CompliantERP

LACTALIS AUSTRALIA

Building Unprecedented Efficiency and Accuracy

How Automated Solutions are Revolutionizing User Access Reviews for a Deeper Understanding of SAP User Access

Problem Definition

SAP-dependent organizations can face significant challenges when it comes to User Access Reviews (UAR) processes, which can be laborious and complex.

User Access Review (UAR) is a crucial process that involves the periodic review of users in an SAP system and the level of access they have to data and functionality. The primary goal of UAR is to ensure that users have appropriate access to the system for legitimate and authorized purposes while minimizing the risk of unauthorized access or data breaches. Through regular UAR processes, organizations can identify any potential access issues, mitigate risks, and ensure compliance with regulatory requirements.

You would expect that knowing who has access to information, functionality, and responsibilities within an organization's SAP system should be straightforward. However, a lack of automation in this area and a reliance on manual processes such as spreadsheets can cause significant problems for companies. Failing to implement best-practice thinking and solutions for User Access Review can lead to unhappy auditors, compliance issues, and potential security breaches, which may result in a high price for the company. It's essential to prioritize automating UAR processes to ensure the security and compliance of the SAP system while minimizing the risk of potential data breaches.

User Access Review

Identifying Compliance Risks

How Do Users Gain Too Much?

Over time, it's common for users to accumulate access rights within an SAP system that are no longer necessary for their job function. When auditors come across these excess security rights during an audit, it often results in an adverse audit finding.

Unfortunately, many organizations are unaware of the extent of exposure they have, leaving them vulnerable to compliance and security risks. In light of this, it's crucial to proactively review users' access rights regularly to ensure that the correct access is given to the right people at the right time.

Organizations that rely on **manual**, **spreadsheet-driven** processes for User Access Review (UAR) are taking a **significant risk**.

A Question of Ownership

People often move jobs, departments, or go on leave, and as a result, they may retain access rights that are no longer relevant or necessary. This can leave organizations vulnerable to security breaches and access violations. Therefore, it's crucial to proactively review user access rights regularly to ensure that the correct access is granted to the right people at the right time.

When it comes to the responsibility of User Access Reviews, it's a joint effort between IT, compliance, and business teams. IT teams are typically responsible for setting up and managing the SAP system, while compliance teams are responsible for ensuring that access rights are granted appropriately to mitigate security risks and compliance violations. Finally, business teams are responsible for ensuring that users have the correct access rights to perform their job functions effectively.

It's essential to establish a clear process and assign roles and responsibilities to ensure that User Access Reviews are conducted regularly, and access rights are managed appropriately to minimize the risk of security breaches and compliance violations.

Establishing accountability for User Access Reviews can be a challenge in large organizations. The responsibility often falls on SAP managers and IT managers to ensure that the reviews are conducted regularly, and access rights are managed appropriately. However, there can be a lack of clarity around who ultimately should be accountable for access management, leading to business-versus-IT ownership issues. If the business isn't driving the process, and IT doesn't have a mandate to solve the problem, it can seem like an insurmountable challenge.

One common issue is that when organizations do attempt to tackle this problem, they often rely on manual processes, such as spreadsheets, which can be time-consuming and error-prone. Automated solutions can help overcome this challenge by streamlining User Access Reviews, ensuring that access rights are managed efficiently and effectively, thus reducing the risk of compliance violations and security breaches.

Ultimately, the responsibility for managing access rights within an SAP system should be a shared responsibility between IT, compliance, and business teams, with clear roles and responsibilities established to ensure that the process is executed efficiently and effectively.

Avoid Security Breaches

Automate Solutions

Shared Responsibility

By implementing automated **User Access Reviews**, organizations can reduce the risk of compliance violations and security breaches, improve the efficiency and effectiveness of access management.

Keep on Swimming in Spreadsheets

Manual User Access Reviews often involve extracting data into spreadsheets and sending them to various role owners, who then have to review the data line-by-line. This can be a time-consuming and frustrating process for role owners who already have a lot of responsibilities to manage. The manual process of User Access Reviews adds an additional burden to their workload, particularly during the yearly audit.

In addition to the human component, manual processes using spreadsheets also have limitations. They do not provide a real-time view of user access across the organization, making it difficult to get a comprehensive overview of access rights.

Automated solutions streamline the User Access Review process, eliminating the need for manual data extraction and review, which saves time and reduces the risk of human error. This enables role owners to focus on their primary responsibilities, rather than spending time on administrative tasks associated with User Access Reviews. Ultimately, automated solutions can help organizations ensure that access rights are managed efficiently, effectively, and in real-time, reducing the risk of security breaches and compliance violations.

By implementing automated User Access Reviews, organizations can ensure that auditors are satisfied with the organization's access control processes. Ultimately, this can have a significant benefit to the organization, improving its overall security posture and reducing the risk of fraud.

Reduce Compliance Risks

Improve Security Posture

Automated access review solutions offer a more
Secure, **Efficient**, and **Effective** way to manage user access in SAP.

Keeping This Status Quo Will Not End Well

Organizations that rely on manual, spreadsheet-driven processes for User Access Review (UAR) are taking a significant risk, especially those that run on SAP systems. The implications of this approach can be far-reaching, with potentially severe consequences. While compliance and auditors are typically the first concerns that come to mind, the risk of internal security breaches is likely to be the most pressing concern for C-suite executives.

Unhappy Auditor

If the business's auditors come to a negative conclusion, they may refuse to certify the financials, which will immediately affect any company that files reports with a stock market. The last thing that senior management wants to see is an IT manager or CFO trying to advise their board that the SAP system is too risky for the auditor to approve financial statements.

A recent example of the consequences of inadequate user access controls and security breaches can be seen in the case of the Equifax data breach in 2017. The breach compromised the personal data of over 143 million consumers, and the company faced significant financial and reputational damage. The breach also resulted in several high-profile resignations, including the CEO and CIO of Equifax.

In addition to the financial and reputational damage, the breach also had legal implications. Two years after the breach, the company said it had spent $1.4 billion on cleanup costs, including "incremental costs to transform their technology and improve application, network, and data security.

This case highlights the importance of robust user access controls and the need for organizations to take proactive measures to manage and mitigate the risks of security breaches. It's critical for organizations to implement automated solutions and adopt best-practice thinking to ensure that access rights are managed efficiently and effectively, and compliance and security risks are mitigated.

The consequences of security breaches can be much more severe, including financial losses, reputational damage, and legal ramifications.

Therefore, it is essential for organizations to prioritize automating their User Access Review processes and ensure that their SAP users have the appropriate access rights.

Successful Audits

Maintain Internal Security

Internal Fraud

There are many different ways that employees can engage in fraudulent activity, and the methods used can vary depending on the individual and the company involved. Usually, it takes the form of diverting money such as setting up as a vendor's bank details and making fraudulent payments to themselves. Others could journal a few cents or fake on multiple transactions, rounding up or down as required, and send off all those tiny amounts to their account.

Enterprises are naturally worried about internal security. Recent research says that 41% of more than 100 SAP customers surveyed from the UK, the US, Europe, and Asia thought internal fraud was the biggest threat to their SAP systems. And fraud is certainly on the rise with 51% of organisations in a 2022 global survey saying they experienced fraud in the past two years, the highest level in 20 years of this research study.

Flaws in your approach to reviewing access rights can also result in external fraud issues due to the risk of collusion where third parties are working with an insider to defraud the organisation.

The Association of Certified Fraud Examiners investigated 2110 cases from 133 countries and according to their report there is a median loss of $117,000 for fraud incidents. It also shows that nearly half of the cases occur due to lack of internal controls and the companies who have existing controls reduced their median loss by half. As it takes nearly 18 months to detect a fraud it is very important to have proper controls in place to avoid the damage that causes to one's organisation.

[Source: 2022 ACFE Report to the Nations]

With automation, the review process can be **streamlined**, freeing up time and resources for other critical security tasks.

Reputation of The Businesss

In highly competitive, consumer-facing markets, adverse publicity around being known as 'victims of fraud' can destroy even the most carefully cultivated public image. Consumers will naturally think that if a company can't even protect their own money, systems, and data...how can they be trusted with theirs?

75% of people wouldn't work in a company with a bad reputation. The reputation of your business influences not only your revenue and client relations but also your operations. Apart from the revenue and the public perception, your reputation also determines the talent you have access to. A solid business reputation will attract and retain not only loyal customers but also loyal, qualified employees. [Source: Glassdoor]

Public Image

Security Policy

Internal Buy-In

The process of reviewing access is crucial for maintaining a secure environment in any organization, but it can also be a complex and challenging task. In many cases, the burden of this task falls on role owners, who may feel overwhelmed by the additional responsibilities and time constraints. This can lead to a negative perception of security policies and protocols within the organization, making it more challenging to engage stakeholders and ensure their full cooperation in the process. A lack of engagement can ultimately compromise the security of the organization, putting it at risk of cyber threats and other security breaches.

By implementing an automated access review solution, organisations can reduce the risk of security breaches and internal fraud, while also improving the efficiency and accuracy of their access review process. Automated platforms can provide real-time visibility and control over user access, ensuring that access is appropriate and aligned with business policies and compliance requirements.

With automation, the review process can be streamlined, freeing up time and resources for other high value tasks. Additionally, automated solutions can provide detailed reporting and audit trails, helping to meet compliance requirements and demonstrate due diligence to auditors and regulators.

The Way Forward

Automated user access review solutions can provide several benefits to businesses, including streamlining the process, reducing the resources required, and minimizing the risk of errors. These solutions enable only the right people with the necessary knowledge to make the right decisions, eliminating the need for IT department involvement. Additionally, these solutions can make job shifts or position changes seamless for individuals, as well as provide a more comprehensive and systematic approach to identifying and addressing excess rights in access. Overall, adopting an automated user access review solution can lead to a more efficient, secure, and effective SAP system for businesses of all sizes.

Having a **purpose-built ruleset** that reflects the requirements of auditors can help businesses stay on top of their compliance and access risk management.

Introducing Cerpass

CERPASS® is an innovative solution developed by CompliantERP that addresses the challenges enterprises face in managing SAP access risks. The solution is designed by a team of experienced SAP security consultants with years of experience in SAP application security and audit. It provides a centralized point for access risk management, making it easy for organizations to make complex decisions based on real-time insights. With built-in trend analysis and proactive reporting, CERPASS® helps reduce the risk of compliance failures and security breaches.

CERPASS® is built on the SAP Business Technology Platform and seamlessly integrates with core SAP systems. The solution offers enterprise-level access security and compliance optimization for organizations of all sizes and budgets. Its access ruleset is tailored to address common SAP access risks across various industry sectors, making it a purpose-built solution that can help organizations improve their access security posture.

Identify And Act On Access Risk In Your Sap System With Cerpass®

The auditing standards of today are the highest ever, thus businesses of all sizes must make sure access risk is addressed as soon as possible if they want to remain compliant. Now more than ever, SAP access security is necessary due to the repercussions of a failed audit, a systems breach, or reputational damage. CERPASS® was specifically developed with these demands in mind based upon five key elements.

Dashboards, Trending And Reporting

With Cerpass, you can identify and act on access risk in your SAP system in real-time. The platform includes built-in what-if modelling and functionality that enables you to take actions like removing access or changing role designs. Scheduled and ad-hoc system scans can pinpoint the cause of any access security violations, while simulations of real-life scenarios can help you anticipate the impact of any changes you make. Cerpass also features multiple reporting modules designed to meet specific business needs and trending capabilities that allow you to analyse access risk over time.

User-Focused Interface

With CERPASS®, the setup process is simple and easy, and the user-friendly interface requires little to no technical skills. The built-in application wizards enable users to create new rule sets and customize them as needed. The platform provides complete visibility into access risk across the entire breadth of SAP's core ERP capability, making it easier to identify potential threats and take action quickly. Additionally, CERPASS® scans data nightly, providing a comprehensive view of the access risk posture in the SAP system on a daily basis.

Robust Access Risk Ruleset

The team at CompliantERP are highly experienced and have developed an access ruleset that is purpose-built to identify common SAP access risks. Having a purpose-built ruleset that reflects the requirements of auditors can help businesses stay on top of their compliance and access risk management. Regular updates to the ruleset also ensure that it stays current and relevant to any new industry or audit requirements. This can provide peace of mind for businesses, knowing that they are always up-to-date with the latest regulations and can make decisions with confidence.

CERPASS® is designed for easy integration with other SAP applications and runs on the SAP HANA® in-memory database.

Business Control Functionality

The business-controls capability in CERPASS® provides organizations with an additional layer of risk management, allowing them to implement controls for users who present specific risks. These controls can be scheduled and recorded automatically and can be customized to meet the specific needs of different divisions within an organization. Real-time reporting and dashboards also provide increased visibility into compliance with controls being deployed.

Integrative Interoperability

CERPASS® is designed for easy integration with other SAP applications and runs on the SAP HANA® in-memory database. The product is built directly on the SAP Business Technology Platform (SAP BTP), which ensures seamless integration with other SAP applications. The custom integration capability simplifies data integration, and data extracts can be scheduled to match your business change cycles. The user interface utilises SAP Fiori, which provides a familiar look and feel to those already using SAP technologies.

Lactalis Sees Access Visibility Transformed, Compliance Guaranteed

Lactalis Australia is a dairy company owned and operated by the Lactalis Group, with a workforce of over 2500 employees collaborating with 500 Australian farmers to produce high-quality dairy products. As a company that runs SAP, they were faced with an annual system audit that reviewed access assignments of all staff, but was challenging to achieved as it was always dreaded IT and the business alike.

For years, the IT Services Manager at Lactalis Australia, had been responsible for ensuring the annual system audit that reviewed access assignments of all staff was completed.

However, like many companies in a similar position, he was relying on spreadsheets to manage the process. As more role owners reported how time-consuming it was, he recognized the need for a change. Multiple spreadsheets were being sent to various role owners, leading to delays and a lack of visibility for the team. Role owners wanted a way to quickly summarize data, make informed decisions, and focus on their daily tasks. Realizing that there had to be a better solution, Lactalis Australia chose CERPASS® as the optimal solution to meet their onsite requirements.

Tailor-Made Implementation

What happened next:

1. Lactalis were the original pilot site for CERPASS®. The development, testing and activation of the User Access Review feature was planned to be deployed just in time for the annual review. The activation is a simple feature switch, followed by populating the role repository with the roles to be reviewed and assigning process ownership.

2. With the roles flagged for review and assigned to relevant owners, the next steps were to define each UAR workflow definition per process owner. The definitions then generate workflows for review that contain all users within the Lactalis system that are assigned to the Owner's roles. As this is by role ownership by process, the next time the workflow is scheduled to generate, the workflows will dynamically generate based upon this already defined selection criteria, ensuring all roles owned and all users assigned will get reviewed. This is where the true automation kicks in, as the dynamic workflow definitions will always pickup current state when they fall due, ensuring nothing gets missed.

3. With the workflows generated, the Security Administrator booked 1 on 1 sessions with each Owner to train them in the UAR process and using CERPASS. Once the first few roles were walked through, the owners were off and running, each completing their review obligations in record time.

Complete **visibility** on the entire access review process and tasks, including high-risk transactions.

Statistically Impressive

- 600 SAP security roles in review.
- 29 generated UAR workflows across all Processes and Subprocesses.
- 55,000 role assignments, of which 91.5% were subject to a review.
- Only 9 role reinstatements required after role removals were performed.
- UAR cycle completed in 1/3 of the time compared to
- the previous year.

Results – At A Glance

These are the benefits that Lactalis Australia has experienced since implementing CERPASS®:

- Complete **visibility** on the entire access review process and tasks, including high-risk transactions, allowing for more effective risk management.
- A **simpler** and **cleaner** interface that makes it **easier** to make decisions and take actions.
- **Consolidation** of the entire process back to just one month, compared to the previous three-month process that involved spreadsheets.
- Increased **buy-in** from role owners due to the ease of use of the tool, resulting in quicker completion of tasks and better attention to the user access review process.
- A shift from a dreaded annual audit process to an accepted compliance task that greatly benefits business operations.

Complete Visibility

Simpler Interface

Increased Buy-In