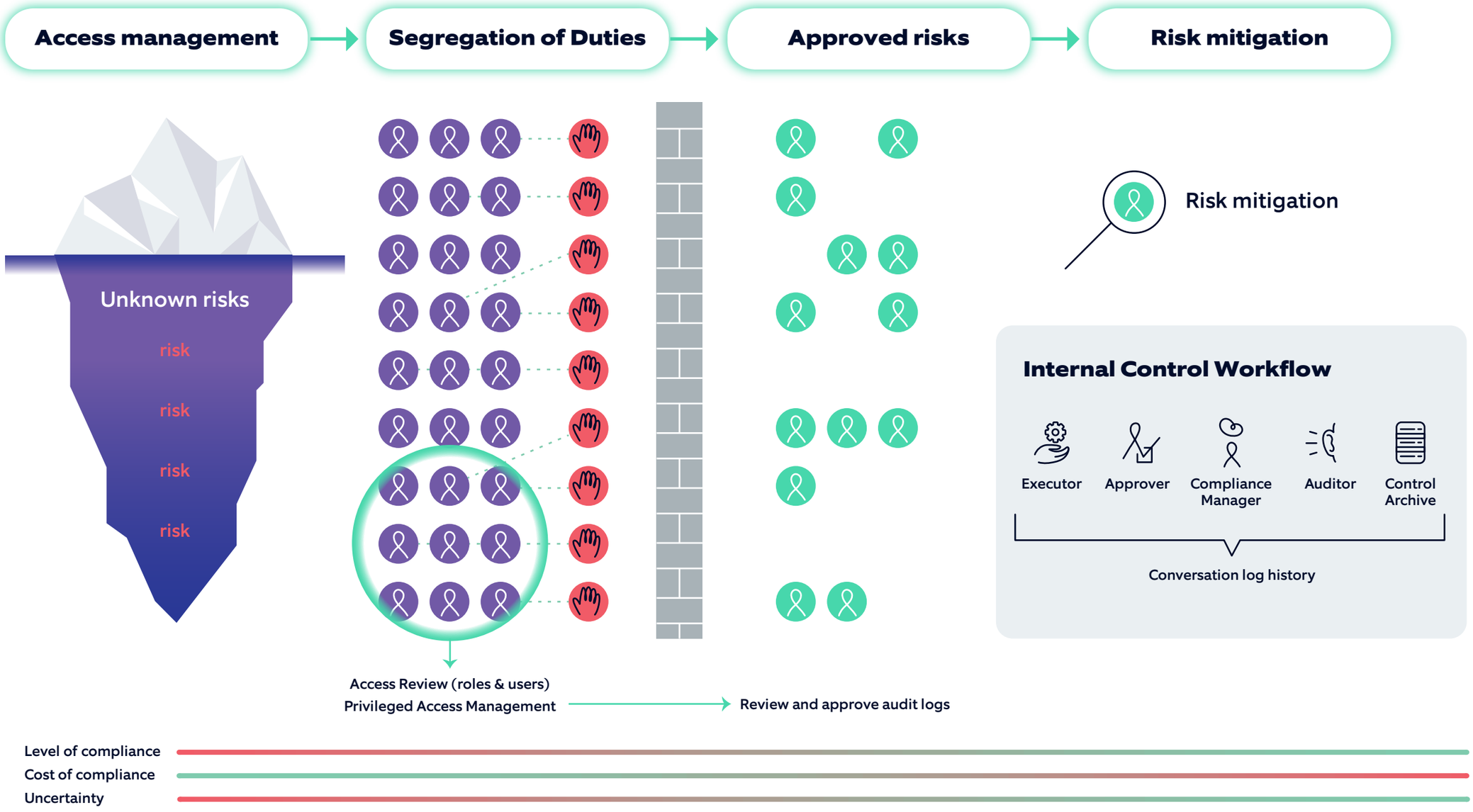
From Access Management to SoD Management and Mitigating Controls

Access Management and SoD Management are **two essential steps** in a good risk management strategy. These two precautions serve as layers of access approval, risk identification, assessment, and approval process.

The graphic below illustrates the mentioned process of risk management in SAP. With just access management in place, we are basically driving blindfolded, not knowing the underlying risks (the bottom part of the iceberg under the water). The SoD process gives us an overview of access risks to be reviewed and approved by the risk owners.

Despite all the effort, there will still be employees that will have accepted risk which cannot be segregated away. This can be mainly due to the way the processes are designed or due to a limited number of people in the team. Therefore, the third step, mitigating controls, will now investigate through dedicated procedures in SAP whether mistakes have occurred or if the trust outlined in the previous steps has been compromised.

Broadly speaking, SoD provides transparency and reduces risks by preventing them, and controls will mitigate the potentially damaging consequences of the risks identified and accepted in the SoD process in a structured way.



Let’s try to describe what a control in SAP looks like

We have selected a finance control called: Bank Master Maintenance and Payments to Vendor

From Access Management to SoD Management and Mitigating Controls

This control is designed to detect and prevent potentially fraudulent activities, such as the creation of fictitious bank accounts and unauthorized payments to vendors. The control measures include the detection of all users with access to both conducted (Function A) Bank Master Maintenance and (Function B) Payment to Vendor.

Additionally, this control checks for any users with approval authority for both functions and investigates instances where the same user has conducted both sides of the conflict.

Purpose of the control

To quickly validate the relevance of the control mentioned above, we define a purpose which in this instance would appear as follows:

“The purpose of this control is to protect the organization's financial integrity by preventing fraudulent activities. It ensures that users do not abuse their privileges to create fictitious bank accounts or make unauthorized payments to vendors.”

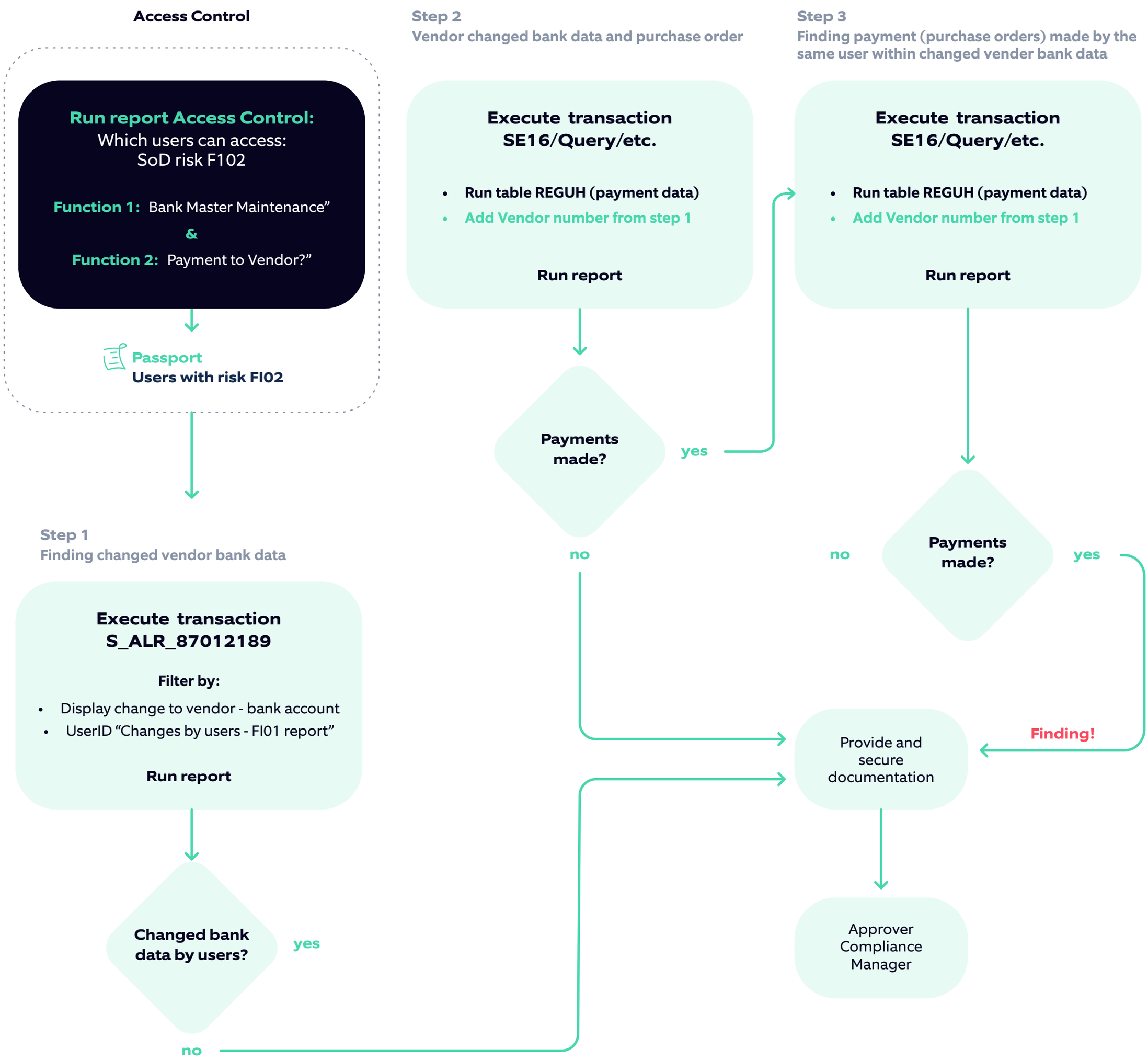
Control execution description

For each control, we provide a detailed, step-by-step description of its execution. In certain instances, we also include a diagram to illustrate the overall process of the control. The depth of the description may vary, but it is designed to serve as a guide for the person executing the control, enabling them to proceed without being an experienced business or SAP expert.

In this case, we have omitted most of the actual description (that is a 4 x 10 step instruction of how to perform a control of ‘Bank Master Maintenance and Payments to Vendor Control’. If you are interested, we would be pleased to forward you a full sample of this control and a few other controls. Just send an email to **info@compliancenow.eu** with the subject line ‘Bank Master Maintenance Control’ to receive your control samples.

Step 1 out of 4 - Audit Changes to Vendors - Bank Account

1. **Navigate** to Transaction S_ALR_87012189.
2. **Specify the users** in the "Changed by" field. These should be users who have access to both processes.
3. Based on the control period, **fill** the "Changed on" field **with the appropriate date.**
4. Optionally, provide **additional parameters** such as "Company code", "Sales organization", etc.
5. **Capture a screenshot** of the selection criteria to serve as evidence.
6. **Execute** the report by pressing F8.
7. **Save the report:** navigate to System -> List -> Save, and store the list as an Excel file for future reference.
8. **Open the file in Excel**, filter the "Field Name" column by "Bank Details".
9. **Extract the "Vendor number"** from the "Vendor" column; this will be used in the next step.
10. **Preserve the list** by saving it as an Excel file, serving as evidence.



The control templates will also include an expected "Documentation" section

A list of items that are suggested to be submitted is included in the control templates provided by CN. See example below. This can help with framing the expectations of what should be submitted and assist in making the control execution easier and more manageable. This will not only help demonstrate how to execute the control, but also enhance documentation for future review and audit purposes as well as make the control execution consistent.

1. Display changes to Vendors – Bank account:

- File with the content of report S_ALR_87012189.
- Screenshot of the selection criteria chosen in SE16N.

2. Settlement data from payment program:

- File with the content of REGUH – Settlement data from the payment program.
- Screenshot of the selection criteria chosen in SE16N.

3. Processed items from payment program:

- File with the content of REGUP – Processed items from the payment program.
- Screenshot of the selection criteria chosen in SE16N.

4. Document numbers – Real documents:

- Checks of all documents against "real-world" invoices, with saved copies of samples for control documentation.

Are there different types of controls?

Yes, the controls vary, both in complexity and in the logic of how to conduct the control. In some situations, the control consists of guidance on how to configure SAP to mitigate the risk. Other controls may be simpler and focus on the use of critical access. The example selected here is more complex and requires multiple steps from the executer to reach a conclusion.

The controls are created as predefined templates and must in some cases be tailored to fit your organization's specific processes.

Preventive and detective controls

- **Preventive Controls:** These controls point out SAP standard functionalities such as sensitive fields, 4-eye principles, the utilization of SAP standard codes for specific functions, and that the correct setup of change log/audit logs are configured.
- **Detective Controls:** These controls facilitate the investigation of specific user actions that may lead to fraud or errors, such as users who have utilized both sides of functions in an SoD conflict or which users have the proper authorization for critical transactions and which users have performed these transactions.

Top 50 ComplianceNow predefined controls

Our goal is to provide our clients with a solid foundation for establishing a process around risk mitigation in SAP. The objective of this initative is to cover all risks from our CN Access Control risk library, providing our customers with a broad selection of controls to choose from. We have currently specified controls in the areas of SAP security, SAP Basis, HR/Payroll, Finance, Procure to Pay, Order to Cash, and Quality Management.

In total, we currently have more than 150 pre-defined control templates that are delivered with our CN Internal Control component. At the moment, all are dedicated to SAP but it is possible to include non-SAP controls as well in CN Internal Control.

In the following section, we have listed a selection of the top 50 SAP controls from our CN Internal Control library.

The Selection Process of the top 50 controls

We've selected these risks based on their potential impact across a wide range of businesses, industries, and technological complexities. However, it's crucial to note that the significance of these risks may vary based on your specific circumstances, risk tolerance, and operational environment.

Don't take our word as the absolute truth. Consult with your internal audit team, an SAP risk consultant or reach out to us for a deeper investigation into the risks most relevant for your organization.

The selected risks provide a general overview within SAP, and the potential pitfalls for any organization, worldwide.

Category	Title	Risk Description	Control Description
SAP – Background Job	**Background jobs, Scheduled in SM36**	Given unrestricted access, users with malicious intent could potentially misuse the background administration in SAP transaction SM36, which is responsible for scheduling large-volume data processes. Such misuse could lead to the unauthorized execution of critical programs, data inconsistencies, or even severe information loss.	The control is designed to regulate background administration in SAP transaction SM36, which is integral to scheduling background jobs in the system. These jobs often execute essential, large-volume data processes, making them potential targets for malicious activity. By restricting access to SM36, the control minimizes these potential vulnerabilities, while also investigating historical changes.
SAP – Basis	**Access to Delete Client**	If unapproved users gain access to the client deletion function in the SAP system, they could inadvertently or intentionally delete clients. This improper client deletion can result in critical data loss, system inconsistencies, and can disrupt business operations. This scenario also poses a risk to the integrity of customer data and may lead to breaches of contract or legal implications if client data is lost.	This control safeguards against unapproved access to and execution of client deletion in the SAP system, a function that could lead to detrimental outcomes like critical data loss. The control limits access to the deletion function to only approved users. In addition, the control facilitates monitoring of changes and investigates any unexpected or unauthorized client deletions, thereby ensuring system integrity and data accuracy.
SAP – Basis	**Transactions, Lock/Unlock**	In the SAP system environment, the modification of transaction lock status by unapproved individuals presents a profound risk. This improper access and alteration of locked transactions could precipitate system instability, potential data loss, and disruption of core business operations. Additionally, unauthorized changes can engender inaccuracies in data reporting, which in turn could result in compliance violations and reputational damage.	The Transactions Lock/Unlock control is engineered to prohibit unapproved users from accessing and modifying the lock status of transactions within the SAP system. This control restricts these critically sensitive functions to only individuals who possess the requisite permissions and approvals. In doing so, it robustly safeguards the system against potential instability and data loss. Moreover, the control investigated the historical changes to the transaction locks and unlocks within the system.
SAP – Basis	**Maintain System Parameter**	There's a heightened risk when unapproved users are allowed to modify system parameters in the SAP system. Inappropriate changes can lead to system instability and potential data loss. This could disrupt the normal functioning of the system and result in significant operational challenges for the organization.	The control limits the ability to modify system parameters in the SAP system to only approved individuals with the aim to prevent system instability and potential data loss due to improper alterations. It ensures that only individuals with the necessary authorization and permissions are granted the ability to maintain system parameters. Additionally, this control necessitates detailed investigations into past modifications.

Category	Title	Risk Description	Control Description
SAP – Basis	**System Option, Change the System Change Option**	A significant risk emerges when unapproved users can modify the System Change Option in the SAP system. Unauthorized alterations to the System Change Option can result in system instability, inconsistencies in data, and potential data loss. These disruptions could adversely affect the organization's operational efficiency and data integrity.	The "Change the System Change Option" control is structured to inhibit unapproved users from modifying the System Change Option in the SAP system. This control serves to avert system instability, data inconsistency, and potential data loss caused by unauthorized alterations. To maintain the reliability of the system, this control requires responsible individuals to probe into historical changes, identifying and rectifying any irregularities, thereby upholding the system's stability.
SAP – Basis	**Client, Change Option + via Tables**	If unapproved users are able to change client options, it could lead to data inconsistencies and potential system instability. These disruptions could adversely affect the organization's operational efficiency and data integrity.	This control regulates access to the client options in the SAP system, allowing only approved users to make changes. It mitigates the risk of unapproved alterations, ensuring data integrity and system stability. Regular investigation of user activity facilitates the detection of any unauthorized changes, aiding in maintaining system security.
SAP – Basis	**External Commands, Restricted Access**	Unapproved access to operating system commands could lead to unauthorized or malicious command execution, potentially causing system instability or security breaches. Such incidents could lead to data loss, disruption of operations, or other adverse effects on the organization.	This control restricts access to operating system commands to approved users only. Investigations into user command activity are facilitated, enabling the detection and response to any unauthorized command executions.
SAP – Basis	**Audit log, delete security audit log**	If unapproved users have the ability to delete security audit logs, it could result in the loss of crucial audit information. This could hinder investigations into potential security incidents, potentially compromising the organization's security posture and regulatory compliance.	This control restricts the deletion of security audit logs in the SAP system to only approved users. By doing this, the control ensures the preservation of crucial audit information and helps mitigate potential security risks. An investigation process is included, allowing for the monitoring of log deletion activity and the prompt detection of unauthorized log deletions.

Category	Title	Risk Description	Control Description
SAP – Finance	**Vendor Master Data, Dual Control, and Sensitive Fields**	There is a risk of unauthorized or fraudulent changes to the vendor master data, potentially leading to financial loss or legal implications. Lack of dual control over sensitive fields can allow alterations without sufficient scrutiny, enabling fraudulent activities. Also, inappropriate access to sensitive fields can lead to data breaches and violation of privacy regulations.	This control includes two separate controls that are designed to prevent fraudulent activity related to vendor master data. The first control involves the requirement for two independent users to approve any changes to sensitive vendor master data fields, while the second control involves a periodic review of changes to sensitive master data fields and verification against supporting evidence.
SAP – Finance	**Closed Period Payment Posting**	Users with access to both the Posting Periods and Account Receivable Payment Posting functions may be able to post false or incorrect entries in a previous accounting period, leading to inconsistencies and incorrect reporting.	The Posting Periods and Account Receivable Payment Posting control is designed to ensure that users cannot open previously closed periods and inappropriately post payments after monthly closure, while also investigating historical changes.
SAP – Finance	**Activity Allocation in Closed Periods**	Users with access to both the Activity Allocation and Posting Periods functions may be able to allocate activities to closed periods, leading to inconsistencies and incorrect reporting.	The Activity Allocation in Closed Periods control is designed to ensure that users cannot allocate activities to previously closed periods after monthly closure, while also investigating conducted historical actions.
SAP – Finance	**Bank Master Maintenance and Payments to Vendor**	The risk intensifies when the same individual can conduct Bank Master Maintenance and Payments to Vendors. This can potentially lead to financial irregularities and damage the organization's credibility with its vendors and financial institutions.	This control aims to identify potential fraud involving the creation of fictitious bank accounts and unauthorized payments to vendors. Specifically, the control checks whether any users who have access to both bank master maintenance and payments to vendors have made any unapproved or unauthorized changes. Additionally, the control checks for any users who have approval authority for both functions and investigates any instances where the same user has conducted both sides of the conflict.

Category	Title	Risk Description	Control Description
SAP – Finance	**Posting Periods and Posting General Ledger Journal Entry**	If users with access to both the Posting Periods and Posting GL Journal Entry functions make unapproved entries into previous accounting periods, it could result in inaccurate or fraudulent entries. Such inaccuracies could introduce inconsistencies in financial reporting and misrepresent the true financial status of the organization. Furthermore, these irregularities could disrupt the auditing process and result in potential compliance issues.	The control ensures that approved users cannot open previously closed periods and inappropriately post entries after the monthly closure. It reinforces the integrity of financial records by preventing unauthorized postings into closed accounting periods. As part of this control, historical changes are to be thoroughly investigated by responsible parties to detect and address any anomalies, thereby ensuring the reliability of financial reporting.
SAP – Finance	**General Ledger Master Maintenance and Journal Postings**	If users who have access to both General Ledger Master Maintenance and Journal Postings functions execute unapproved actions, it may lead to the creation of fictitious GL accounts and obscure activities through journal postings. These unauthorized activities could result in inaccurate financial records and may disrupt financial audits. Furthermore, it could potentially lead to non-compliance issues and harm the reputation of the organization.	The control maintains the integrity of the GL master data and ensures that no unapproved or erroneous postings are made. It accomplishes this by requiring that changes or creations of GL master data, as well as postings, are executed only by approved users. Moreover, this control requires responsible parties to conduct thorough investigations into historical changes, facilitating the detection and rectification of any discrepancies, thereby strengthening the reliability and accuracy of financial reporting.
SAP – Finance	**Bank Master Maintenance and Cash Maintenance**	If users with both Bank Master Maintenance and Cash Maintenance functions take unapproved actions, they could potentially make unauthorized changes to bank master data or divert incoming payments. This could compromise the financial integrity of the organization, leading to financial irregularities and potential legal issues.	The control ensures that only approved users can make changes to bank master data or manage incoming payments. It enforces strict access controls and mandates that responsible individuals should probe into historical changes, identifying and rectifying any irregularities to uphold the financial integrity of the organization.
SAP – Finance	**Vendor Invoices Maintenance and Journal Postings**	Users with simultaneous access to Vendor Invoices Maintenance and Journal Postings functions could potentially undertake unapproved actions. This might entail manipulating balances through vendor invoice entries, subsequently concealed via journal postings. Such actions can precipitate financial inaccuracies, complicate audits, and potentially invoke legal repercussions.	The control is designed to preclude balance manipulation through illicit vendor invoice entries and subsequent journal postings. By enforcing stringent access restrictions, only approved users are permitted to execute these tasks. Additionally, the control necessitates that responsible parties diligently scrutinize historical changes, identify and rectify irregularities, thereby safeguarding the organization's financial accuracy.

Category	Title	Risk Description	Control Description
SAP – Finance	**Customer Payments and Journal Postings**	When individuals access both customer payments and journal postings, financial manipulation may occur. Unauthorized alterations could lead to inaccurate records, disrupt audits, and potentially undermine the organization's credibility.	The control safeguards financial balances by restricting access to approved users. It mandates responsible individuals to probe into historical changes, rectifying any irregularities to uphold financial integrity.
SAP – Finance	**Bank Master Maintenance and Payments from Customer**	When users have access to both bank account creation and customer payment processing, there's a heightened risk of payment fraud through the creation and misuse of fictitious bank accounts. This could disrupt financial audits and impact on the organization's financial stability, potentially damaging its reputation in the long term.	This control ensures that approved users with both bank account creation and payment processing permissions cannot engage in unauthorized activities. To maintain the financial stability of the organization, this control mandates an in-depth investigation into historical changes, ensuring the rectification of any detected discrepancies.
SAP – Finance	**Maintain Posting Periods and Process Vendor Invoices**	When users have the ability to manipulate both posting periods and vendor invoices, there is a risk of misrepresentation in financial reports. Such actions could compromise the organization's financial stability and audit compliance.	The "Maintain Posting Periods AND Process Vendor Invoices" control mitigates the risk of inaccurate entries from previous periods by approved users. This control necessitates detailed investigations into past modifications, thereby maintaining the financial accuracy of the organization.
SAP – Human Capital Management	**HR Transactions, Access All**	The risk arises when unrestricted users have access to all HR transactions. Unapproved access and potential fraudulent activities could disrupt HR operations and compromise the confidentiality of sensitive employee data.	This control focuses on identifying and limiting the authorization to access all HR transactions to approved users only. The goal is to prevent unauthorized access and mitigate potential fraudulent activities. This control requires an investigation into any changes made to the HR transactions, ensuring only authorized modifications are made, hence upholding the integrity and transparency of the organization's HR operations.
SAP – Human Capital Management	**HR reports, Broad Access**	Unauthorized users with broad access to HR reports present a significant risk. These users can override the P_ORGIN and PERNR authorization objects, potentially leading to unauthorized alterations of HR data and potential breaches of data privacy.	The control is designed to ensure that no unauthorized users have extensive access to HR reports. This control is particularly crucial because users with this access can override the P_ORGIN and PERNR authorization objects. By scrutinizing users' access rights and applying strict restrictions, this control effectively reduces the risk of unapproved access and potential misuse of sensitive HR data.

Category	Title	Risk Description	Control Description
SAP – Human Capital Management	**HR Tables, Change Person Data**	Unapproved users with the ability to modify all HR tables related to person data pose a risk to data integrity and compliance with data privacy regulations. Unauthorized modifications to these tables could lead to inaccuracies in personal data and potential breaches of privacy regulations.	The "HR Tables, Change Person Data" control verifies that no unapproved users have the ability to modify all HR tables related to personal data. By doing so, it aims to safeguard the integrity of personal data and ensure compliance with data privacy regulations. Any modifications made to these tables are to be investigated thoroughly to detect any irregularities, further enhancing the organization's data security and compliance measures.
SAP – Human Capital Management	**HR Payroll Run Release**	If unapproved users have the ability to release a payroll run, this could lead to unauthorized payroll activities, potentially causing financial discrepancies. The integrity of payroll records might be compromised, negatively impacting the organization's financial position.	This control ensures that only approved individuals can execute and activate payroll releases. It also requires a thorough investigation into past payroll releases to identify and correct any discrepancies, thereby maintaining payroll accuracy and integrity.
SAP – Human Capital Management	**HR Time, Maintain and Approval**	Unapproved users maintaining and approving employee time data could lead to inaccuracies in payroll calculations and records. This risk may result in financial inaccuracies, employee dissatisfaction, and could potentially lead to legal issues.	This control is designed to verify that only approved users can maintain and approve time data, including attendance or absence records, for employees. It necessitates an examination of past time data maintenance and approvals to ensure data accuracy prior to the payroll run.
SAP – Human Capital Management	**Employee Master Data Maintenance and Payroll Maintenance**	If unapproved users can maintain employee master data and alter payroll results in SAP HR, this could lead to unauthorized creation, modification, or deletion of personal information, payroll data, or time management data. Unapproved alterations to payroll results, including adjustments to wage types, bonus payments, and retroactive pay, could also occur. These actions pose a significant risk of financial discrepancies, breaches of employee privacy, and potential legal consequences.	This control restricts access to personnel master data and payroll results modification within SAP HR. Only approved users should create, modify, or delete personnel master data, or alter payroll results. The control necessitates a detailed review of personnel master data and payroll alterations to identify and rectify any irregularities.
SAP – RFC Connection	**RFC - Administrator**	If unapproved users manage RFC connections, it can pose significant security threats to the organization. Such users may lack the necessary knowledge or may act maliciously, leading to potential data loss or system instability. The consequence could be severe, disrupting the smooth operation of the SAP system and potentially causing significant data loss.	The control safeguards in the SAP system by strictly limiting the management of Remote Function Call (RFC). By preventing unapproved users from managing these connections, the control ensures protection against potential system instability and data loss, thereby maintaining the integrity and reliability of the system.

Category	Title	Risk Description	Control Description
SAP – Role and Authorization	**Transactions, call any**	Unapproved access to any transaction codes could result in severe consequences. Unauthorized users could potentially access sensitive data or execute critical transactions, posing a risk of misuse, errors, or fraud. This can lead to data breaches, unauthorized transactions, and potential disruption to the organization's operations.	The control is designed to secure the SAP system by allowing only approved users to execute any transaction codes. Transaction codes in SAP are shortcuts to various functional and technical areas of the system. Ensuring that only approved users have this power is vital in reducing the risk of unauthorized transactions and preventing potential data breaches. With continual investigation, it prevents unauthorized access to transaction codes.
SAP – Role and Authorization	**HR Payroll Run Release**	If unapproved users have the ability to release a payroll run, this could lead to unauthorized payroll activities, potentially causing financial discrepancies. The integrity of payroll records might be compromised, negatively impacting the organization's financial position.	This control ensures that only approved individuals can execute and activate payroll releases. It also requires a thorough investigation into past payroll releases to identify and correct any discrepancies, thereby maintaining payroll accuracy and integrity.
SAP – Role and Authorization	**Profiles, maintain**	Unauthorized changes to user profiles can pose a significant risk. Unapproved users may alter permissions in a way that compromises system security, leading to potential unauthorized activities and security breaches. This could result in data loss or unauthorized access to sensitive information.	The control prevents unapproved users from modifying user profiles in the SAP system. This control ensures the stability and security of the system by only allowing approved users to make changes. It also facilitates the investigation of historical unauthorized modifications of user profiles.
SAP – Role and Authorization	**Roles, maintain**	If unapproved users are allowed to maintain roles, it could lead to a compromise in system security. They might grant excessive privileges, which can result in unauthorized transactions or access to sensitive data. Such a situation can potentially lead to misuse, errors, or fraud.	The control restricts the maintenance of user roles to approved users only, preventing the risk of granting excessive privileges to unapproved users. User roles in SAP define the access rights for different transactions, and unauthorized changes to these roles can lead to security breaches. Regular investigation ensures that only authorized users maintain user roles.
SAP – Role and Authorization	**SAP_ALL & SAP_NEW Profile Assignment in Production**	Unauthorized assignment of SAP_ALL and SAP_NEW profiles to users can pose a significant security risk. These profiles provide full access to the system, and if assigned to unapproved users, can potentially lead to data breaches, unauthorized system changes, and other malicious activities. This could disrupt the system's operation and compromise sensitive information.	This control ensures that only approved users are assigned these profiles, significantly reducing the risk of security breaches. By limiting the assignment of these powerful profiles, the control helps maintain the security and integrity of the system. This control includes an investigation section to prevent unauthorized assignment of critical profiles.

Category	Title	Risk Description	Control Description
SAP – Role and Authorization	**Transactions, call any**	If inactive users are not automatically logged off, it could allow unapproved individuals to exploit their open sessions. This can result in unauthorized access to sensitive data or system functions, potentially leading to data breaches, data manipulation, or other malicious activities. These disruptions could harm the organization's operational efficiency, data integrity, and overall security.	The control is designed to enforce automatic logoff for inactive users in the SAP system. To mitigate this security risk, the control facilitates the automatic logs off of users after a period of inactivity.
SAP – Role and Authorization	**Authorizations check, Disable Check in Tcode**	The risk arises when unapproved users disable authorization checks, creating a security vulnerability. This could lead to unauthorized access to critical system functions and sensitive data, potentially causing security breaches and compromising the integrity of the system.	The control prevents unapproved users from disabling authorization checks within a transaction code in SAP. These checks are vital to ensure that users have the necessary permissions to execute certain operations. The control also includes an investigation phase to verify changes to these checks.
SAP – User Management	**User, Maintain and Password Change**	If unapproved users perform maintenance functions or change passwords, it can lead to unapproved access and potential security breaches. Unauthorized access to sensitive data and critical system functions can result in data loss, system disruptions, and other security-related incidents.	The control restricts user maintenance functions and password changes to approved personnel only. This ensures that critical functions, such as creating, modifying, and deleting user accounts, are performed by approved individuals. The control includes a regular audit process to verify the correct application of these permissions.
SAP – Order to Cash	**Credit Management and Sales Order Maintenance**	Users with access to both Credit Management and Sales Order Maintenance functions might bypass credit checks and process sales orders without proper approval, leading to potential losses and inaccurate revenue recognition.	This control is designed to prevent potential issues related to credit risk and sales order inaccuracies. The Credit Management and Sales Order Maintenance control ensures that the same user cannot manage customer credit and maintain sales orders while investigating conducted historical changes.
SAP – Order to Cash	**Customer Invoices Maintenance and Credit Management**	Users with access to both Customer Invoices Maintenance and Credit Management functions could potentially manipulate invoices and alter credit limits, leading to financial discrepancies and incorrect reporting.	This control aims to mitigate the risk of incorrect invoicing and unregulated credit management. The control ensures that users cannot simultaneously maintain customer invoices and manage credit to maintain financial integrity and accurate reporting. This control also investigates which changes have been made in regard to the conflict functions.

Category	Title	Risk Description	Control Description
SAP – Procure to Pay	**Release of Batches Which Are Not Inspected**	It is a risk that users might release product batches that have not undergone necessary quality checks, leading to the distribution of potentially defective or non-compliant products.	This control targets potential quality issues by ensuring that product batches are properly inspected before release. The control ensures that only inspected batches are released to maintain product quality and compliance.
SAP – Procure to Pay	**Purchase Order Maintenance and Purchase Order Release**	Users with access to both Purchase Order Maintenance and Purchase Order Release functions could potentially alter orders and then release them without appropriate checks, leading to financial losses and discrepancies with suppliers.	This control aims to prevent unauthorized changes to purchase orders and the release of incorrect or fraudulent orders. The control ensures that users cannot both maintain and release purchase orders without separate approval to maintain financial accuracy and supplier relationships, while also investigating conducted historical actions.
SAP – Procure to Pay	**Inventory Count and Adjustment**	Incorrect or fraudulent manipulation of inventory levels can constitute a risk. Discrepancies between the recorded and actual inventory could lead to financial misstatements, stockouts, or excess stock, all of which have operational and financial impacts. Unmonitored inventory adjustments could also enable theft or misuse of inventory.	This control ensures that users are not able to intentionally or unintentionally manipulate the stock quantity by checking for any receive or issue of incorrect amounts and adjusting via the IM stock count. By performing this control, organizations can detect and prevent any potential fraud, error or misuse that could occur during the inventory count and adjustment process.
SAP – Procure to Pay	**Purchase Order Approval and Process Vendor Invoices**	The risk arises when a single individual can access the functions related to both Purchase Order Approval and Vendor Invoice Processing. The lack of segregation of duties can potentially facilitate fraudulent activities, leading to financial discrepancies and impairing trust in business relationships. To mitigate this risk, a clear division of these responsibilities is essential.	This control is designed to identify a segregation of duties conflict where the same user is able to approve Purchase Orders and Processing Vendor Invoices, while also examining changes in the past.
SAP – Procure to Pay	**Purchase Order Maintenance and Goods Receipts**	If users have access to both maintaining purchase orders and posting goods receipts, there's a risk of potential discrepancies in inventory and financial records. This could lead to inaccurate reporting and disrupt operational efficiency, posing a threat to the organization's financial stability.	The control ensures that the same approved user doesn't both maintain a purchase order and post a goods receipt. To maintain the integrity of the procurement process, this control requires an investigation into historical activities, rectifying any deviations found to maintain the organization's financial accuracy.

Category	Title	Risk Description	Control Description
SAP – Procure to Pay	**Purchase Order Maintenance and Payments to Vendor**	The risk escalates when users can both maintain purchase orders and modify vendor bank information. This can lead to unauthorized changes in vendor payment details, potentially resulting in fraudulent transactions. Such actions can significantly impact the organization's financial standing and compromise its vendor relationships.	The control ensures that no user has the ability to both maintain a purchase order and alter the bank information of a one-time vendor. In order to uphold the organization's financial accuracy, this control mandates an in-depth review of past transactions to identify and correct any irregularities in cases where both functions was conducted by the same user.
SAP – Procure to Pay	**Unauthorized employes can enter results and release batches**	If unapproved employees have the ability to enter results and release batches, it poses a significant risk. These individuals could make unauthorized changes, manipulate data, or execute transactions that could have adverse financial implications for the company. The integrity of the company's data and the security of its financial transactions could be compromised.	The control implements a series of checks to prevent unapproved employees from entering results and releasing batches. Initially, a payment proposal list is reviewed and approved by an independent authority within the company. Any modification to vendor master data requires the participation of two separate users. Periodically, a report listing all changes to sensitive master data fields (like bank account numbers) is generated and reviewed against supporting evidence. This multi-step control process ensures transparency and accountability while minimizing the risk of unauthorized actions.
SAP – Procure to Pay	**Vendor Master Maintenance and Vendor Master data Confirmation**	The risk of financial irregularities heightens when users can create or change vendor master data without following the four-eyes principle. This can lead to the creation of fictitious vendors or unauthorized changes to bank account information, potentially redirecting payments to incorrect accounts. These actions could significantly impact the organization's financial standing and vendor relationships.	The control requires the observance of the four-eyes principle to create or change vendor master data. It necessitates a review of the "Master Data Change Protocol" before each payment run. The check, performed by an approved individual without master data maintenance authorization, ensures that no single user has both maintained and confirmed changes to the Master Data.
SAP – Procure to Pay	**Process Vendor Invoices and Goods Receipts to Purchase Orders (PO)**	If one user can both receive goods and process AP invoices for the same supplier, there is an increased risk of errors, misuse, and fraud. Such a scenario could lead to misplaced goods, unauthorized invoices, and potential financial losses for the organization. This could significantly disrupt the organization's operational efficiency and financial stability.	The "Process Vendor Invoices and Goods Receipts to Purchase Orders (PO)" control is set to verify that the same approved user hasn't both received goods and processed Accounts Payable (AP) invoices for the same supplier. This control necessitates an in-depth examination of past transactions to spot and correct any irregularities when both actions are conducted by the same user.

Category	Title	Risk Description	Control Description
SAP – Procure to Pay	**Vendor Master Maintenance and Maintenance of Purchase Order**	If a user has the ability to both change vendor bank details and create purchase orders, this can pose a significant risk. This access could potentially facilitate the creation of fictitious vendors and unauthorized purchase orders, leading to financial discrepancies. The resulting irregularities could significantly affect the organization's financial health and create disruptions in its procurement process.	This control ensures that no individual user has the authority to both modify vendor bank details and create a purchase order. This control mandates a comprehensive investigation into historical transactions, aimed at identifying any anomalies where the same user has performed both tasks.
SAP – Password	**Password, initial, never logged in**	Allowing users with initial passwords who have never logged in to the system poses a risk of unauthorized access. These accounts are prime targets for hackers, who could potentially gain access to sensitive data and disrupt the system's integrity and confidentiality.	The control identifies users with default passwords who have never accessed the system. This control mitigates the risk of potential unauthorized access by ensuring these accounts are either limited or deleted. The control includes an investigation stage to ensure effective management of these accounts.
SAP – Password	**Password Length**	If passwords are allowed to be shorter than eight characters, it can significantly increase the risk of unauthorized access. Shorter passwords are easier for attackers to crack, which can lead to data breaches and compromise the security of the system.	The "Password Length" control ensures that passwords are of a minimum length, typically eight characters. This control reduces the risk of unauthorized access by making passwords harder to crack. The control includes a regular review process to maintain the enforcement of this standard.
SAP – Password	**Password, Productive Expiration**	If productive passwords remain valid for an extended period without use, it increases vulnerability to unauthorized access and potential cyber attacks. This can lead to security breaches and compromise the protection of sensitive data.	The control manages the validity period of productive passwords, ensuring they're used within a specified timeframe. By enforcing a maximum validity period, this control minimizes the risk of unauthorized access and security breaches. An investigation stage is included to verify the application of password expiration policies.

CN Internal Control Template Library

Now that you have had a look at our Top-50 control list, we hope you found it interesting, although it was only possible to share the control headlines and description. The controls selected may not be your company's initial focus and probably you would not initially need 50 or more controls to cover your risk situation. In the ComplianceNow Internal Control library, we have defined more than 150 controls templates for you to select from and new ones are continuously being added.

The Full ComplianceNow Suite

Proactive Risk Management

Access Control

- SoD mitigation in SAP
- Preventive workflow
- Fast implementation/ Low operation costs

Privileged Access Management

- Self-service firefighting
- Audit & logging
- Audit management process

Internal Control

- Centralized internal controls
- Control library - SoD risks
- Workflow & logging in a trusted system

Compliance Operation

Usage Monitor

- SAP Access analysis
- Enable data-driven decisions
- Optimize & reduce costs

Authorization Process Manager

- Remove project risks
- Reduce testing time by 75%
- Improve quality and satisfaction

Password Reset

- 24/7 self-service
- Lower admin costs
- Improve user experience

Your Assurance

- SAP certified any-premise & ext. cloud
- ISAE 3402 Type II Certified

Handholding Trough Installation

- Hosted/On-premise
- Fixed price installation support
- Full CN suite installation in 2-3 weeks

Facilitated Adoption

- CN specific extended services
- CN devoted managed services

Low Total Cost of Ownership - Why?

- Fair pricing
- Dedicated support center in DE/DK
- 3 yearly releases with updates & innovation

About ComplianceNow

ComplianceNow is an innovative product division of Nagarro, providing high-end SAP compliance solutions to improve the productivity, effi ciency, and transparency of compliace processes in companies and organizations running SAP. Our goal is to innovate, build, and deliver proven compliance products that will make a difference to our customers in their efforts towards handling the wide-reaching system complexity while adjusting to the ever more restrictive governance standards on the path to compliance.

With more than 15 years of experience building SAP compliance products, we have not only delivered a range of high-end and proven compliance products to hundreds of international costumers. But we have also built up the groundwork for constantly refining our products to meet our customers' present and future demands.

A fundamental development guideline for us is simplicity over complexity. In other words, we deliver products that work, are easy to use and with a dedicated concentration on key aspects.

Book a demo

In a one-hour demo we will show you:

- The overall flow and functions of CN Access Control
- How you work with the Risk Library, upload files and the general System Configuration
- How Access Control works with Preventive Check supporting Critical Access and SoD Functionalities
- Learn how you work with Legacy Risk Management & Legacy Approval
- Walkthrough of Risk Approval Workflow, Preventive Check Log and Rule-Set Log
- Finally, we will show you the different options for Risk Reporting and the Management Dashboard

Get in touch

info@compliancenow.eu

www.compliancenow.eu