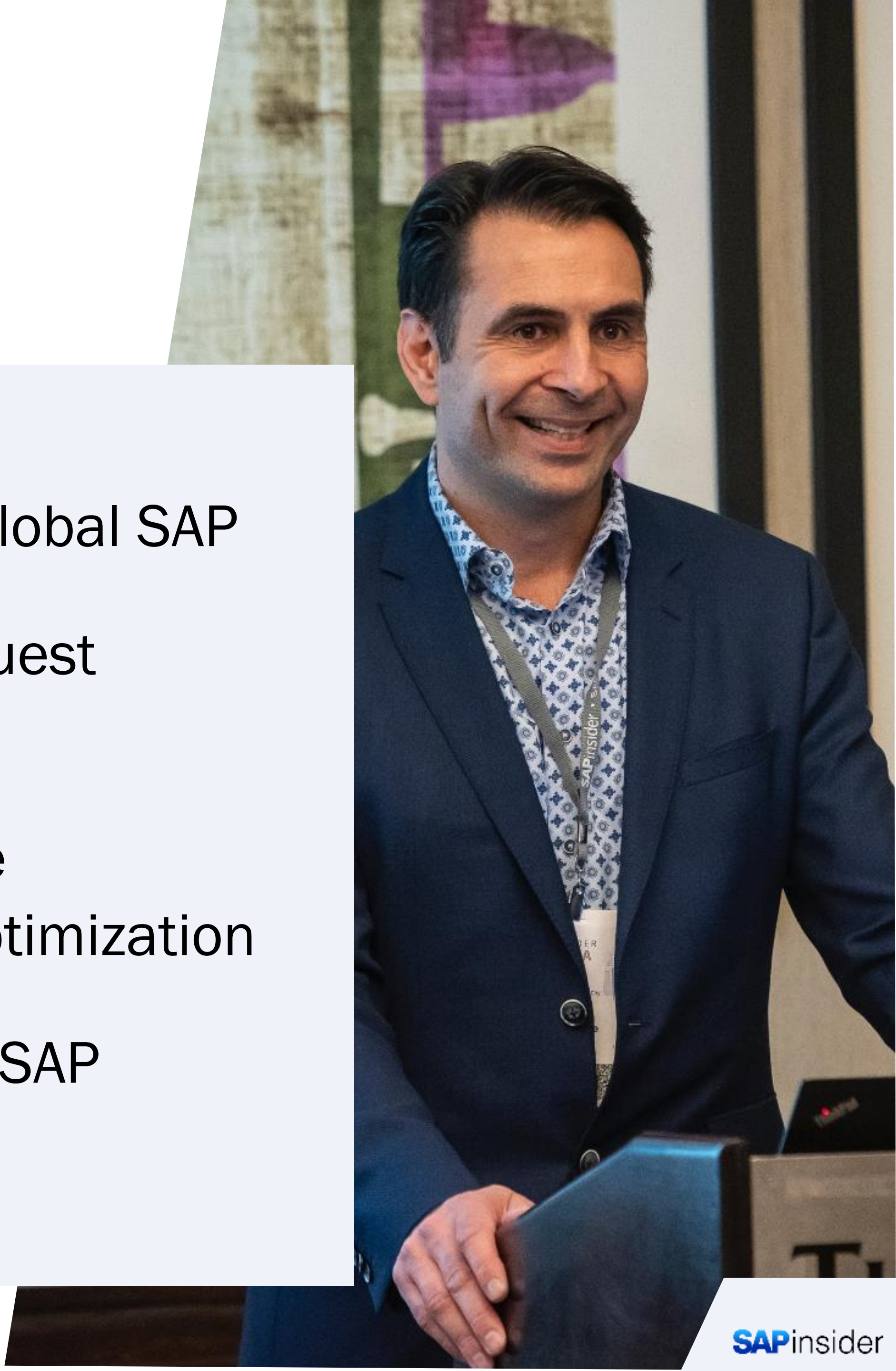
Implementation Of SAP Access Control In Kerry Group And What Comes After That

Guillermo Casado, Kerry Group

In This Session

Agenda

- Who am I / Introducing Kerry
- Kerryconnect project – Achieving a global SAP landscape
- Evolution of Kerry's SAP Access Request process
- Leavers Process IGA Integration
- Early Watch Alerts now in SAP for Me
- Self-Service Execution of Security Optimization Service via Solution Manager
- Exploring Cyber Security tools for an SAP landscape
- Wrap up



Who am I / Introducing Kerry

Who am I / Introducing Kerry

WHO AM I

GUILLERMO CASADO

ICT SAP Security Lead at

KERRY

SAP Security, IT audit and controls and GRC. Supporting project implementation and business-as-usual maintenance, as well as long term security strategy definition.

18 years of total experience in SAP
ABAP -> WM / FICO -> Basis -> Security
13 years as SAP Security expert

Accenture

PepsiCo

APTIV

Findus

Henkel

Iveco

DuPont

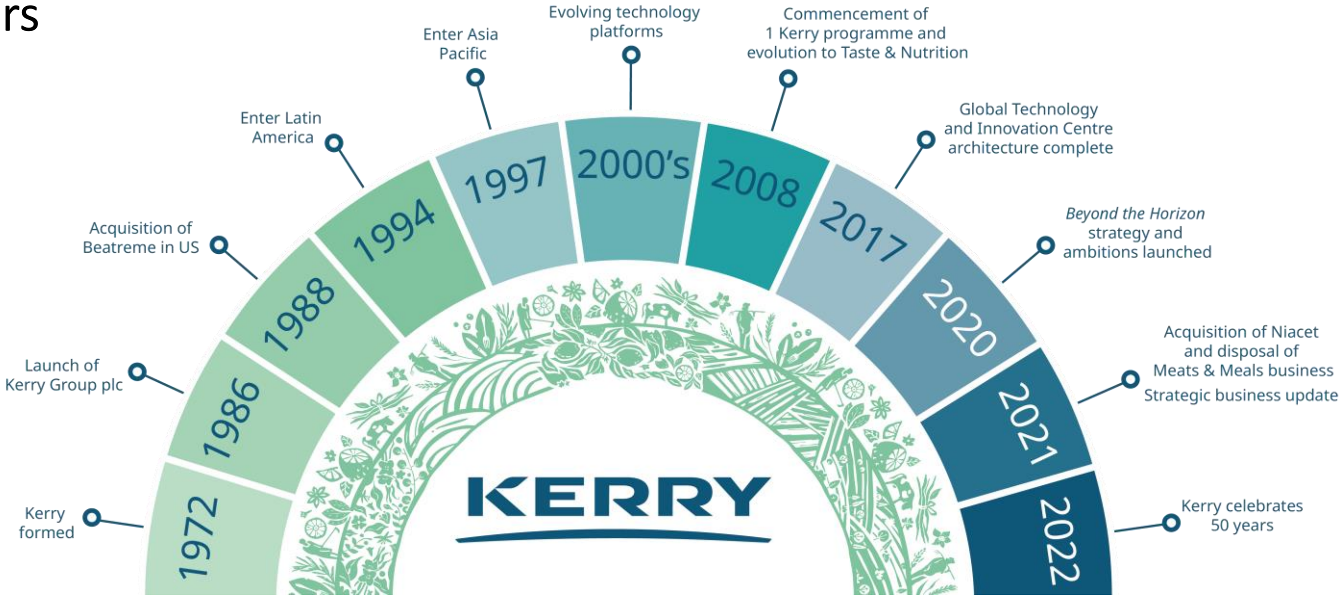
GB Foods

Damm

BAT

Who am I / Introducing Kerry

- World's leading taste and nutrition partner for the food, beverage and pharmaceutical markets, our broad range of ingredients solutions currently reaching over 1 billion consumers
- Our purpose is to inspire food and nourish life and our vision is to be our customers' most valued partner, creating a world of sustainable nutrition
- Our customers include the largest consumer goods businesses, foodservice operators, food manufacturers and pharmaceutical companies in the world, as well as some of their fastest growing challengers



1972 Kerry formed

1986 Launch of Kerry Group plc

1988 Acquisition of Beatreme in US

1994 Enter Latin America

1997 Enter Asia Pacific

2000's Evolving technology platforms

2008 Commencement of 1 Kerry programme and evolution to Taste & Nutrition

2017 Global Technology and Innovation Centre architecture complete

2020 *Beyond the Horizon* strategy and ambitions launched

2021 Acquisition of Niacet and disposal of Meats & Meals business

Strategic business update

2022 Kerry celebrates 50 years

Who am I / Introducing Kerry

€8.8bn Revenue

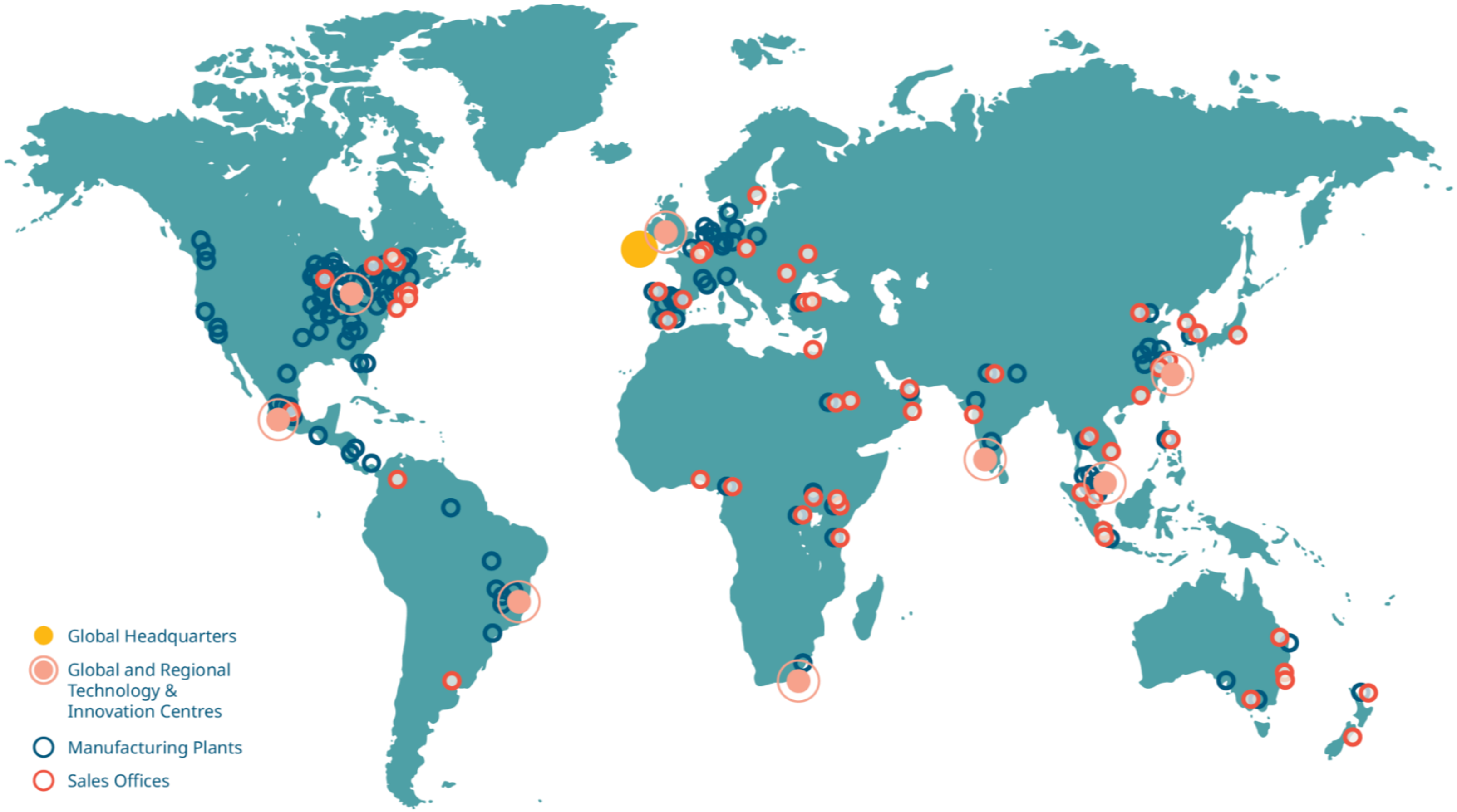
1.2bn Consumer reach

147 Manufacturing locations

70+ Technology and Innovation centres

23,000+ Employees

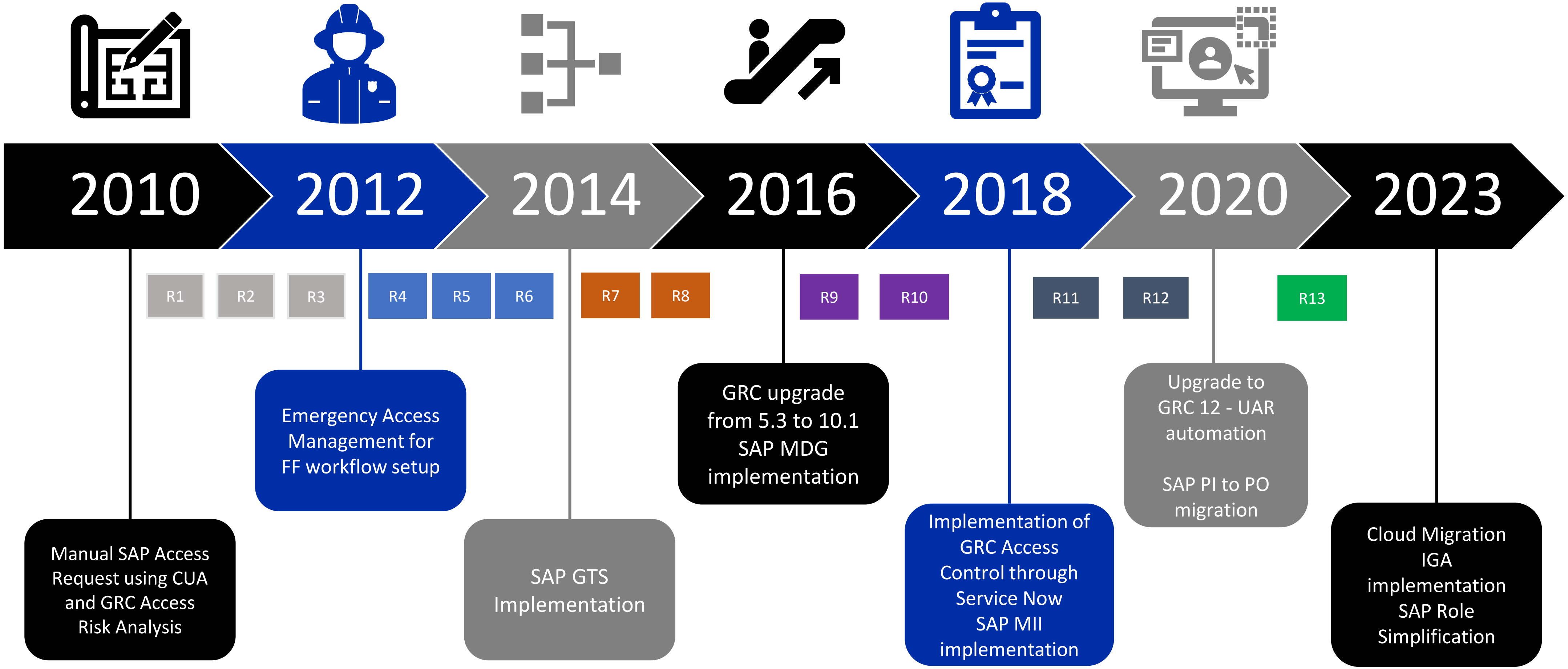
1,100+ R&D scientists



Note
Ireland & UK: 24 manufacturing plants, 2 sales offices

Kerryconnect project – Achieving a global SAP landscape

Kerryconnect project – Achieving a global SAP landscape



2010

2012

2014

2016

2018

2020

2023

R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11 R12 R13

Manual SAP Access Request using CUA and GRC Access Risk Analysis

Emergency Access Management for FF workflow setup

SAP GTS Implementation

GRC upgrade from 5.3 to 10.1
SAP MDG implementation

Implementation of GRC Access Control through Service Now
SAP MII implementation

Upgrade to GRC 12 - UAR automation

SAP PI to PO migration

Cloud Migration
IGA implementation
SAP Role Simplification

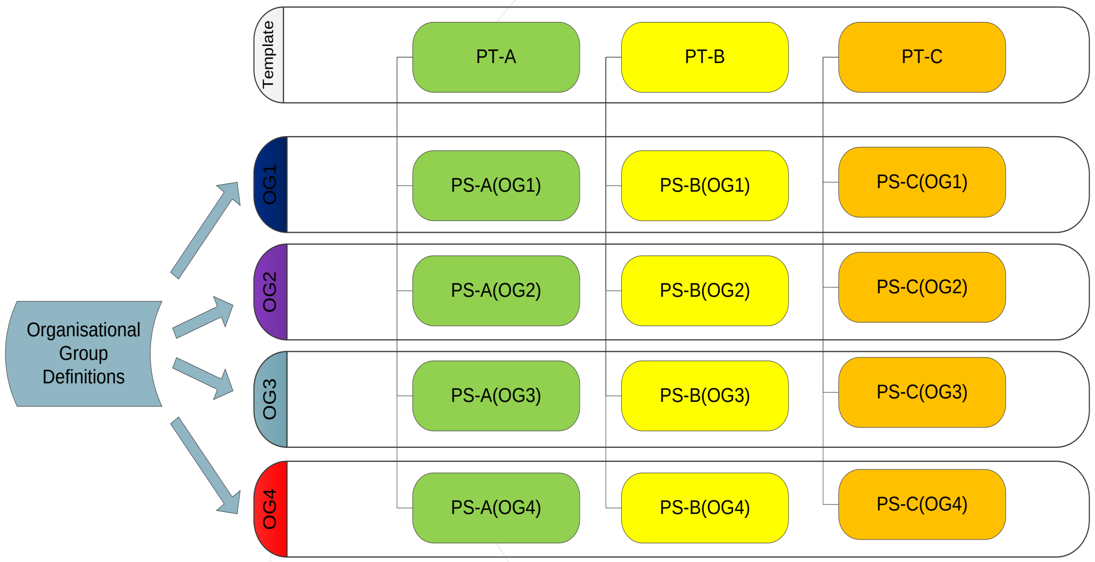
Evolution of Kerry’s SAP Access Request process

Evolution of Kerry’s SAP Access Request process

Definition of a global role design

Role derivation

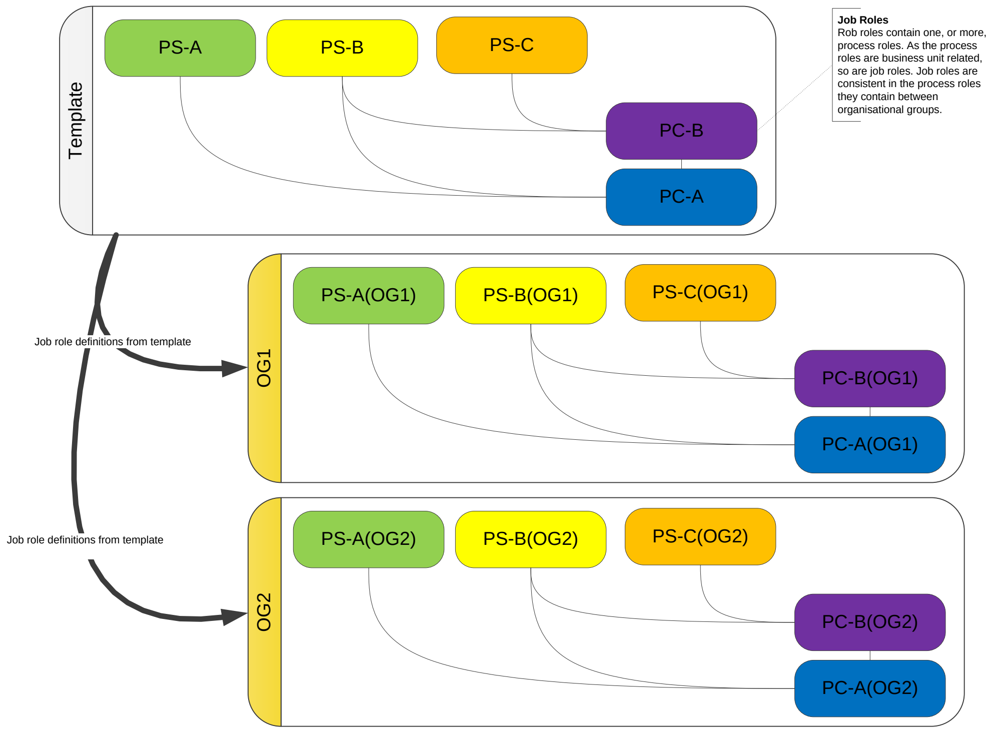
Template Roles
Non-organisational roles which define the transactions and non-organisational object level permissions



Organisational Groups
Organisational Groups define the organisational values which an individual process role will receive

Process Roles
Business Unit-defined variations based on the process template roles. Same transactions and non-organisational objects, but business-unit specific values

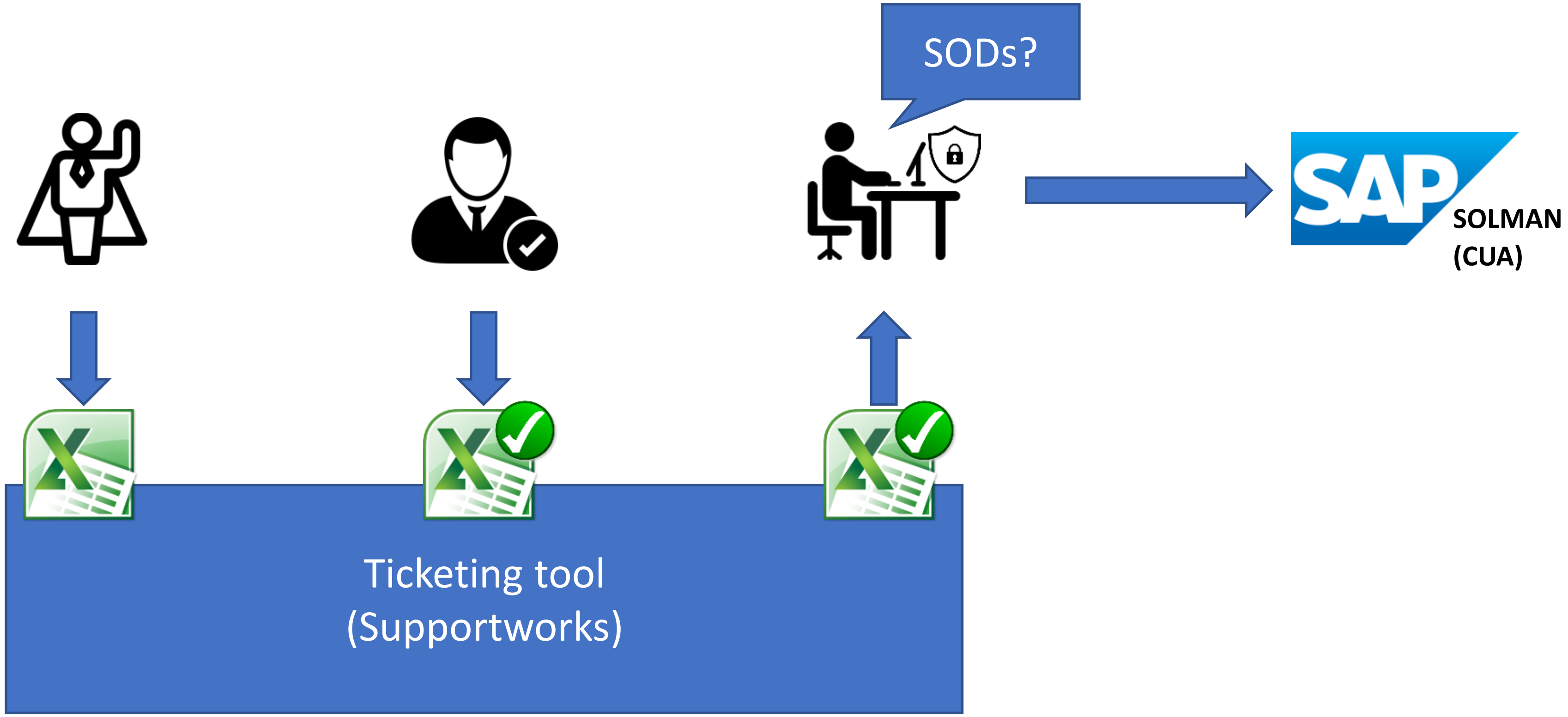
Use of composite roles



Job Roles
Rob roles contain one, or more, process roles. As the process roles are business unit related, so are job roles. Job roles are consistent in the process roles they contain between organisational groups.

Evolution of Kerry’s SAP Access Request process

Initial User Management Process



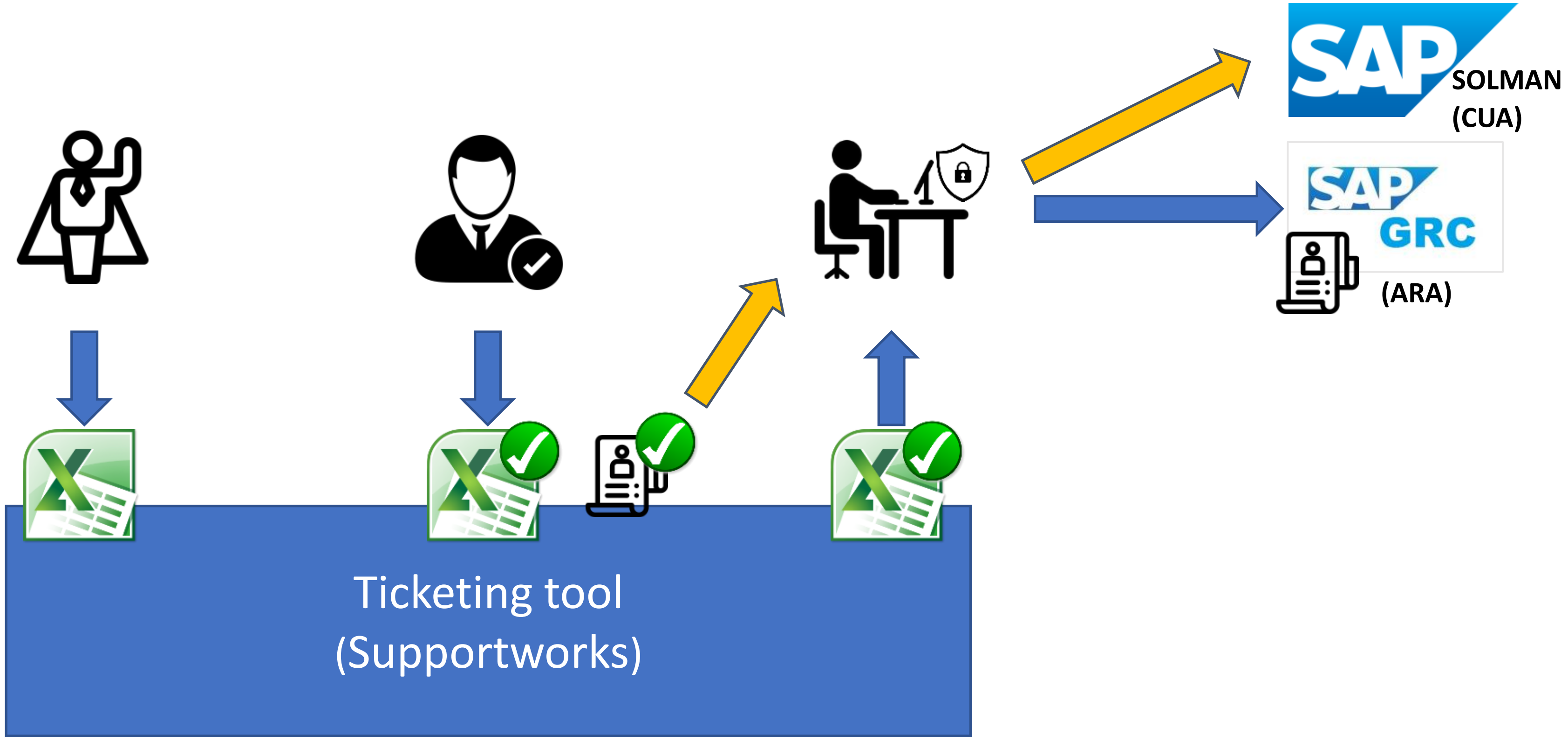
SODs?

SOLMAN (CUA)

Ticketing tool (Supportworks)

Evolution of Kerry’s SAP Access Request process

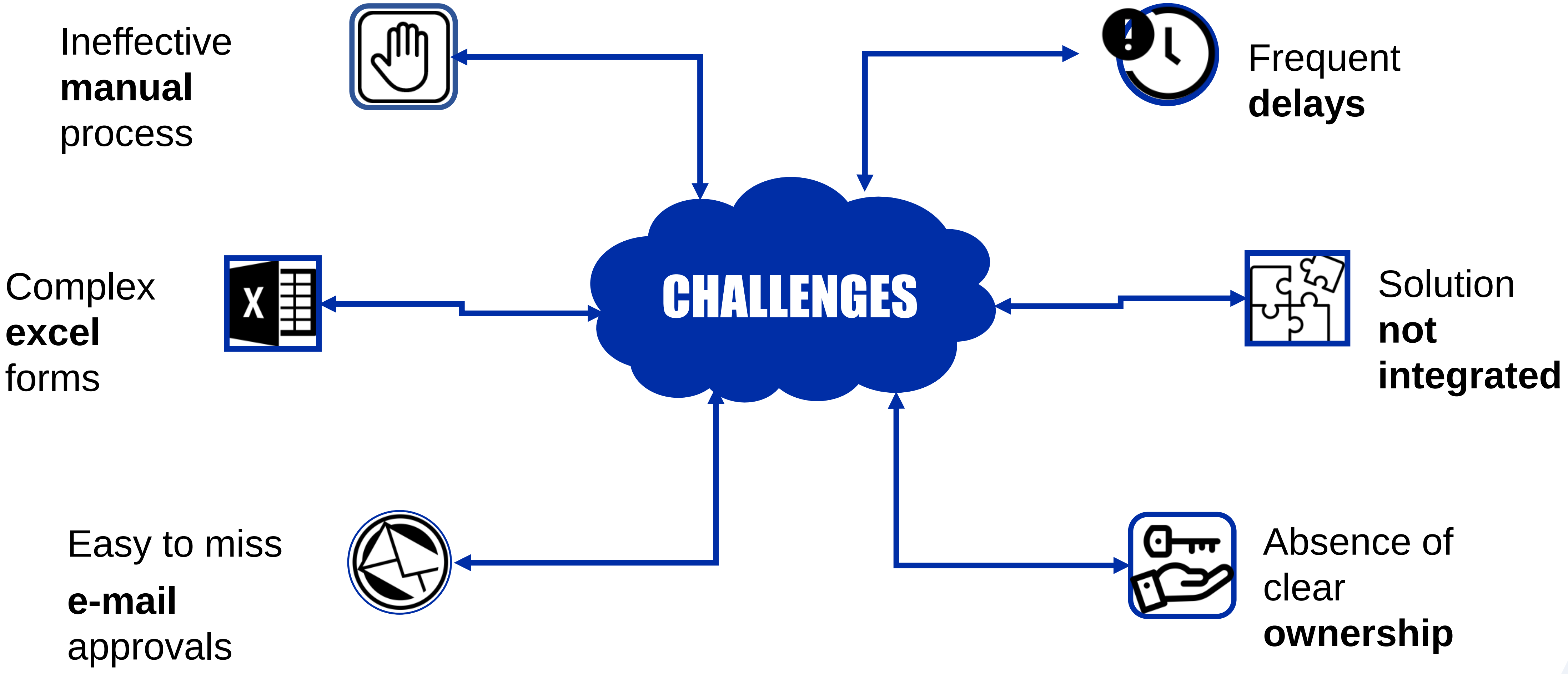
Initial User Management Process



Classified as General Business

Evolution of Kerry's SAP Access Request process

Initial User Management Process – Key Challenges



Ineffective **manual** process

Complex **excel** forms

Easy to miss **e-mail** approvals

CHALLENGES

Frequent **delays**

Solution **not integrated**

Absence of clear **ownership**

Evolution of Kerry’s SAP Access Request process

Transition to SAP GRC Access Control

ARM

BRM

UAR

EAM

Evolution of Kerry’s SAP Access Request process

Transition to SAP GRC Access Control

Access Request Management

- Automating the user creation, role assignment and role replacement
- Integration with Access Risk Analysis

Business Role Management

- Cross-system role definition
- Simplifying role ownership

User Access Review

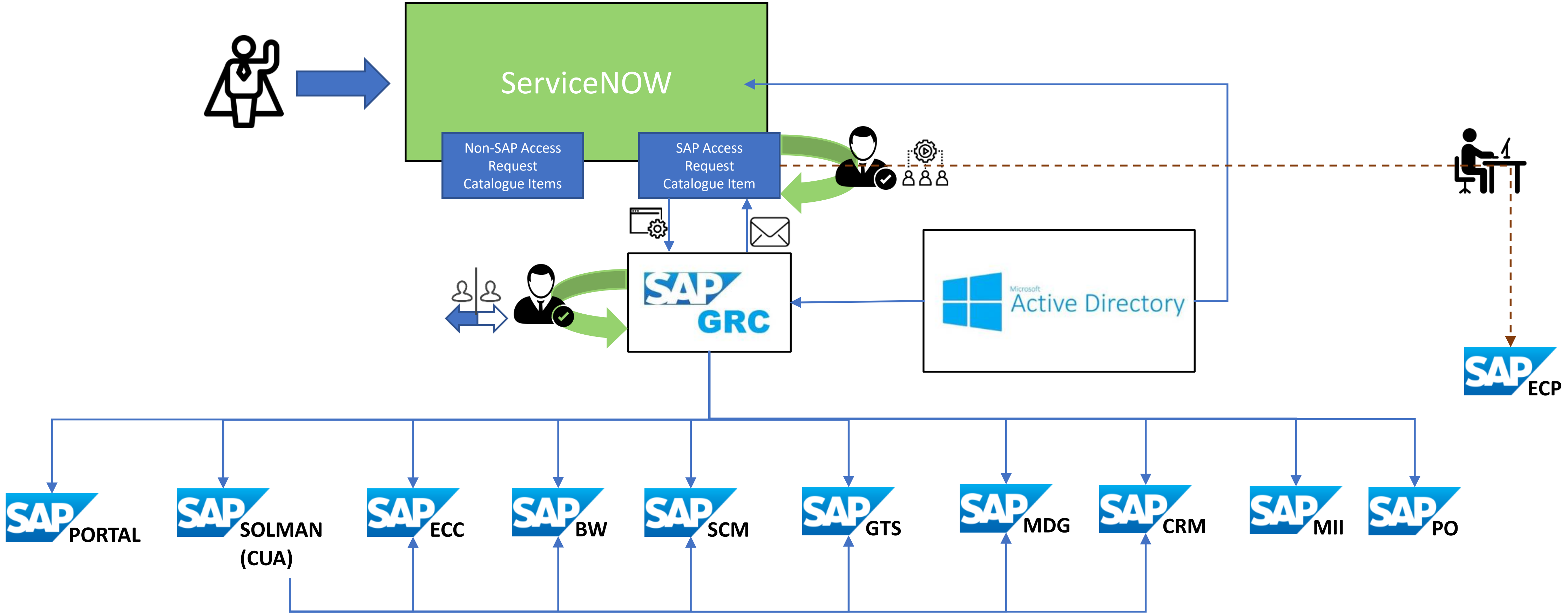
- Role owner approval using standard workflow
- Role owners defined at a functional area level

Emergency Access Management

- Centralized standard FF workflow
- Replacing manual assignment, removal and usage analysis of FF roles

Evolution of Kerry's SAP Access Request process

Consolidated Process with Service Now



Leavers Process IGA Integration

Leavers Process IGA Integration

- **Challenges of the leavers process for user ID termination**
  - Termination of user IDs in SAP is just one piece (an important one) of the offboarding process
  - Multiple not connected systems and applications without a fully centralized repository
  - Integration with HR systems and country specific processes
  - Differences in the way internal employees and external contractors are managed
  - Complex timing to revoke access promptly preventing unauthorized access and avoid security risks but also expedited access restoration when needed (incorrect termination, rehiring, contract extension after due date)

- **Our case: manual termination with a partial automation**
  - User IDs terminated in Active Directory would be sent in a file to a custom program in SAP Solution Manager to lock the accounts (only for production systems)
  - Service Desk team would manually terminate all leavers, internal employees and contractors, in all systems, including AD and SAP via SAP CUA, as a result of a request in Service Now created from SuccessFactors

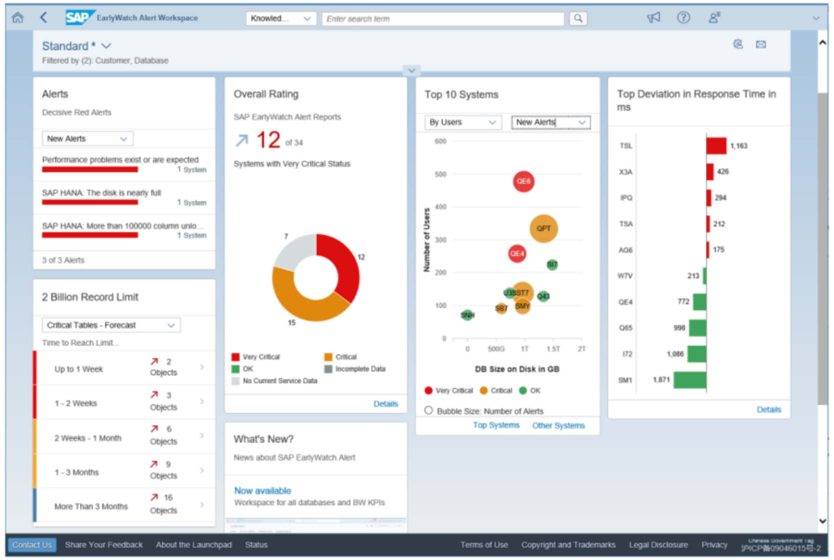
Leavers Process IGA Integration

- **IGA solutions help automate the entire identity lifecycle**
  - Defining a central repository for user management that all systems can rely on
  - Identifying the status of all users and making sure it remains aligned across the landscape
  - While we decided to keep the current user creation and access management processes through Service Now and SAP GRC for SAP systems, we can consider integrating it in our IGA tool in the future if we see a benefit on doing so
- **Automated SAP access termination**
  - All existing accounts for a leaver are now revoked at once, including all SAP systems by automatically raising a termination request in GRC for that user, applied to production and non-production
  - Mass termination is equally feasible when required (divestiture, end of project)
  - Reactivation of terminated users is feasible for 1 week only, a new access request is required after that
- **Audit and compliance**
  - IGA systems maintain a comprehensive audit trail of all active/inactive accounts, for internal and external users

Early Watch Alerts now in SAP for Me

Early Watch Alerts now in SAP for Me

- **SAP EarlyWatch Alert is an automatic service analyzing the essential administrative areas of an SAP system. Alerts indicate critical situations and give solutions to improve performance and stability.**
- The alerts and recommendations of this early warning service can be consumed in a cloud application called [SAP EarlyWatch Alert Workspace]() in [SAP for Me]()



Filtered by (2): Customer, Database

Alerts

Decisive Red Alerts

New Alerts

Performance problems exist or are expected — 1 System

SAP HANA: The disk is nearly full — 1 System

SAP HANA: More than 100000 column unlo... — 1 System

3 of 3 Alerts

2 Billion Record Limit

Critical Tables - Forecast

Time to Reach Limit...

Up to 1 Week	↗ 2 Objects
1 - 2 Weeks	↗ 3 Objects
2 Weeks - 1 Month	↗ 6 Objects
1 - 3 Months	↗ 9 Objects
More Than 3 Months	↗ 16 Objects

Overall Rating

SAP EarlyWatch Alert Reports

↗ 12 of 34

Systems with Very Critical Status

What's New?

News about SAP EarlyWatch Alert

Now available

Workspace for all databases and BW KPIs

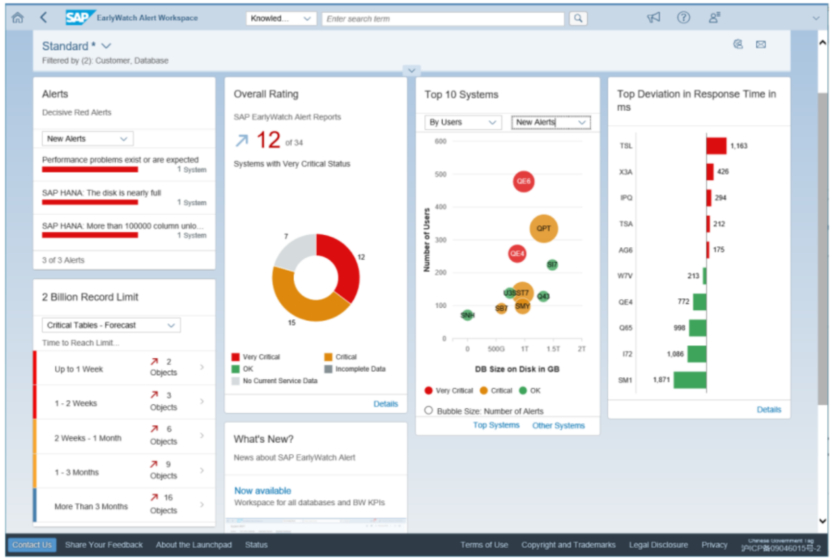
Top 10 Systems

Top Deviation in Response Time in ms

- You can see alerts for all systems or filter for specific ones you are more interested into
- SAP recommends to access the SAP EarlyWatch Alert Workspace once per week. You can also schedule a full report to be sent to you on an specific frequency.

Early Watch Alerts now in SAP for Me

- **SAP EarlyWatch Alert is an automatic service analyzing the essential administrative areas of an SAP system. Alerts indicate critical situations and give solutions to improve performance and stability.**
- The alerts and recommendations of this early warning service can be consumed in a cloud application called [SAP EarlyWatch Alert Workspace]() in [SAP for Me]()



Performance problems exist or are expected — 1 System

SAP HANA: The disk is nearly full — 1 System

SAP HANA: More than 100000 column unlo... — 1 System

Up to 1 Week	2 Objects	
1 - 2 Weeks	3 Objects	
2 Weeks - 1 Month	6 Objects	
1 - 3 Months	9 Objects	
More Than 3 Months	16 Objects	

Workspace for all databases and BW KPIs

- EWA reports are sorted by rating and date, displaying first those requiring immediate attention
- You can see alerts for all systems or filter for specific ones you are more interested into
- SAP recommends to access the SAP EarlyWatch Alert Workspace once per week. You can also schedule a full report to be sent to you on an specific frequency.

Self-Service Execution of Security Optimization Service via Solution Manager

Self-Service Execution of Security Optimization Service via Solution Manager

- **SAP Security Optimization Service**
  - SOS report provides a complete overview of the status of the security of your SAP landscape
  - Next step after you are satisfied with your EWA report results, going on more detail and exploring different configurations security relevant
  - Frequently used by external auditors to identify any risks as part of ITGC

- **How to execute the report**
  1. Make sure all prerequisites are checked
  2. Access to Solution Manager - SM_WORKCENTER and create a new session
  3. Execute the session using the Guided Self-Service for Security Optimization
  4. Select the criteria (system type and system ID) and credentials if the RFCs are not maintained with a trusted ID
  5. Maintain the questionnaire with an exception list for IDs authorized to have elevated access
  6. Schedule or run the data collection, or reuse an existing one
  7. Customize report output with the level of detail you want on the results
  8. Perform Analysis

Self-Service Execution of Security Optimization Service via Solution Manager

- **SAP Security Optimization Service results**
  - SOS initial results can be reviewed after the analysis is completed
  - Any exceptions that weren’t maintained in the exception list during the setup can be deleted prior to obtaining the final report
  - The report can be generated as a Word or a PDF document
  - It shows the number of potential security issues and specific recommendations on how to fix them
  - SOS report can be huge; a prioritization of risks analysis and resolution can be done based on the ratings included
  - Frequency of SOS execution should be defined based on results and improvement rates (yearly, twice per year, quarterly)

Exploring Cybersecurity tools for an SAP landscape

Exploring Cybersecurity tools for an SAP landscape

- **SAP Landscape Assessment**
  - Map the scope and complexity of your SAP landscape, including the number of systems, applications, and their interconnections
  - Identify the critical assets and data that need protection
  - Consider the regulatory and compliance requirements relevant to your industry
- **Requirement Gathering**
  - Determine your specific cybersecurity needs, such as data protection, access control, threat detection, and incident response, talking to the corresponding stakeholders (Internal and external audit, Internal Controls, SOC, SAP Technical Leads)
  - Clarify and remediate any knowledge gaps
  - Review and confirm your security policy and set objectives
- **Research Cybersecurity Tools**
  - Research and identify cybersecurity tools and solutions available in the market that match your specific security requirements

Exploring Cybersecurity tools for an SAP landscape

- **Vendor Assessment**
  - Arrange sessions and demos with each of the vendors, evaluating how each tool performs against your requirements using metrics and indicators
  - Request references from other organizations using their products
  - Determine the total cost of ownership for implementation and operations, also considering infrastructure requirements
  - Connect with a third-party consulting agency to support with the tool selection process
  - Proceed with a Proof of Concept when possible
- **Deployment Planning**
  - Develop a detailed deployment plan that outlines the installation and configuration process for the selected tools
  - Include the definition of an incident response plan that outlines how to react to any alerts, with an alert classification and RACI matrixes
  - Establish a clear process for investigating and remediating security breaches
  - Consider any necessary training sessions for teams involved

Exploring Cybersecurity tools for an SAP landscape

- **Fine Tuning**
  - Adjust the patterns and configuration of the tool to obtain the desired results, focusing on the risk classification and removing false positives when detected
  - Implement changes in SAP role design to remediate any detected risks that can be completely removed by restricting access
  - Report the progress to all stakeholders involved generating regular security reports

- **Remember that Cybersecurity is an ongoing process, and it requires a proactive approach to adapt to evolving threats and vulnerabilities in your SAP landscape. Regularly revisit and refine your cybersecurity strategy to ensure the highest level of protection, with planned reviews of the procedures.**

Wrap up

Wrap up

- SAP GRC Access Control streamlines the process of managing and validating user access as well as risk analysis and critical access monitoring
- Centralization of user management for SAP and non-SAP systems is key, especially for terminations
- SAP EWA and SOS are very useful to detect security risks with clear instructions to remediate them
- Defining a SAP Cybersecurity strategy requires a good understanding of your SAP landscape, the specific requirements of your organization and the available tools, and it is an ongoing process

Where to Find More Information

- SAPinsider - The largest and fastest growing SAP community worldwide
- Kerry Group - Taste & Nutrition Ingredients and Science
- Security Optimization Services Portfolio
- SOS on SolMan 7.2 (sap.com)
- SIEM and Cybersecurity | SAP Enterprise Threat Detection
- EarlyWatch Alert Service (EWA)

Key Points to Take Home

- Document and sign-off every decision
- Spread SAP Security awareness
- Keep the system tidy
- BAU process definition during projects
- Start defining your SAP cybersecurity strategy (if you haven’t yet!)

KERRY

Guillermo Casado

ICT SAP Security Lead at Kerry Group

Guillermo.Casado@kerry.com

https://www.linkedin.com/in/guillermo-casado-17059051/

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 750,000 global members.