

Pactiv Evergreen's Access Management Playbook: Streamlining Processes and Simplifying Acquisitions

Satyen Mehta, Director of IT Enterprise Systems at Pactiv Evergreen Inc.
Jennifer Noe, Director of IT Compliance at Pactiv Evergreen Inc.

Las Vegas

2024

SAPinsider



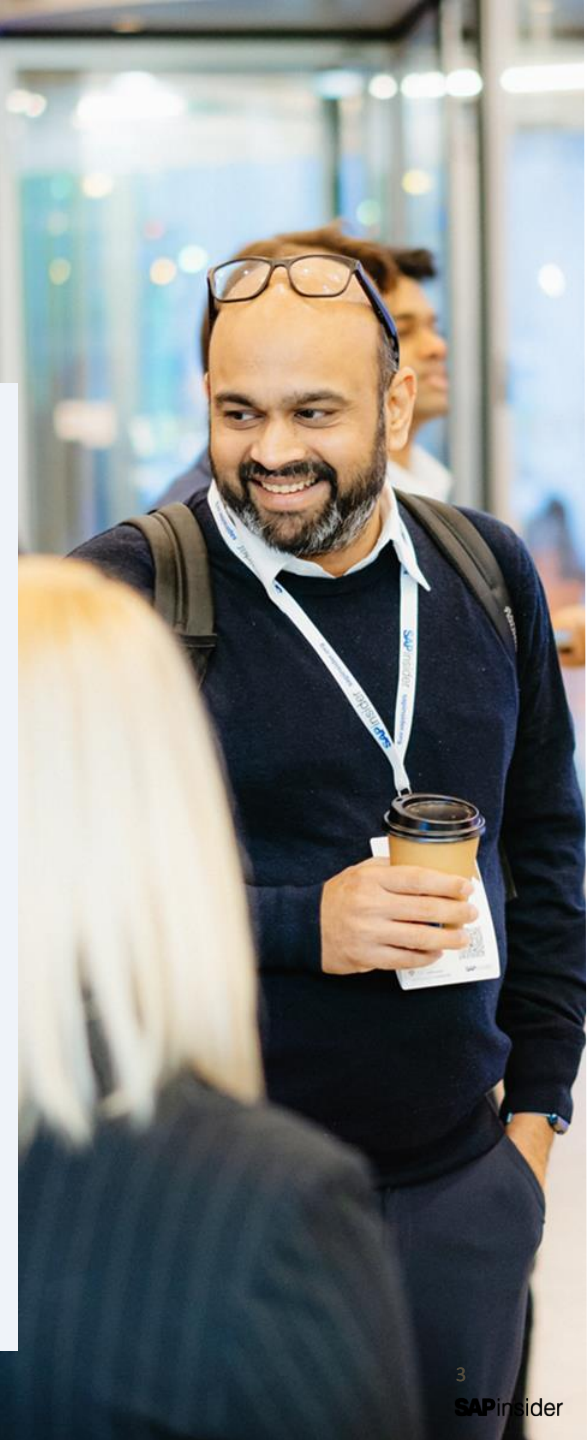
In This Session

Learn about how Pactiv Evergreen:

- **Transformed their complex SAP environment** by successfully redesigning their security and utilizing SAP GRC's business role concept
- **Streamlined the end-user experience** by implementing SAP GRC Access Request Management
- **Built an SAP Access Management Playbook** to simplify the process of bringing newly acquired businesses onto their existing SAP landscape

What We'll Cover

- Company Overview
- Pactiv's SAP Transformation Project
- Laying the Foundation for the Future
- Our SAP Access Management Playbook
- The Playbook in Action
- Wrap-Up



Company Overview:

Pactiv Evergreen



Pactiv Evergreen is a leading manufacturer of **fresh food and beverage packaging** in North America.

Pactiv Evergreen has over **14,000** unique products that people use **5 BILLION** times each week in the U.S. alone.

In 2020, Pactiv and Evergreen Packaging came together as part of a public offering under the name **Pactiv Evergreen** (NASDAQ: PTVE).



Project TRIO Objectives

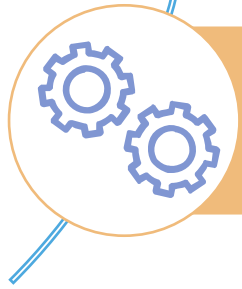
In 2020, Pactiv embarked on a journey that we called **Project TRIO (Transforming Risk Into Opportunities)**. The following were our objectives:



Redesign SAP security roles in enabling effective Segregation of Duties (SOD) risk management by aligning user access with how the business uses SAP to process transactions.



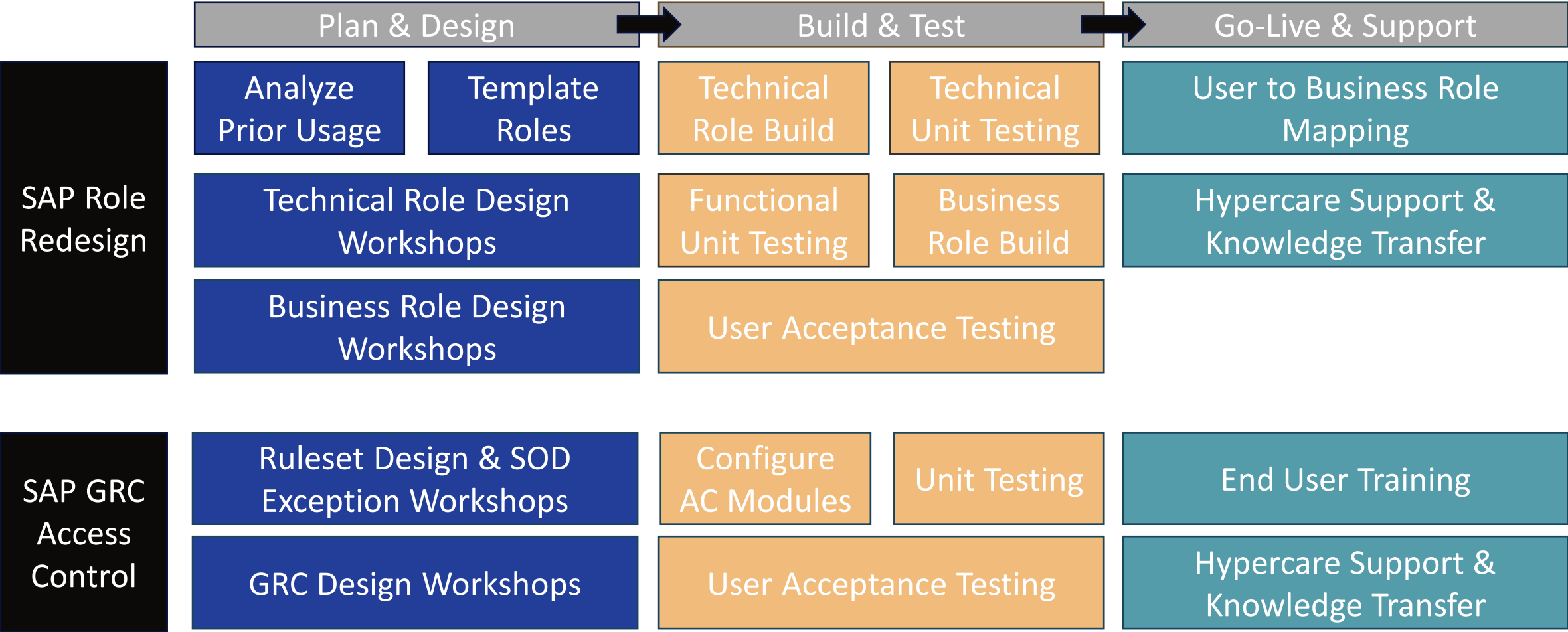
Refresh the SAP SOD ruleset to align with management's priorities and external audit applicable risks.



Configure the SAP GRC Access Control Access Request Management, to automate user provisioning in the SAP system and User Access Review for user access certification, modules of Pactiv's existing SAP GRC solution.

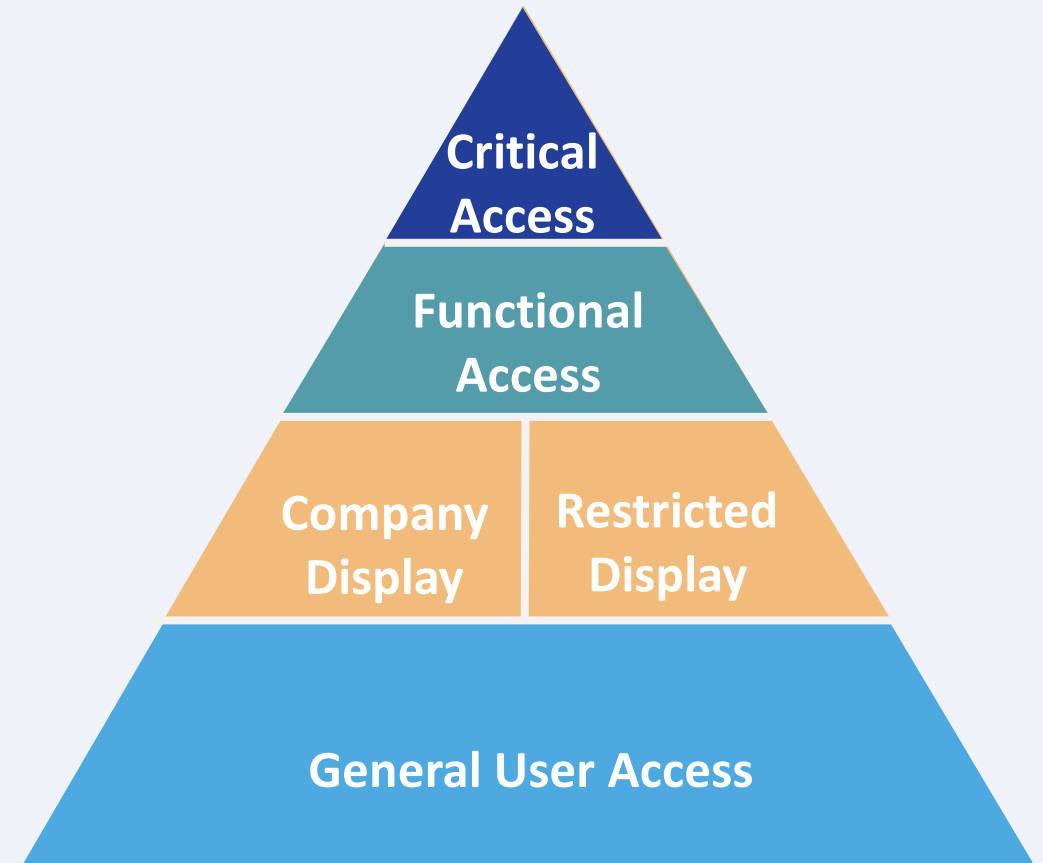
Project Approach

We had a multi-workstream, multi-phased approach to achieve our objectives, as follows:



Key Principles for Sustainability

- A **4-tiered role architecture** was employed to designate access (ex. display vs update) within task roles.
- A **role naming convention** was established so roles would be easy to identify and to understand the access granted within each role.
- **Proper ownership** of task roles and business roles was established during role design workshops. Same individuals would be included in GRC to approve role assignments to users.
- All task roles were built **SOD-free**.
- A **least privileged user access** approach was adopted to reduce excessive access in the system.
- The repository of mitigating controls in GRC were mapped to the **internal controls framework**.



Laying the Foundation for the Future

We were able to achieve the objectives set forth by TRIO and establish a clean foundation that we could build from.

Existing SOD Ruleset enhanced to be **comprehensive** of all potential risks and **signed-off by Functional Leads**.

New **SOD-Free** task roles created for **all business functions** across Pactiv.

New SAP **user provisioning process through GRC** implemented and deployed to users for 4 SAP systems, **simplified** with the use of business roles.

Preventative SOD check built-in to provisioning process and **involves Managers** up-front for risk acceptance.

100%

Reduction in
Role-Level
SOD Risks

27%

Reduction in
number of
users with
SOD Conflicts

40%

Reduction in
average number
of transactions
assigned to
users

Reduction from
average of 27
task roles per
request to
average of **2
business roles
per user.**

Lessons Learned from Project TRIO

- **Involvement Commitment** is fundamental and necessary from beginning to end
- Essential to have a **Change Management Plan** in place for the key stages and milestones of the project
- **Governance** is critical to project success
- Remember that this is not just “Once & Done”



SAP Access Management Playbook

After the TRIO journey, it was clear we needed to **build a playbook** to bring in new business units (i.e., Evergreen) or new acquisitions (i.e., Fabri-Kal) into our existing SAP environment.

This playbook would allow for a **consistent approach** for each “integration” project and ensure all the appropriate SAP Security and GRC-related tasks were completed prior to Go-Live.

Our playbook has two parts:

1) Onboarding Questionnaire

- Basic questions regarding the business unit / organization that will be integrated into Pactiv’s existing SAP landscape

2) Checklist of Project Activities

- Detailed list of Security and GRC activities broken into categories and with appropriate ownership noted for each

SAP Access Management Playbook – Example

The following is an example of a question from the onboarding questionnaire.

- Only Yes or No questions to drive activities checklist
- Additional tabs are provided in the file for reference

#	Question	Answer
1	<p>Will the BU/Org be bringing in any new organizational elements?</p> <p><u>Examples:</u></p> <ul style="list-style-type: none">- Company Codes- Purchasing Groups- Plants- Divisions- Shipping Points <p>*Refer to tab “Org Elements” for full list of organizational elements that are currently being restricted in each Production System</p>	Yes

SAP Access Management Playbook – Example (Continued)

The following are examples of Security/GRC activities from the checklist.

- Based on the answers from the questionnaire, certain activities will be noted as required

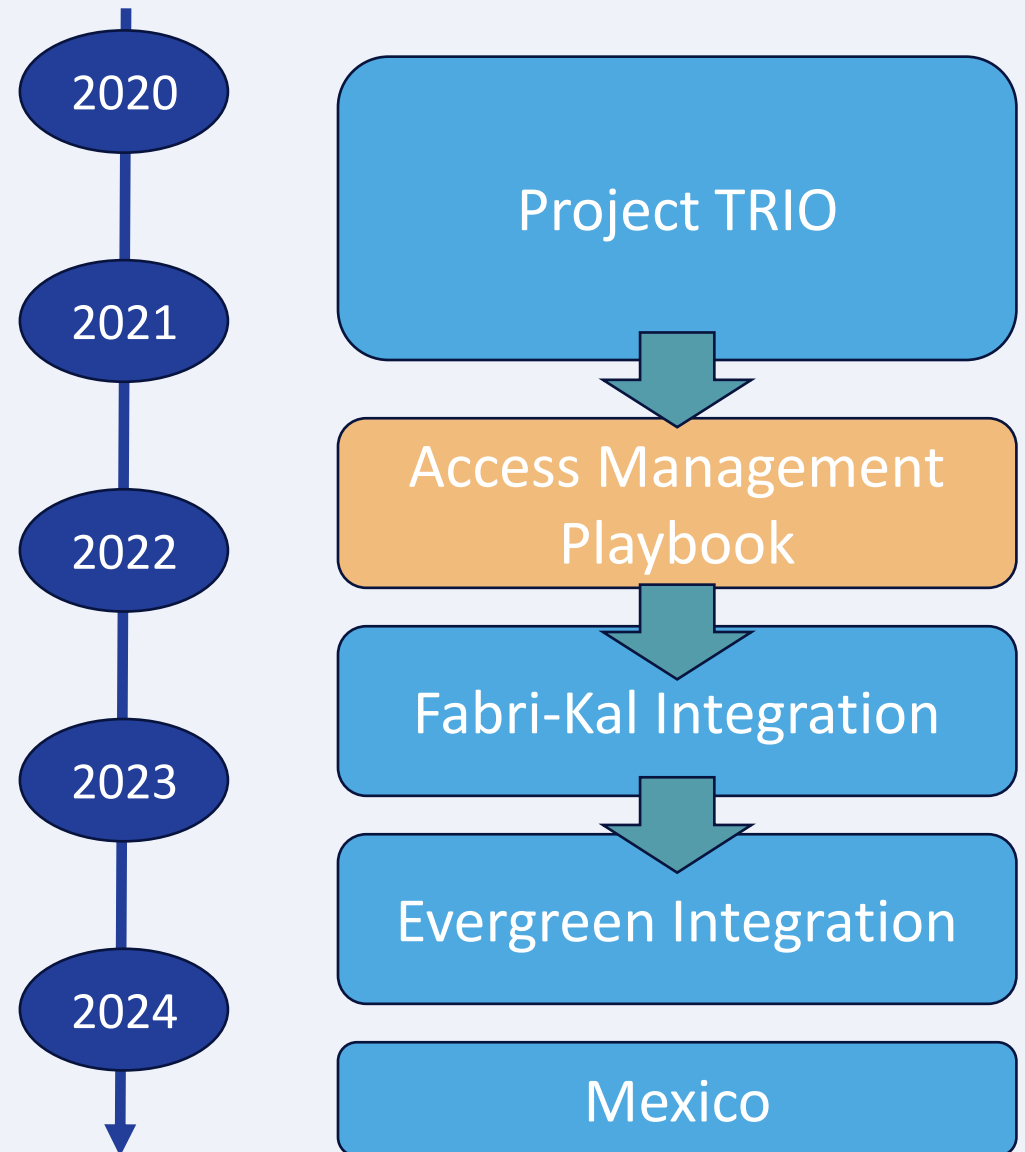
#	Activity	Required?	Owner
B	Role Maintenance		
B.1	Identify all new organizational elements that will be added into your existing SAP system.	Yes	SAP Security Team
B.2	Identify all business processes and tasks that will be performed by new business unit / organization	Yes	SAP Security Team
B.3	Determine all relevant (based on business process tasks identified) SAP master roles which will need to be derived and build a list of all new task roles that need to be created.	Yes	SAP Security Team
B.4	Determine all relevant (based on business process tasks identified) GRC business roles which will need to be created / updated and build a list of them	Yes	SAP Security Team

The Journey Continues...

In 2021, Pactiv Evergreen acquired a foodservice and consumer brand packaging manufacturer Fabri-Kal Corporation.

In 2022, Pactiv completed a project to integrate Fabri-Kal **(550+ users)** into the existing SAP environment.

In 2023, Pactiv completed a project to integrate Evergreen **(800+ users)** into the existing SAP environment.



The Playbook in Action

Thanks to the Playbook we built, we had all the key required activities already outlined for both our Fabri-Kal integration and Evergreen integration projects.

SOD Ruleset Design

Role Maintenance

User Mapping

User SOD Evaluation

Access Provisioning

Go-Live & Hypercare

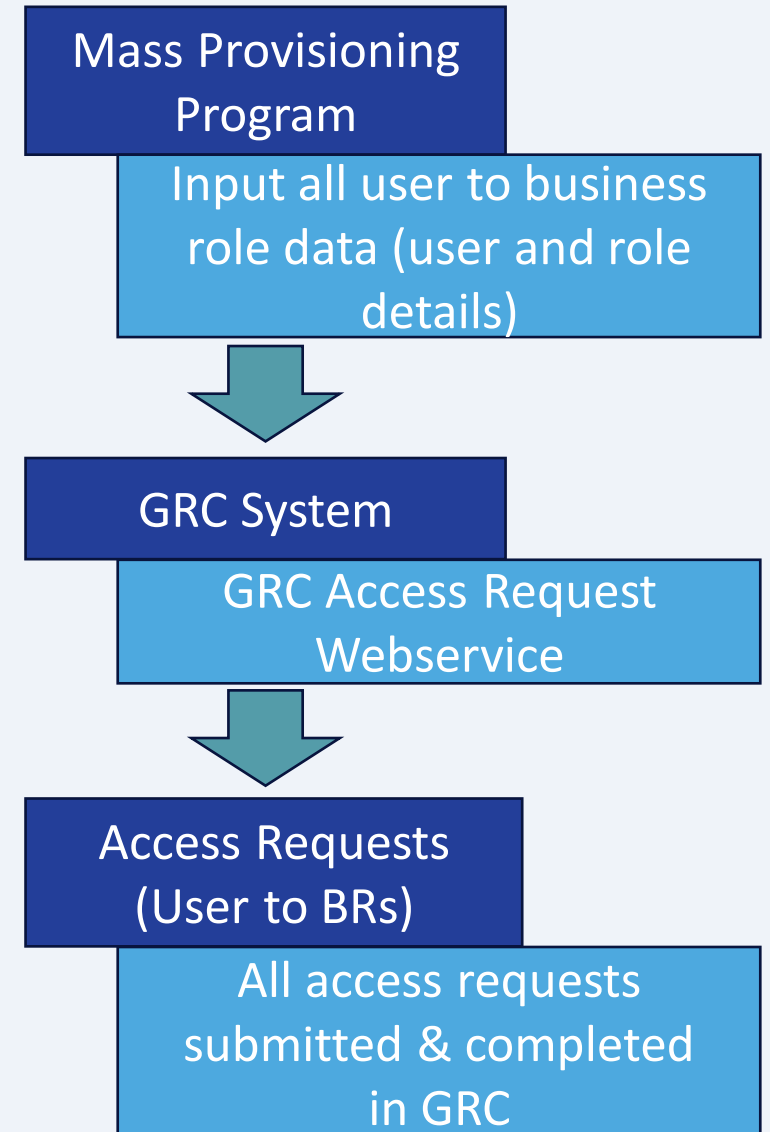
Mass User Access Provisioning

When migrating a large number of users into your existing SAP environment, note the following:

- If using GRC business role to user assignments, you **must** provision access to users through GRC Access Request Management to maintain the user to GRC business role relationship.
- If using task role or composite role to user assignments, you can provision access directly to end users in SAP but can use GRC to maintain audit trail for all SAP access in one location.

At Pactiv, we used a custom program for both integrations to create individual GRC access requests (1300+) in mass.

- Zero-stage workflow utilized in GRC. Approvals obtained through the user mapping process.





Wrap Up

- Employ good **application access controls**
- Utilize User Access Management **Tools & Controls**
- **GRC is your BFF**
- Changes? **Obtain buy-in** from all stakeholders
- Engage a **reliable and skilled partner**

Key Points to Take Home

- Having a **clean security design** approach as your foundation is necessary when growing your business
- Utilize a GRC solution to **automate** your security processes and **reduce your risk** exposure
- Consider your **end-user experience** when designing your GRC processes and implementing technology
- Build out your **access management playbook** so you don't miss any key steps when bringing on new acquisitions
- Find the **right partner** to provide leading practice guidance and expertise to make you successful in your SAP journey

Where to Find More Information

<https://sapblog.protiviti.com/2024/01/24/system-integrator-or-security-specialist-who-should-be-responsible-for-implementing-s-4hana-security-and-controls/>

- A recent blog post discussing the importance of security, including points about building a scalable design for acquisitions

https://help.sap.com/docs/SAP_ACCESS_CONTROL

- Follow Product Hierarchy > Financial Management > Governance, Risk, Compliance (GRC) and Cybersecurity > SAP Access Control

<https://learnmore.protiviti.com/SAPInsightssubscription>

- Subscribe to SAP Insights featuring SAP blogs and monthly newsletters

Thank you! Any Questions?

Satyen Mehta, Pactiv Evergreen Inc.

Satyen.Mehta@pactivevergreen.com

[Linkedin.com/in/Satyen-Mehta](https://www.linkedin.com/in/Satyen-Mehta)

Jennifer Noe, Pactiv Evergreen Inc.

Jennifer.Noe@pactivevergreen.com

Please remember to complete
your session evaluation.

SAPinsider



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2024 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

**SAPinsider
comprises the
largest and fastest
growing SAP
membership group
with more than
800,000 members
worldwide.**
