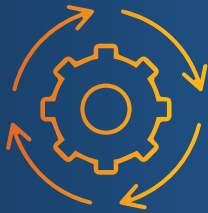




Maximising the Value of your GRC Investment - **The Importance of Defining a GRC Roadmap**

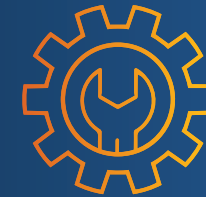
Struggling to extract value from your GRC investment (Under-utilisation)?



Implementation



Ownership



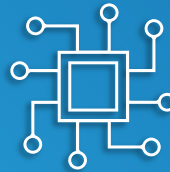
Change Control



Implementation



Vendor /
Implementation
Partner



IT



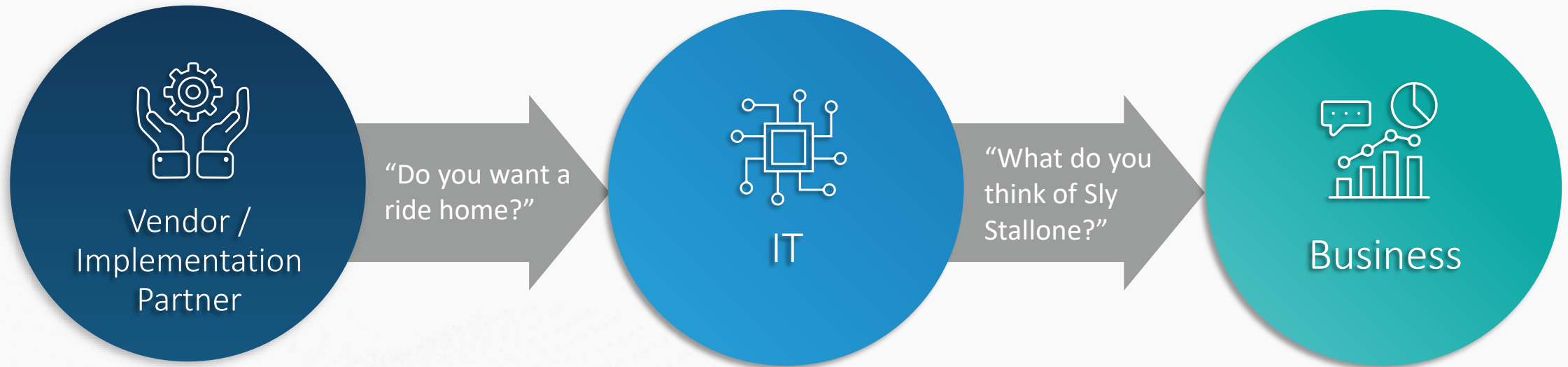
Business



Project Time Lines



Implementation



Project Time Lines



Implementation



Business



IT



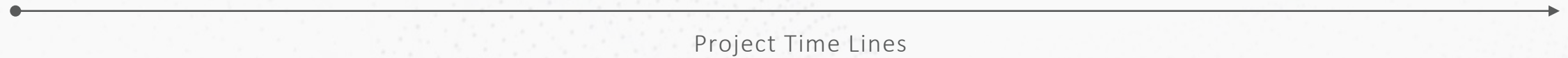
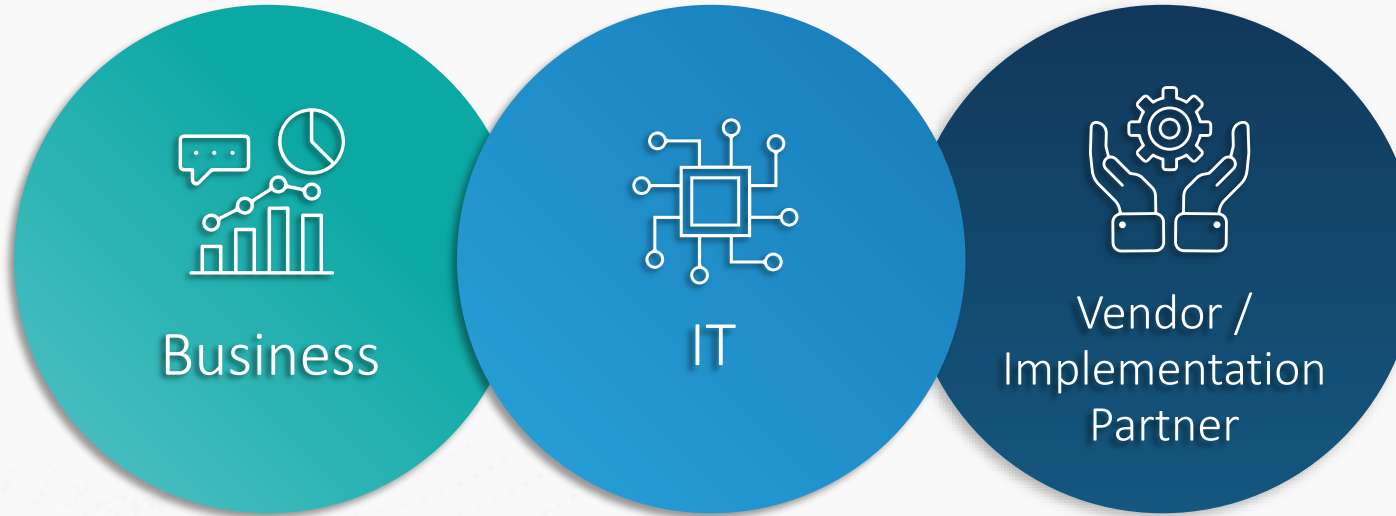
Vendor /
Implementation
Partner

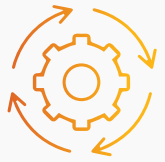
- ▶ Secure SAP solution
- ▶ Improve Efficiencies
- ▶ Comply with regulations
- ▶ Standardisation
- ▶ Business Ownership

Project Time Lines

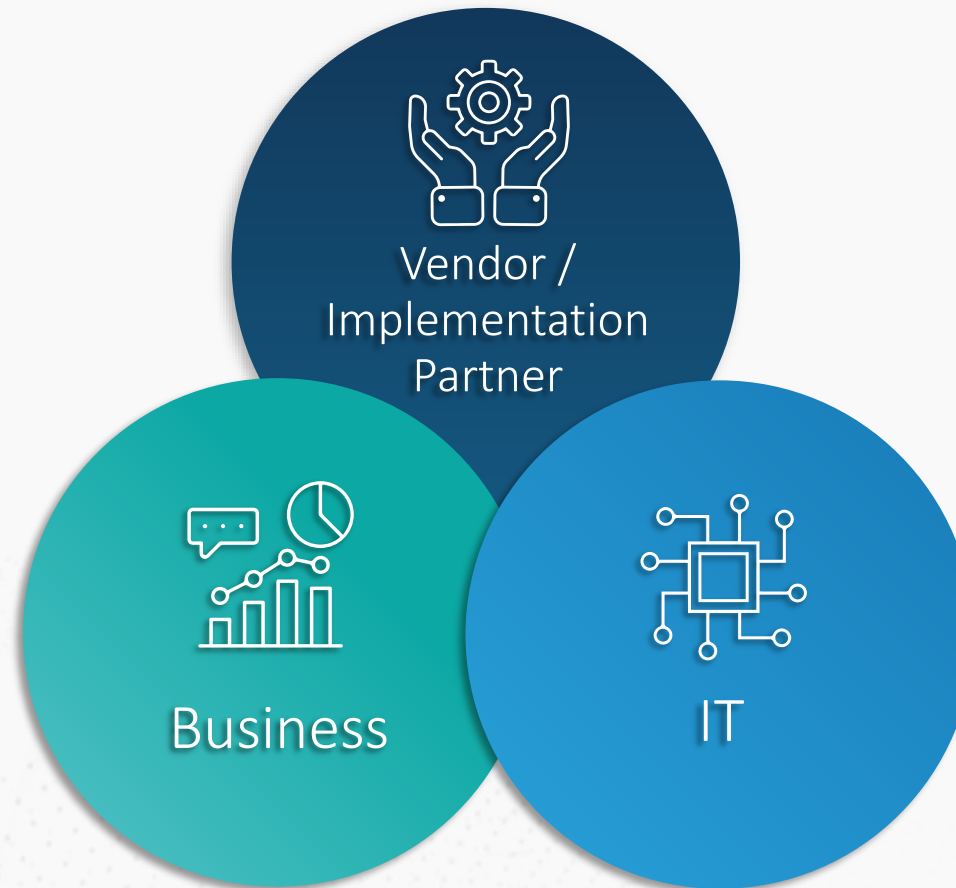


Implementation





Implementation



Project Time Lines

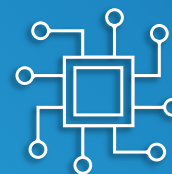


Ownership



Business

- ▶ GRC solutions are technical. Business users struggle to make decisions relating to functionality



IT

- ▶ Should not own access risks
- ▶ Cannot ask business to perform tasks



Ownership - Split?



Business

- ▶ Responsible for the on-going use of the solution
- ▶ Responsible for decisions (Access approvals, rule set etc)



IT

- ▶ Responsible for the delivery of the solution



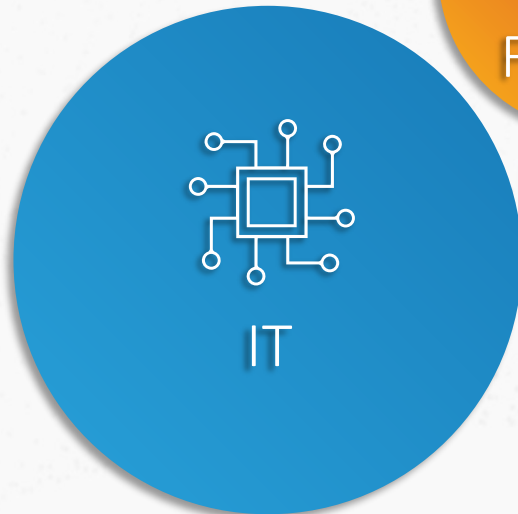
Ownership - Intermediary Department



- ▶ Responsible for the on-going use of the solution
- ▶ Responsible for decisions (Access approvals, rule set etc)

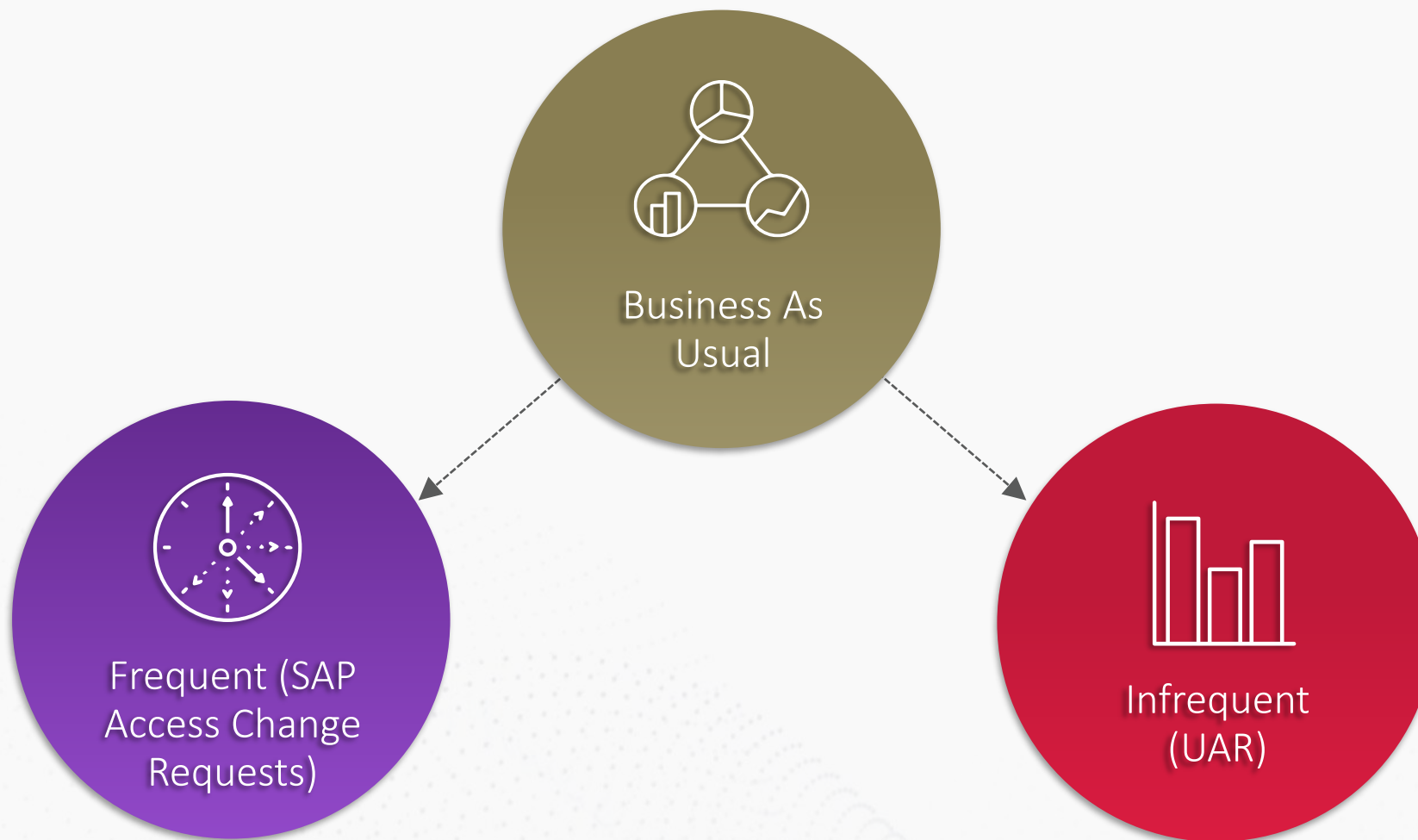


- ▶ Responsible for the delivery of the solution

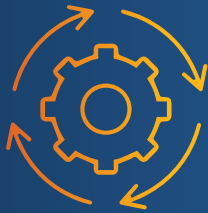




Change Control



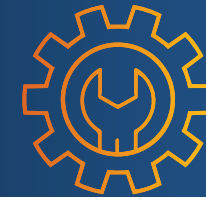
Struggling to extract value from your GRC investment (Under-utilisation)?



Implementation



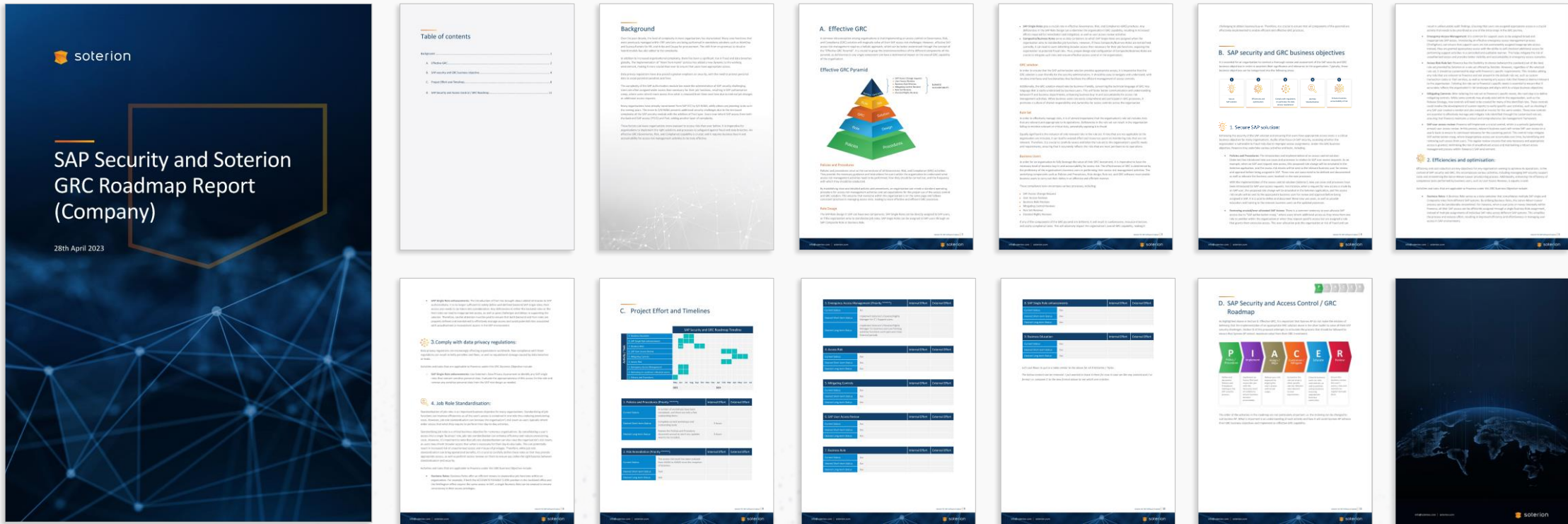
Ownership



Change Control



What is the Purpose of a GRC Roadmap?





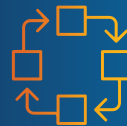
Typical Challenges with SAP Security and GRC



In-appropriate
Access



Rule Set
Customisation



Mitigating
Control Definition



Compliance Tasks



Business Role
Definition



Understanding your Organisation's GRC Business Objectives



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



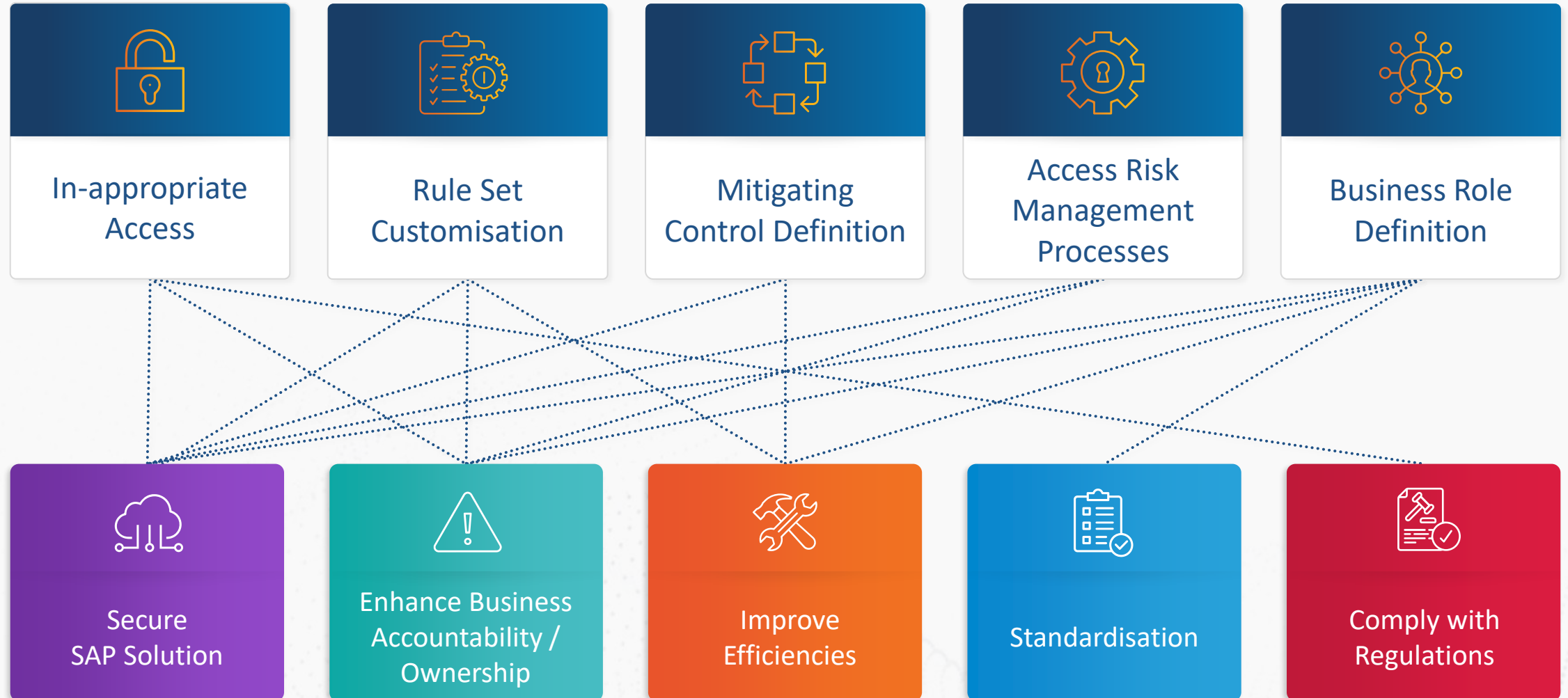
Standardisation



Comply with
Regulations



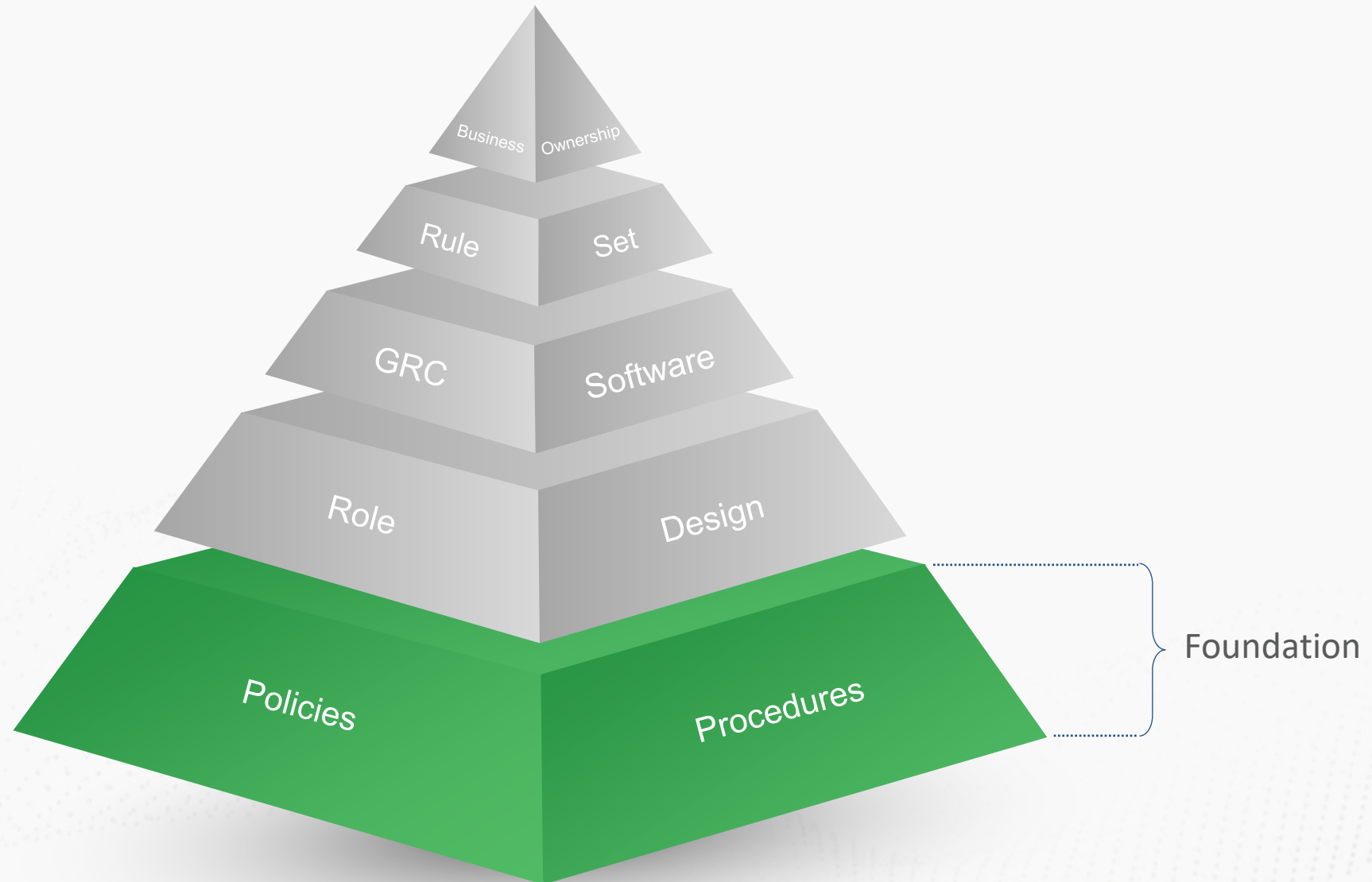
Typical Challenges with SAP Security and GRC



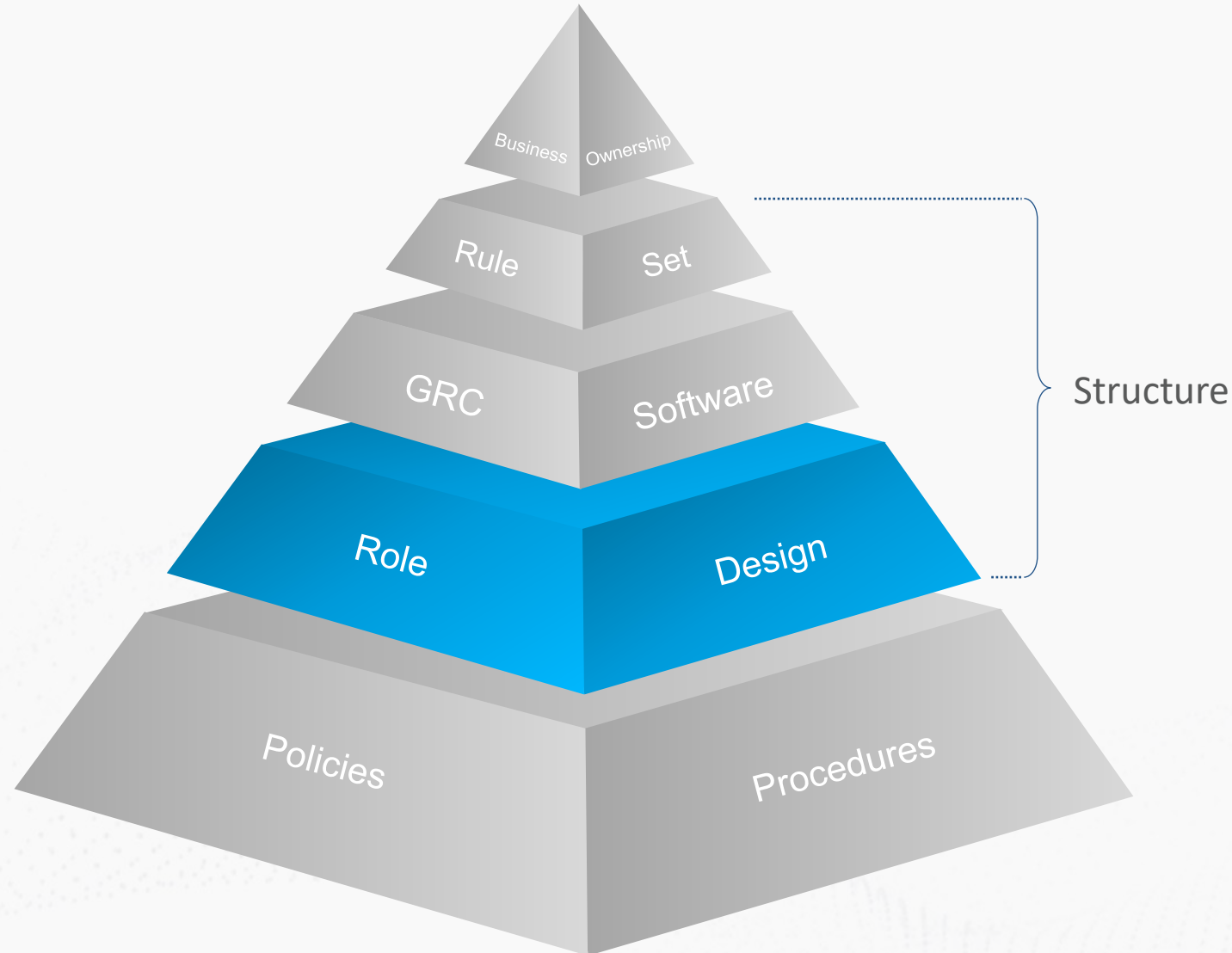
Holistic view to GRC → using the effective GRC Pyramid



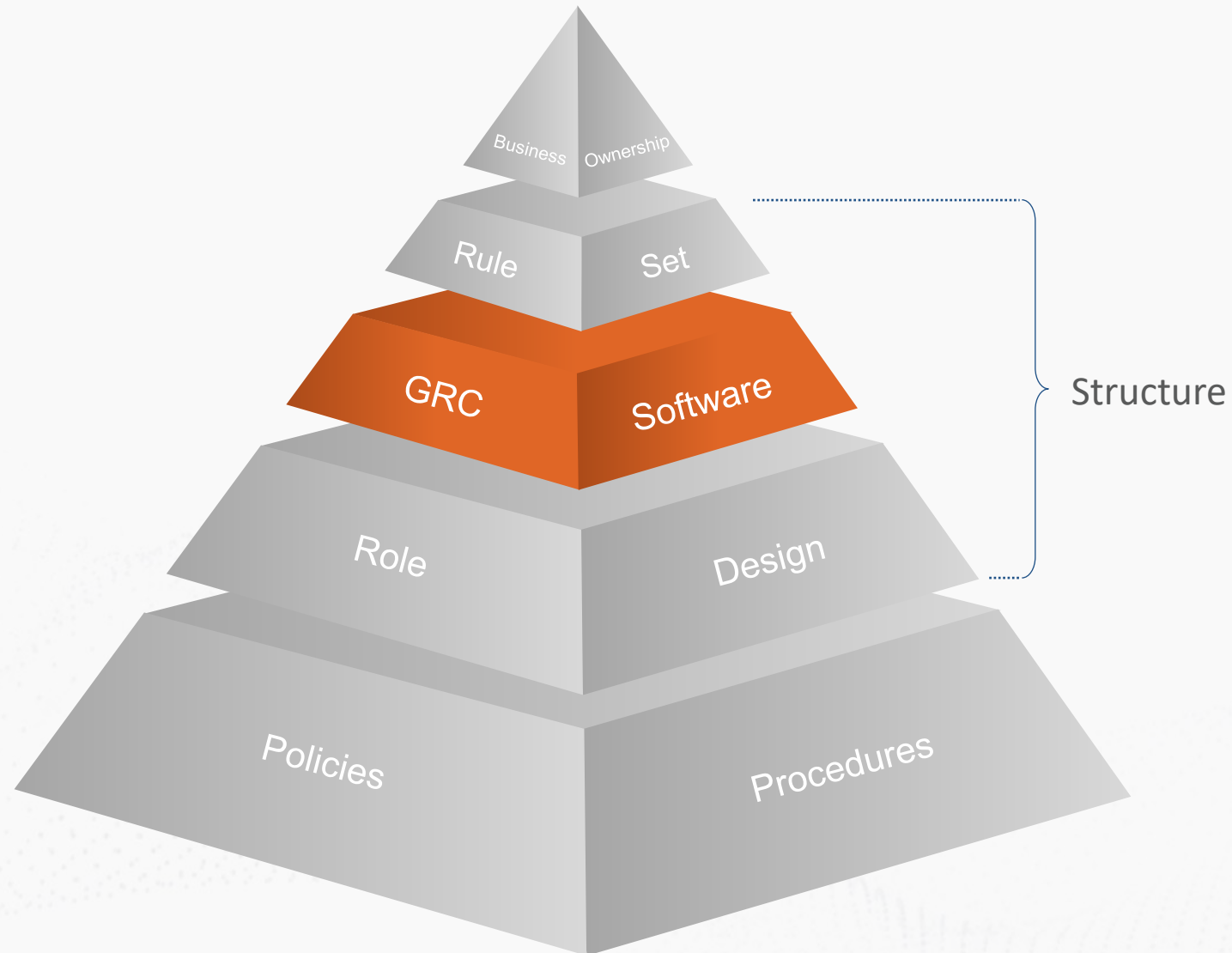
Holistic view to GRC → using the effective GRC Pyramid



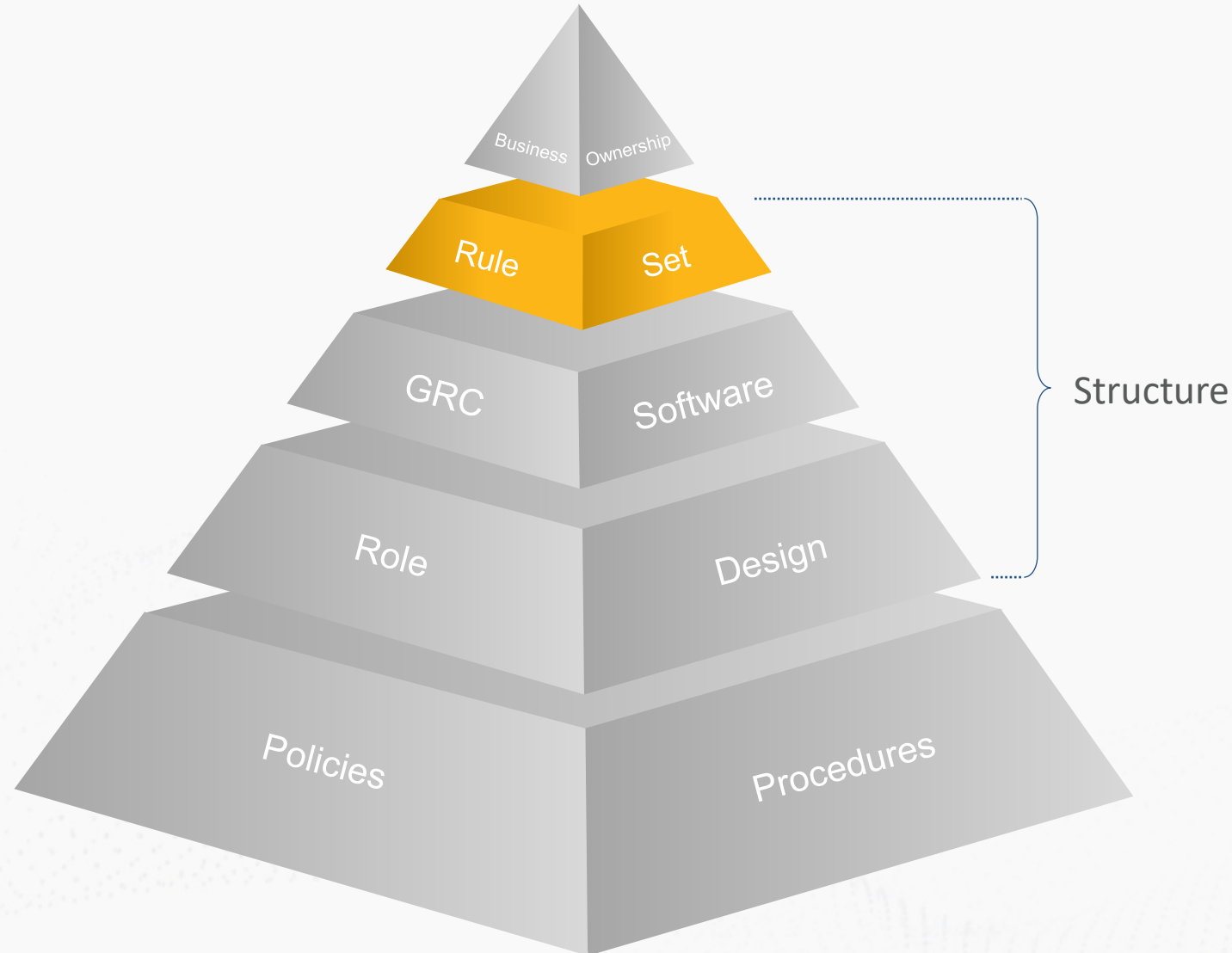
Holistic view to GRC → using the effective GRC Pyramid



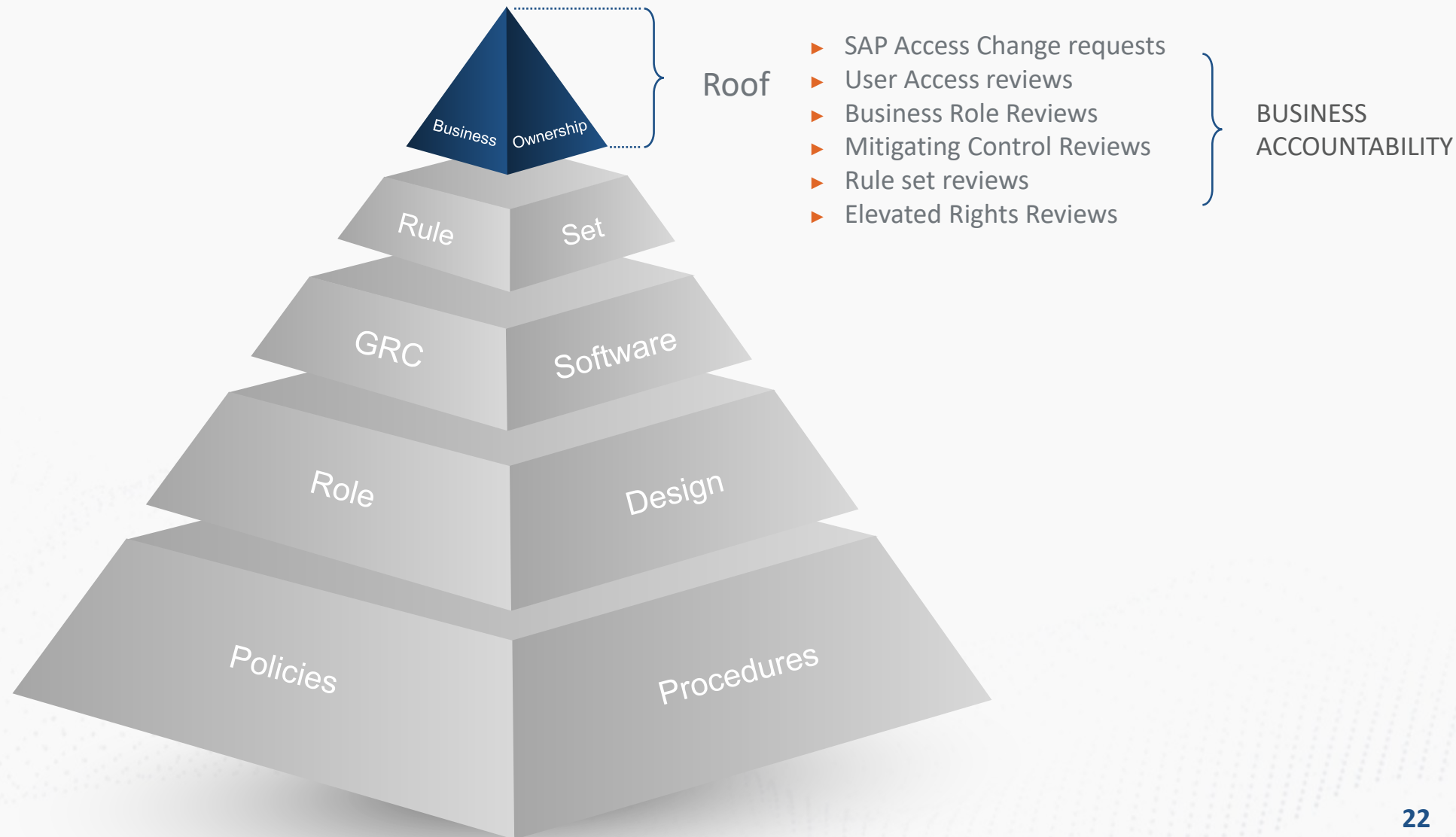
Holistic view to GRC → using the effective GRC Pyramid



Holistic view to GRC → using the effective GRC Pyramid



Holistic view to GRC → using the effective GRC Pyramid




Holistic view to GRC → using the effective GRC Pyramid








GRC Roadmap



SAP Security and Soterion GRC Roadmap Report (Company)


28th April 2023

1




Secure SAP solution

2




Efficiencies and optimisation

3




Comply with regulations
(in particular, the data privacy regulations)

4



Job Role Standardisation

5



Enhance business accountability of risk

Table of contents

Background

A. Effective GRC


B. SAP security and GRC business objectives


2. Efficiencies and optimisation

4. Job Role Standardisation

Effective GRC Pyramid

P I A C E R



 soterion

25



26



GRC Roadmap





2. **Research and analysis** – After identifying the problem, you need to research the problem to understand its context, scope, and causes.
3. **Developing a solution** – Once you have a clear understanding of the problem, you need to develop a solution. This involves brainstorming ideas, evaluating them, and selecting the best one.
4. **Implementation** – Once you have a solution, you need to implement it. This involves creating a plan, assigning tasks, and monitoring progress.
5. **Evaluation** – Once you have implemented the solution, you need to evaluate its effectiveness. This involves collecting data, analyzing it, and comparing it to the original problem.

Key Skills for Problem Solving:

- **Communication** – You need to be able to communicate effectively with others. This involves listening, speaking, and writing.
- **Teamwork** – You need to be able to work effectively with others. This involves sharing ideas, supporting others, and taking responsibility.
- **Problem Solving** – You need to be able to identify the problem, analyze it, and develop a solution.
- **Decision Making** – You need to be able to make decisions quickly and effectively. This involves weighing the pros and cons of different options.
- **Time Management** – You need to be able to manage your time effectively. This involves prioritizing tasks and meeting deadlines.

Resources for Problem Solving:

- **Books** – There are many books available on problem solving. Some popular ones include "The 7 Habits of Highly Effective People" by Stephen Covey, "The 48 Laws of Power" by Robert Greene, and "The Art of War" by Sun Tzu.
- **Online Courses** – There are many online courses available on problem solving. Some popular ones include "The Science of Problem Solving" by Coursera, "The Art of Problem Solving" by Khan Academy, and "The Psychology of Problem Solving" by edX.
- **Workshops** – There are many workshops available on problem solving. Some popular ones include "The Design Thinking Process" by IDEO, "The Lean Startup Method" by Steve Blank, and "The Agile Mindset" by Spotify.

Conclusion:

Problem solving is a skill that is essential for success in any field. By following the steps outlined above, you can develop your problem-solving skills and become a more effective problem solver.



GRC Roadmap



SAP Security and Soterion GRC Roadmap Report (Company)

28th April 2023



2. Efficiencies and optimisation:

Table of contents

- 1. Introduction
- 2. SAP security and GRC business objectives
- 3. Project Objectives
- 4. Job Role Standardisation

Background

Over the past decade, the level of complexity in business operations has increased. This has led to a growing need for more robust security and compliance measures. SAP, as a leading provider of enterprise resource planning (ERP) software, has a critical role to play in ensuring that businesses can meet these challenges. This report outlines the key findings of a recent study conducted by Soterion, a leading provider of SAP security and compliance solutions. The study focused on the challenges faced by businesses in implementing SAP security and compliance measures, and the role of Soterion in helping them overcome these challenges. The report also provides a detailed overview of the SAP security and compliance landscape, and the key findings of the study. The report is structured as follows:

- 1. Introduction
- 2. SAP security and GRC business objectives
- 3. Project Objectives
- 4. Job Role Standardisation

A. Effective GRC

Effective GRC Pyramid



The Effective GRC Pyramid is a framework for implementing SAP security and compliance measures. It is structured into four levels, each representing a different level of complexity and risk. The levels are: Foundation, Core, Advanced, and Expert. The Foundation level is the base of the pyramid, and it represents the most basic level of security and compliance. The Core level is the second level, and it represents a more advanced level of security and compliance. The Advanced level is the third level, and it represents a more complex level of security and compliance. The Expert level is the top of the pyramid, and it represents the most advanced level of security and compliance. The pyramid is designed to help businesses understand the scope and complexity of their SAP security and compliance requirements, and to provide a clear path for implementing these measures. The pyramid is structured as follows:

- 1. Foundation
- 2. Core
- 3. Advanced
- 4. Expert

B. SAP security and GRC business objectives

1. Secure SAP solution:



The SAP security and GRC business objectives are the key goals that businesses should aim to achieve when implementing SAP security and compliance measures. These objectives are: 1. Secure SAP solution, 2. Efficient and optimisation, 3. Risk management, and 4. Compliance. The objectives are designed to help businesses understand the scope and complexity of their SAP security and compliance requirements, and to provide a clear path for implementing these measures. The objectives are structured as follows:

- 1. Secure SAP solution
- 2. Efficient and optimisation
- 3. Risk management
- 4. Compliance

4. Job Role Standardisation

Job Role Standardisation



Job Role Standardisation is a key objective of the SAP security and GRC business objectives. It involves defining the roles and responsibilities of the SAP security and compliance team, and ensuring that these roles are clearly defined and consistent across the organization. The job roles are: SAP Security Administrator, SAP Security Analyst, SAP Security Auditor, and SAP Security Manager. The job roles are designed to help businesses understand the scope and complexity of their SAP security and compliance requirements, and to provide a clear path for implementing these measures. The job roles are structured as follows:

- 1. SAP Security Administrator
- 2. SAP Security Analyst
- 3. SAP Security Auditor
- 4. SAP Security Manager

5. Risk Management

Risk Management



Risk Management is a key objective of the SAP security and GRC business objectives. It involves identifying the risks associated with SAP security and compliance, and ensuring that these risks are managed effectively. The risk levels are: Low, Medium, High, and Critical. The risk levels are designed to help businesses understand the scope and complexity of their SAP security and compliance requirements, and to provide a clear path for implementing these measures. The risk levels are structured as follows:

- 1. Low
- 2. Medium
- 3. High
- 4. Critical

6. Compliance

Compliance



Compliance is a key objective of the SAP security and GRC business objectives. It involves ensuring that businesses are compliant with the relevant SAP security and compliance regulations. The compliance levels are: Basic, Intermediate, Advanced, and Expert. The compliance levels are designed to help businesses understand the scope and complexity of their SAP security and compliance requirements, and to provide a clear path for implementing these measures. The compliance levels are structured as follows:

- 1. Basic
- 2. Intermediate
- 3. Advanced
- 4. Expert



30



3. Comply with data privacy regulations:



GRC Roadmap

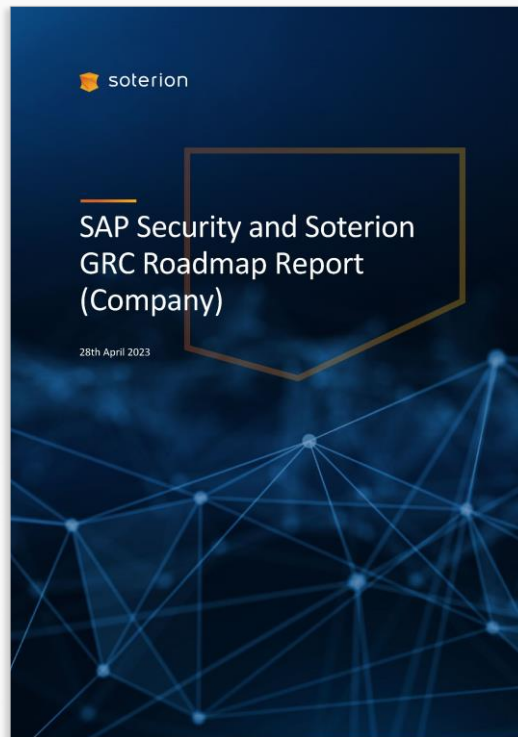


Table of contents

1. Background	1
2. Effective GRC	2
3. SAP security and GRC business objectives	3
4. Project Effect and Timelines	4
5. SAP Security and Access Control / GRC Roadmap	5

Background

Over the past decade, the level of complexity in GRC has increased significantly. This complexity has led to a growing demand for GRC solutions that can provide a comprehensive view of an organization's GRC posture. SAP Security and GRC business objectives are designed to address this demand by providing a comprehensive view of an organization's GRC posture, enabling organizations to identify and address GRC risks effectively.



B. SAP security and GRC business objectives

SAP Security and GRC business objectives are designed to address the growing demand for GRC solutions that can provide a comprehensive view of an organization's GRC posture. The objectives are designed to enable organizations to identify and address GRC risks effectively, ensuring that their GRC posture is robust and resilient.



2. Influence and extension

Influence and extension are key factors in the success of a GRC program. Influence refers to the ability of a GRC program to impact the organization's overall risk posture, while extension refers to the ability of a GRC program to extend its reach across the organization's entire GRC posture.

3. Comply with data privacy regulations

Compliance with data privacy regulations is a critical requirement for organizations. SAP Security and GRC business objectives are designed to ensure that organizations can comply with these regulations effectively, reducing the risk of non-compliance and associated penalties.



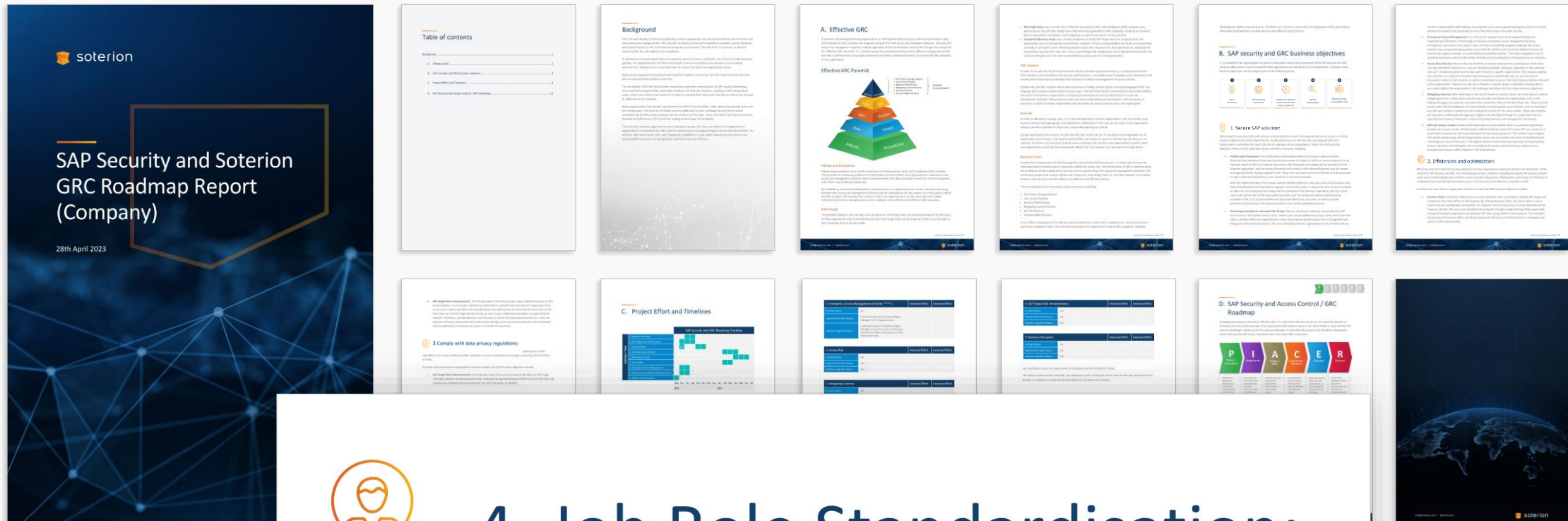
D. SAP Security and Access Control / GRC Roadmap

Category	Item	Start Date	End Date	Status
SAP Security	SAP Security Audit	2023-01-01	2023-03-31	Completed
	SAP Security Assessment	2023-04-01	2023-06-30	In Progress
	SAP Security Implementation	2023-07-01	2023-09-30	Planned
	SAP Security Monitoring	2023-10-01	2023-12-31	Planned
SAP GRC	SAP GRC Audit	2023-01-01	2023-03-31	Completed
	SAP GRC Assessment	2023-04-01	2023-06-30	In Progress
	SAP GRC Implementation	2023-07-01	2023-09-30	Planned
	SAP GRC Monitoring	2023-10-01	2023-12-31	Planned
SAP Access Control	SAP Access Control Audit	2023-01-01	2023-03-31	Completed
	SAP Access Control Assessment	2023-04-01	2023-06-30	In Progress
	SAP Access Control Implementation	2023-07-01	2023-09-30	Planned
	SAP Access Control Monitoring	2023-10-01	2023-12-31	Planned
SAP User Management	SAP User Management Audit	2023-01-01	2023-03-31	Completed
	SAP User Management Assessment	2023-04-01	2023-06-30	In Progress
	SAP User Management Implementation	2023-07-01	2023-09-30	Planned
	SAP User Management Monitoring	2023-10-01	2023-12-31	Planned





GRC Roadmap



4. Job Role Standardisation:

[illegible]



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

- a. Policies and Procedures
- b. Removing un-used / over-allocated access
- c. Role redesign
- d. Emergency Access Management process
- e. Access Risk Rule Set
- f. Mitigating Controls
- g. User Access Reviews



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



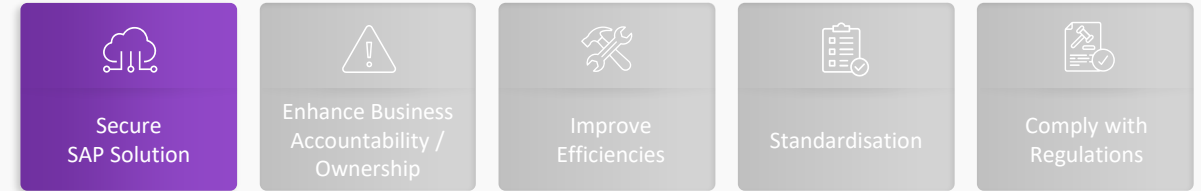
Comply with
Regulations

a. Policies and Procedures

- b. Removing un-used / over-allocated access
- c. Role redesign
- d. Emergency Access Management process
- e. Access Risk Rule Set
- f. Mitigating Controls
- g. User Access Reviews

- ▶ How many days of inactivity constitutes a dormant SAP user?
- ▶ How are terminated users handled in SAP?
- ▶ If SAP access requests result in risk, what are the conditions for this access to be approved / assigned?
- ▶ How many user access reviews need to be conducted on an annual basis?
- ▶ Will reviews be split (User – Role review vs Business Role content review)?
- ▶ Who will approve SAP access (line managers, risk owners, role owners)?

GRC Roadmap



a. Policies and Procedures

b. Removing un-used / over-allocated access

c. Role redesign

d. Emergency Access Management process

e. Access Risk Rule Set

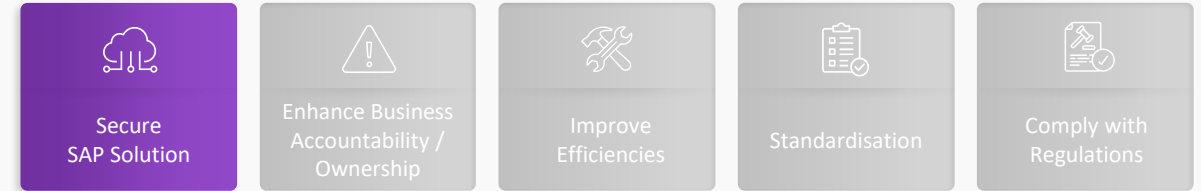
f. Mitigating Controls

g. User Access Reviews

Use Case 1 -> New SAP User



GRC Roadmap



a. Policies and Procedures

b. Removing un-used / over-allocated access

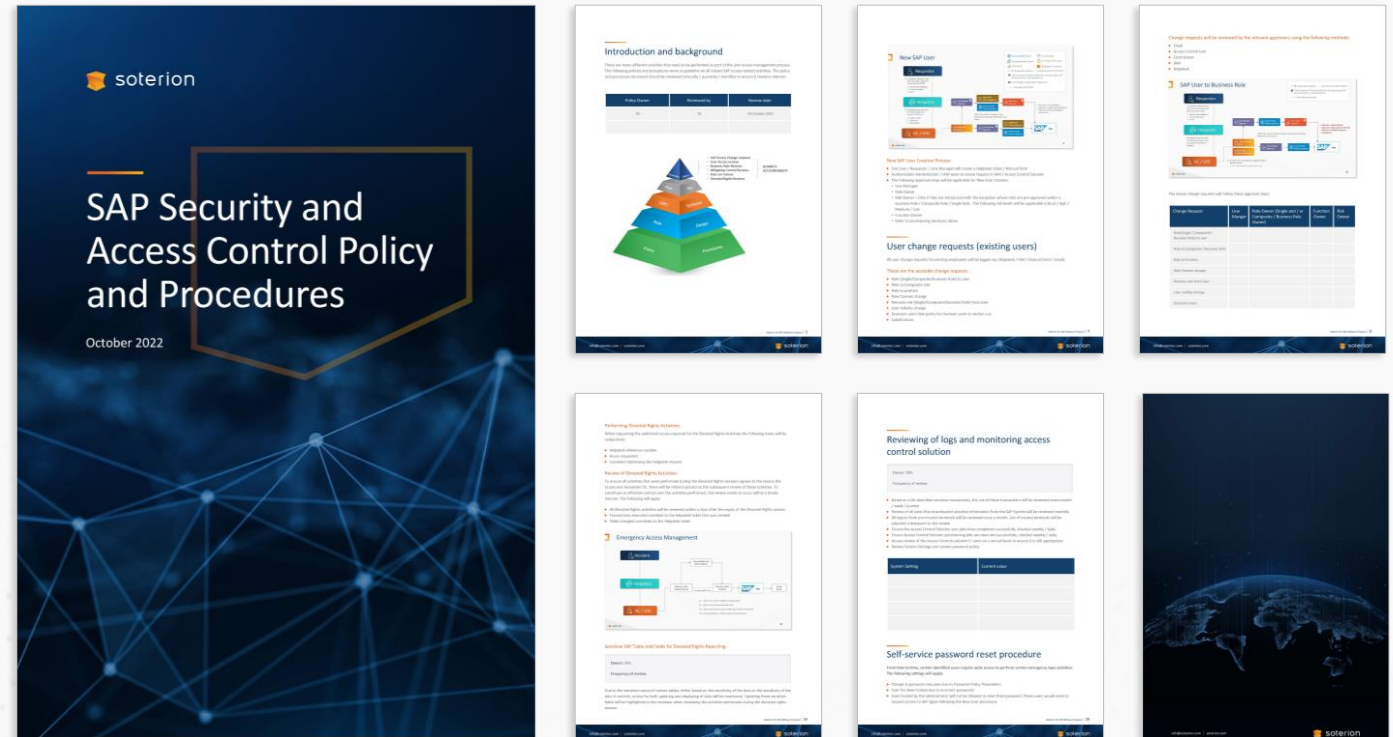
c. Role redesign

d. Emergency Access Management process

e. Access Risk Rule Set

f. Mitigating Controls

g. User Access Reviews





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

a. Policies and Procedures

b. Removing un-used / over-allocated access

c. Role redesign

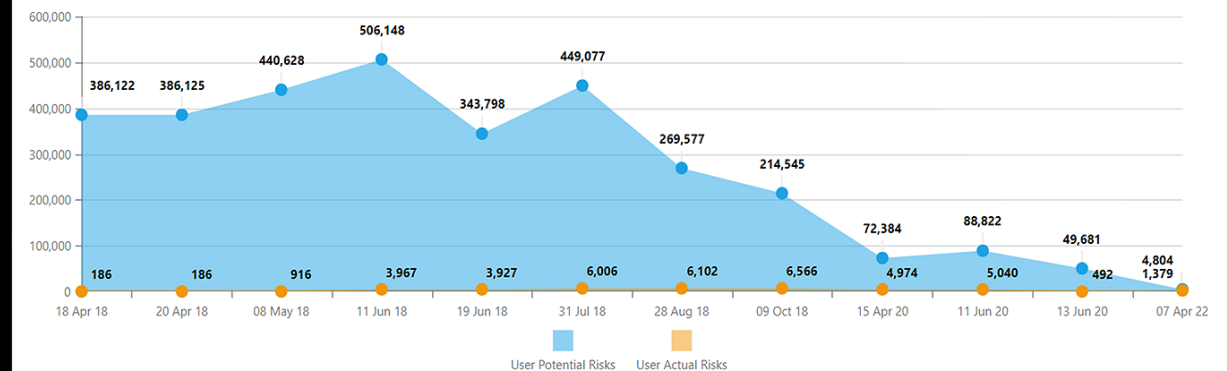
d. Emergency Access Management process

e. Access Risk Rule Set

f. Mitigating Controls

g. User Access Reviews

User SOD Risk Trends





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



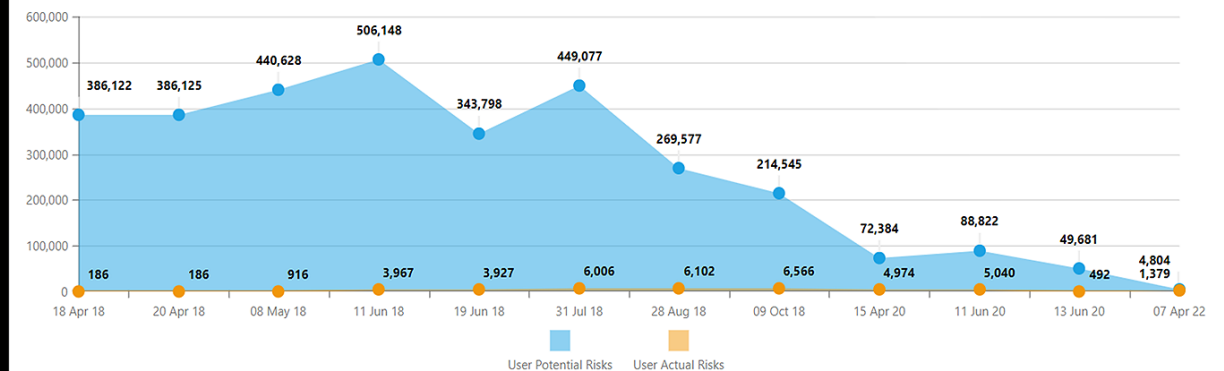
Standardisation



Comply with
Regulations

- a. Policies and Procedures
- b. Removing un-used / over-allocated access
- c. Role redesign**
- d. Emergency Access Management process
- e. Access Risk Rule Set
- f. Mitigating Controls
- g. User Access Reviews

User SOD Risk Trends





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

- a. Policies and Procedures
- b. Removing un-used / over-allocated access
- c. Role redesign

d. Emergency Access Management process

- e. Access Risk Rule Set
- f. Mitigating Controls
- g. User Access Reviews



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies

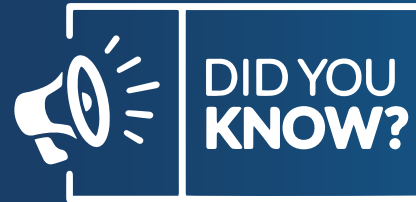


Standardisation



Comply with
Regulations

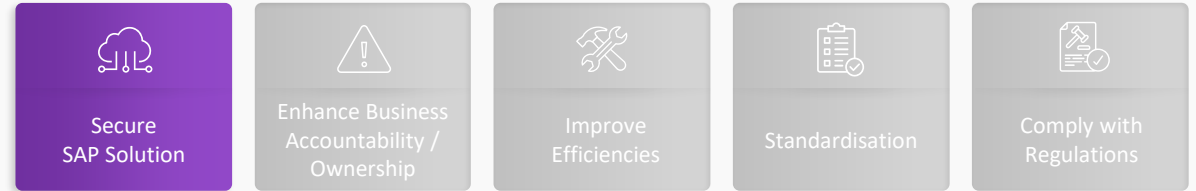
- a. Policies and Procedures
- b. Removing un-used / over-allocated access
- c. Role redesign
- d. Emergency Access Management process
- e. Access Risk Rule Set**
- f. Mitigating Controls
- g. User Access Reviews



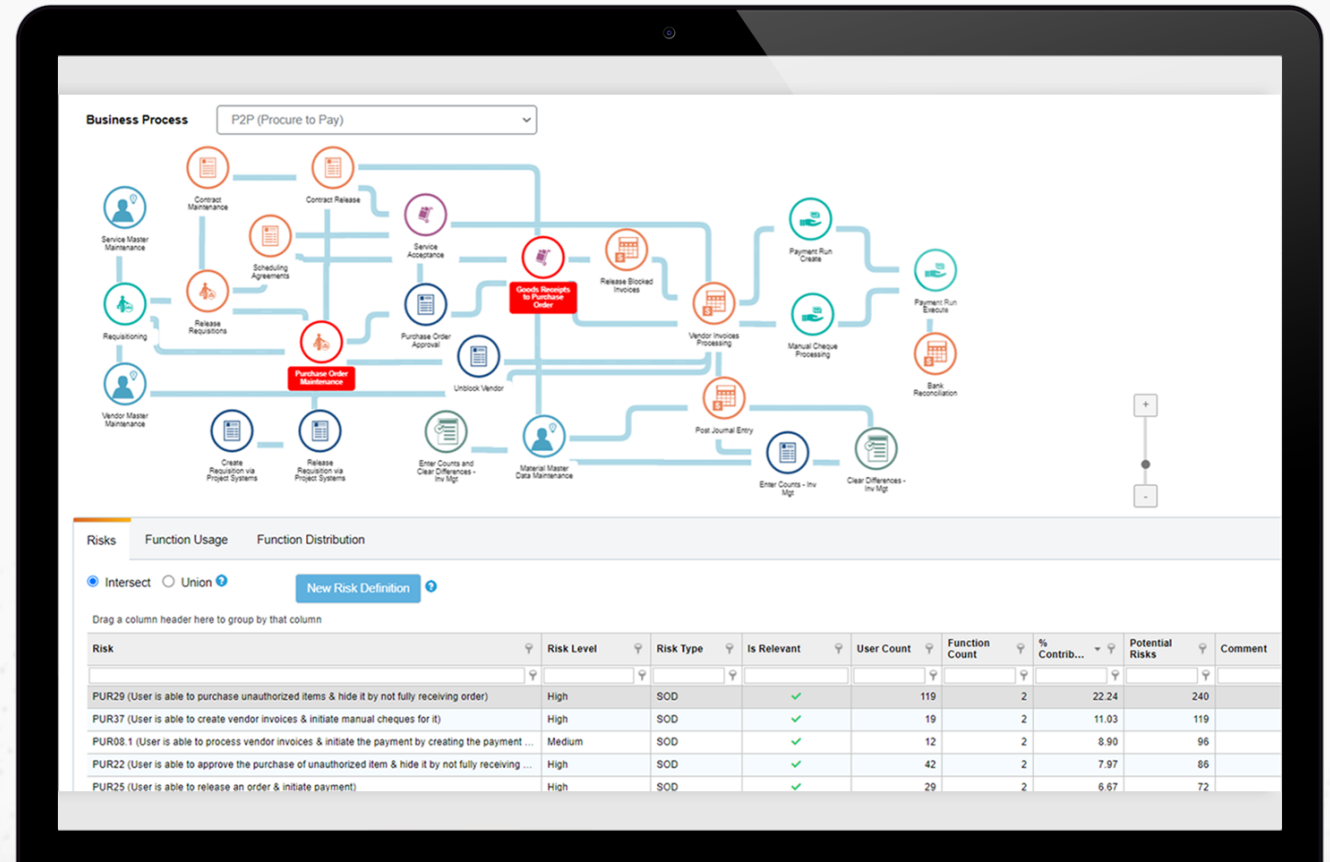
Less than 50% of
companies have not
customised the rule set

- ▶ Do organisations believe the out-the-box rule set is adequate?
- ▶ Do organisation's not place enough value on GRC activities to justify a rule set project?
- ▶ Do organisation's not know how to perform such an activity?

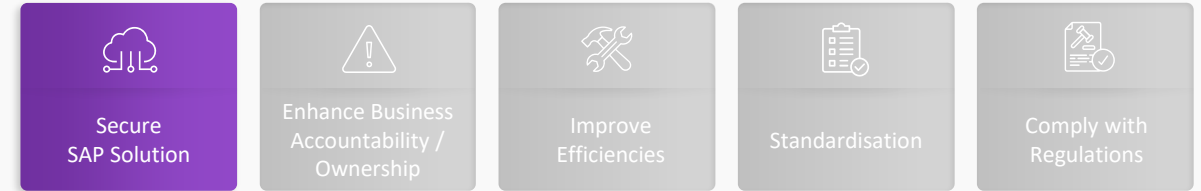
GRC Roadmap



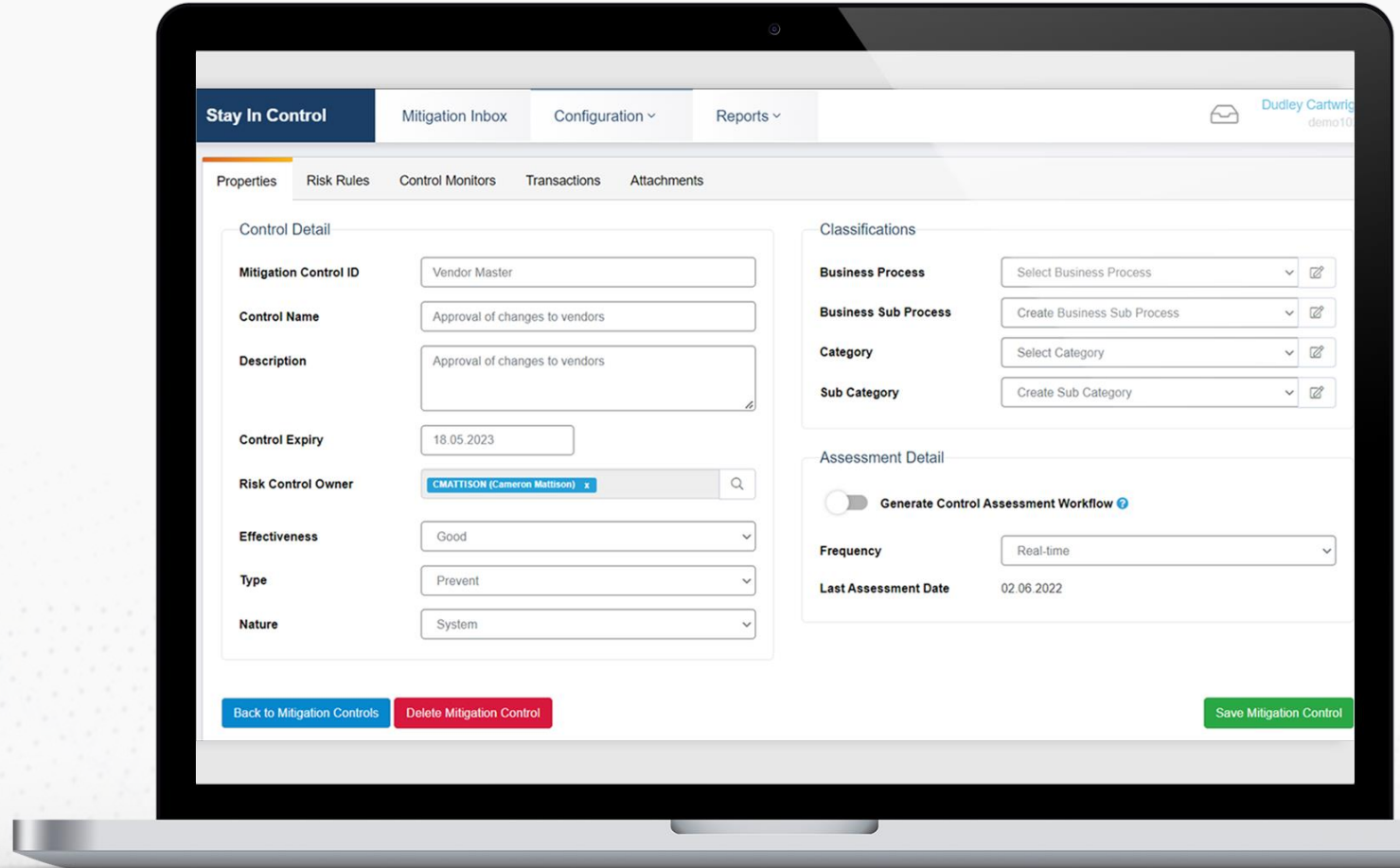
- Policies and Procedures
- Removing un-used / over-allocated access
- Role redesign
- Emergency Access Management process
- Access Risk Rule Set**
- Mitigating Controls
- User Access Reviews



GRC Roadmap

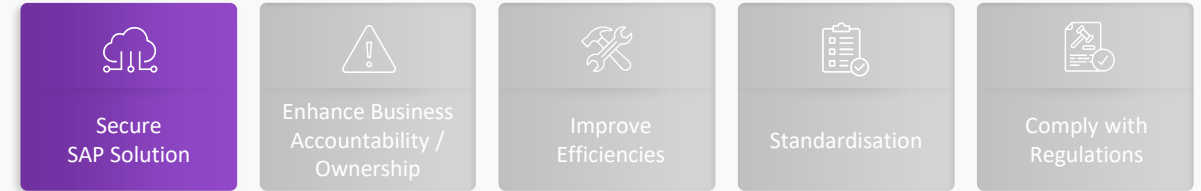


- a. Policies and Procedures
- b. Removing un-used / over-allocated access
- c. Role redesign
- d. Emergency Access Management process
- e. Access Risk Rule Set
- f. Mitigating Controls**
- g. User Access Reviews

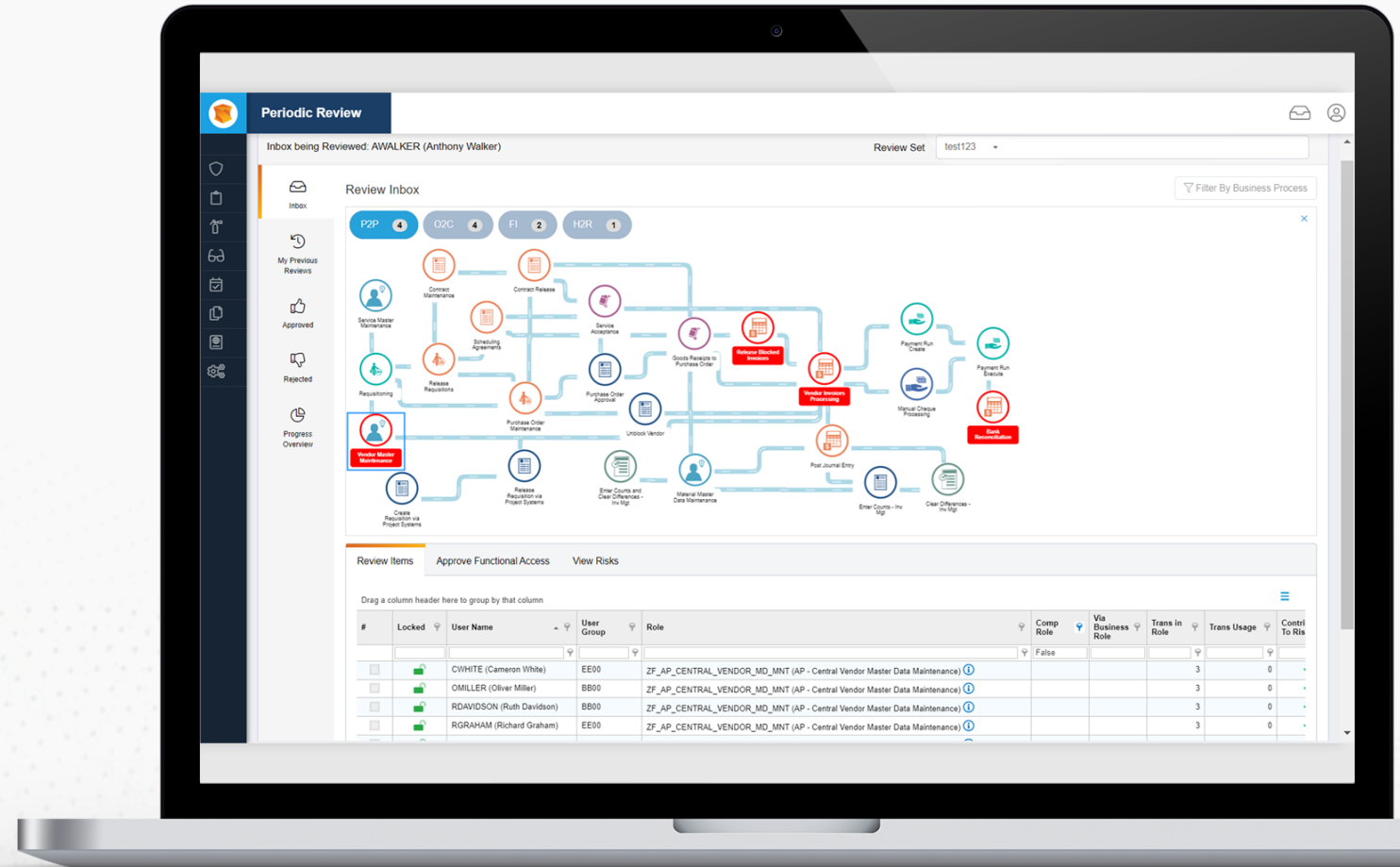


The screenshot displays the 'Mitigation Control' configuration page in the Soterion GRC system. The interface includes a top navigation bar with tabs for 'Stay In Control', 'Mitigation Inbox', 'Configuration', and 'Reports'. Below this, a sub-navigation bar shows 'Properties', 'Risk Rules', 'Control Monitors', 'Transactions', and 'Attachments'. The main content area is divided into two columns. The left column, titled 'Control Detail', contains fields for 'Mitigation Control ID' (Vendor Master), 'Control Name' (Approval of changes to vendors), 'Description' (Approval of changes to vendors), 'Control Expiry' (18.05.2023), 'Risk Control Owner' (CMATTISON (Cameron Mattison)), 'Effectiveness' (Good), 'Type' (Prevent), and 'Nature' (System). The right column, titled 'Classifications', includes dropdowns for 'Business Process', 'Business Sub Process', 'Category', and 'Sub Category'. Below these is the 'Assessment Detail' section, which features a toggle for 'Generate Control Assessment Workflow', a 'Frequency' dropdown (Real-time), and a 'Last Assessment Date' (02.06.2022). At the bottom, there are three buttons: 'Back to Mitigation Controls', 'Delete Mitigation Control', and 'Save Mitigation Control'.

GRC Roadmap



- Policies and Procedures
- Removing un-used / over-allocated access
- Role redesign
- Emergency Access Management process
- Access Risk Rule Set
- Mitigating Controls
- User Access Reviews**





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

a. Business Education

i. Processes – P&P

ii. Risk Impact (educating them on the rule set)

b. Business Roles



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



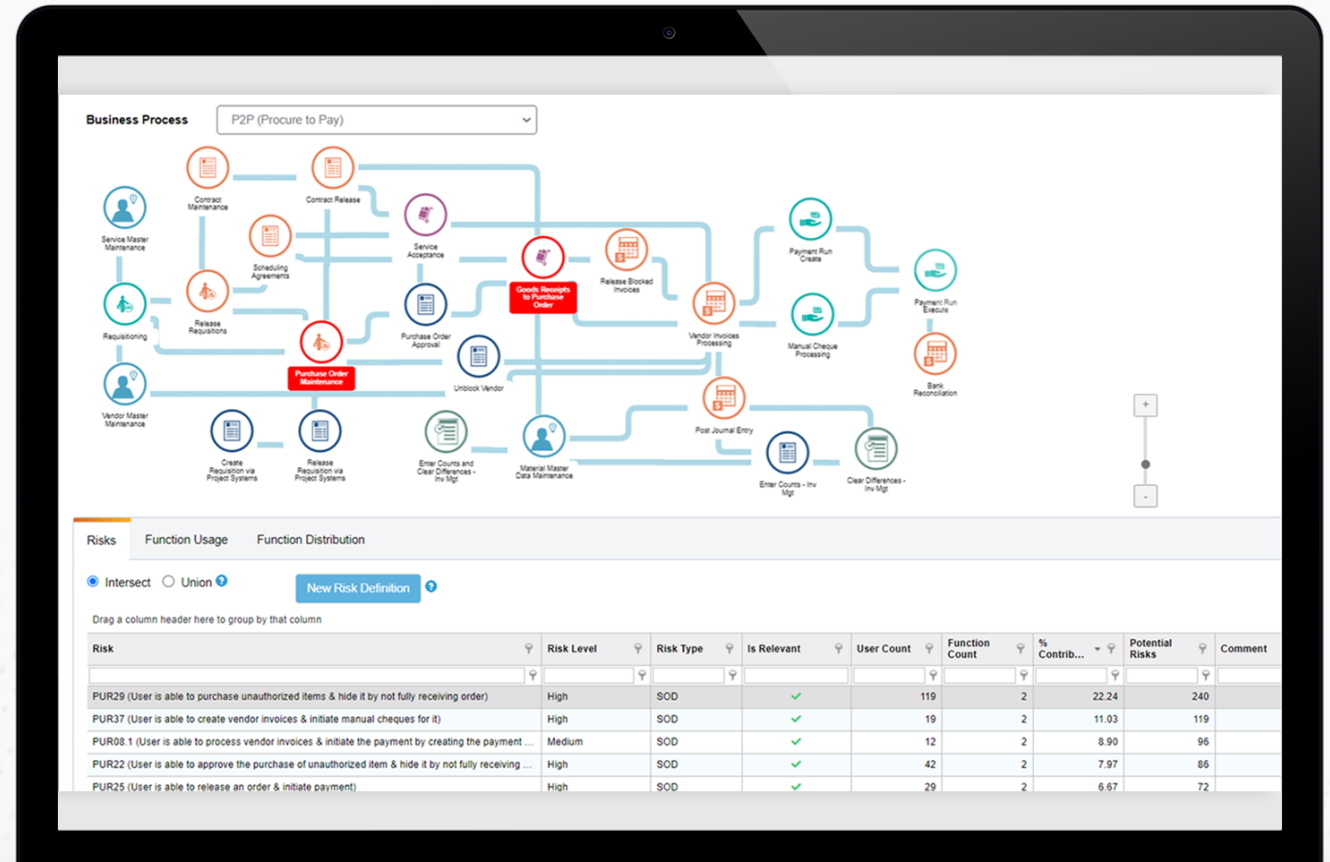
Comply with
Regulations

a. Business Education

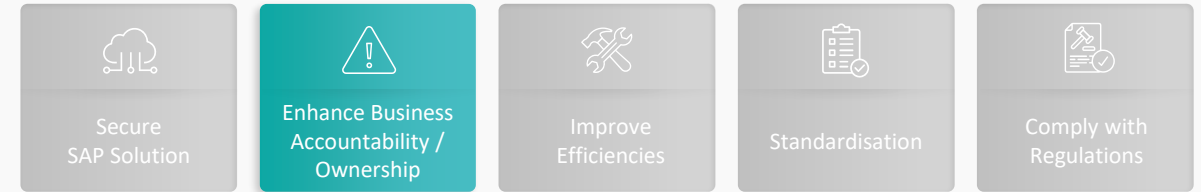
i. Processes – P&P

ii. Risk Impact (educating them on the rule set)

b. Business Roles



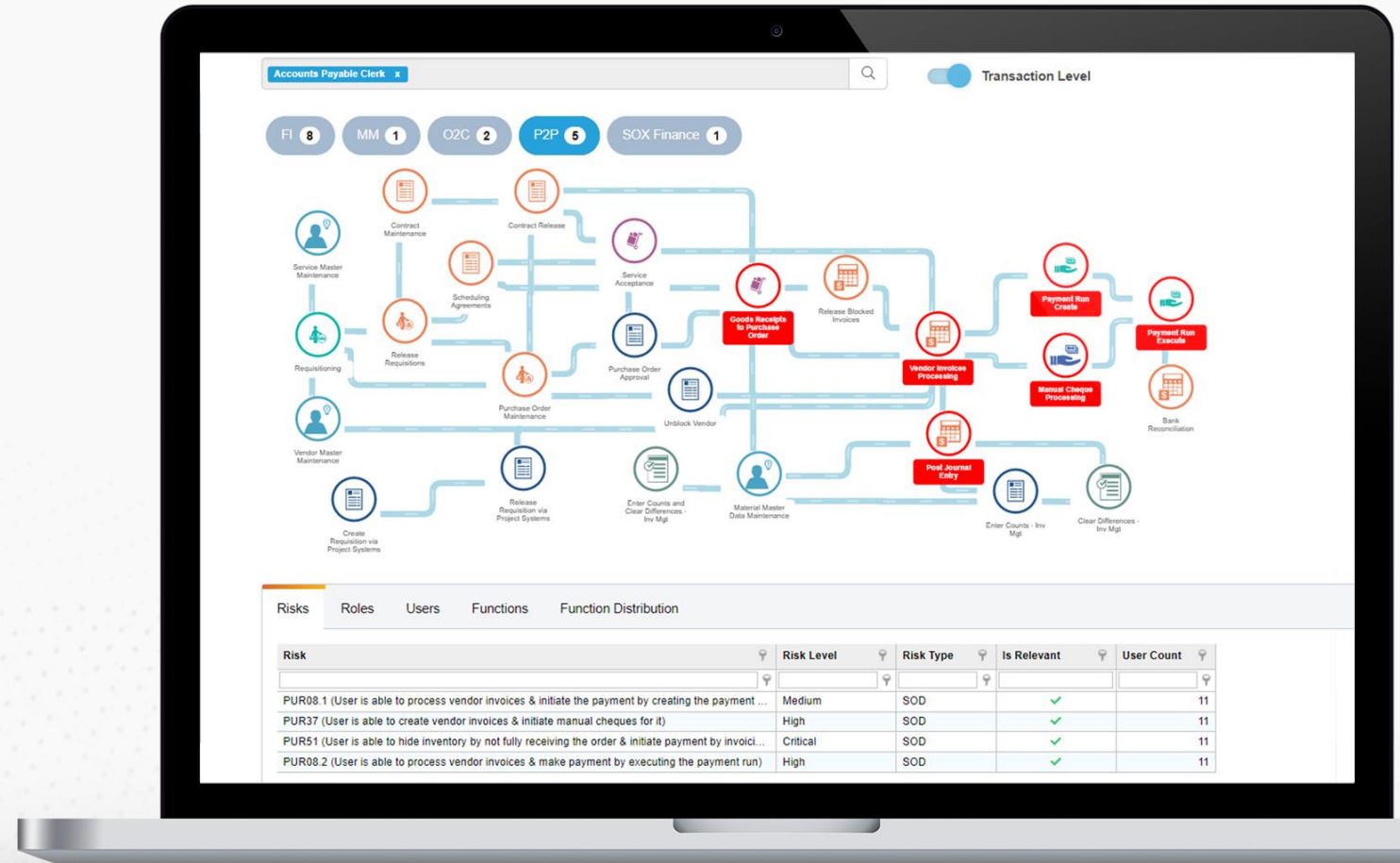
GRC Roadmap



a. Business Education

- Processes – P&P
- Risk Impact (educating them on the rule set)

b. Business Roles





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

- a. Business Roles
- b. SAP single role enhancements
- c. Compliance Tasks



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

a. Business Roles

b. SAP single role enhancements

c. Compliance Tasks



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

a. Business Roles

b. SAP single role enhancements

c. Compliance Tasks



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



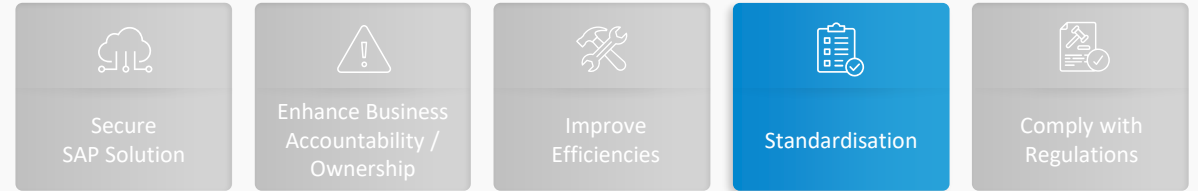
Standardisation






Comply with
Regulations

- a. Business Roles
- b. SAP single role enhancements
- c. Compliance Tasks**

GRC Roadmap



a. Business Roles

 Name	 SAP User ID	 Job Title
John Smith	JSMITH	Accounts Payable Clerk
Sarah Hallow	SHALLOW	Accounts Payable Clerk
Pete Drummond	PDRUMMOND	Accounts Payable Clerk
Tee Fox	TFOX	Accounts Payable Clerk
Kirtsy Stevens	KSTEVENS	Accounts Payable Clerk
Alan Duj	ADUJ	Accounts Payable Clerk
Kerry Long	KLONG	Accounts Payable Clerk
Tashni Song	TSONG	Accounts Payable Clerk



GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies

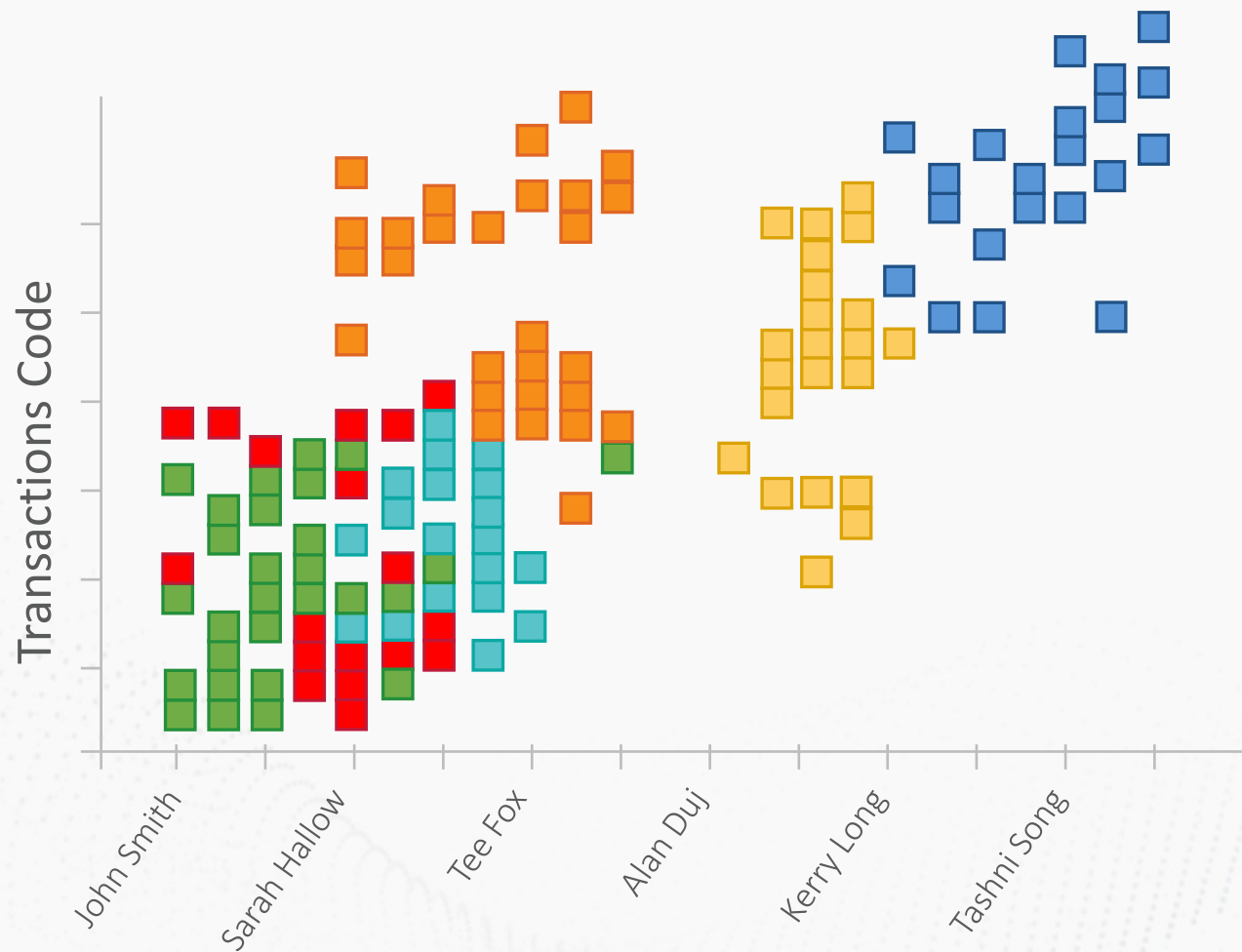


Standardisation



Comply with
Regulations

a. Business Roles





GRC Roadmap



Secure
SAP Solution



Enhance Business
Accountability /
Ownership



Improve
Efficiencies



Standardisation



Comply with
Regulations

a. Data Privacy Rule sets

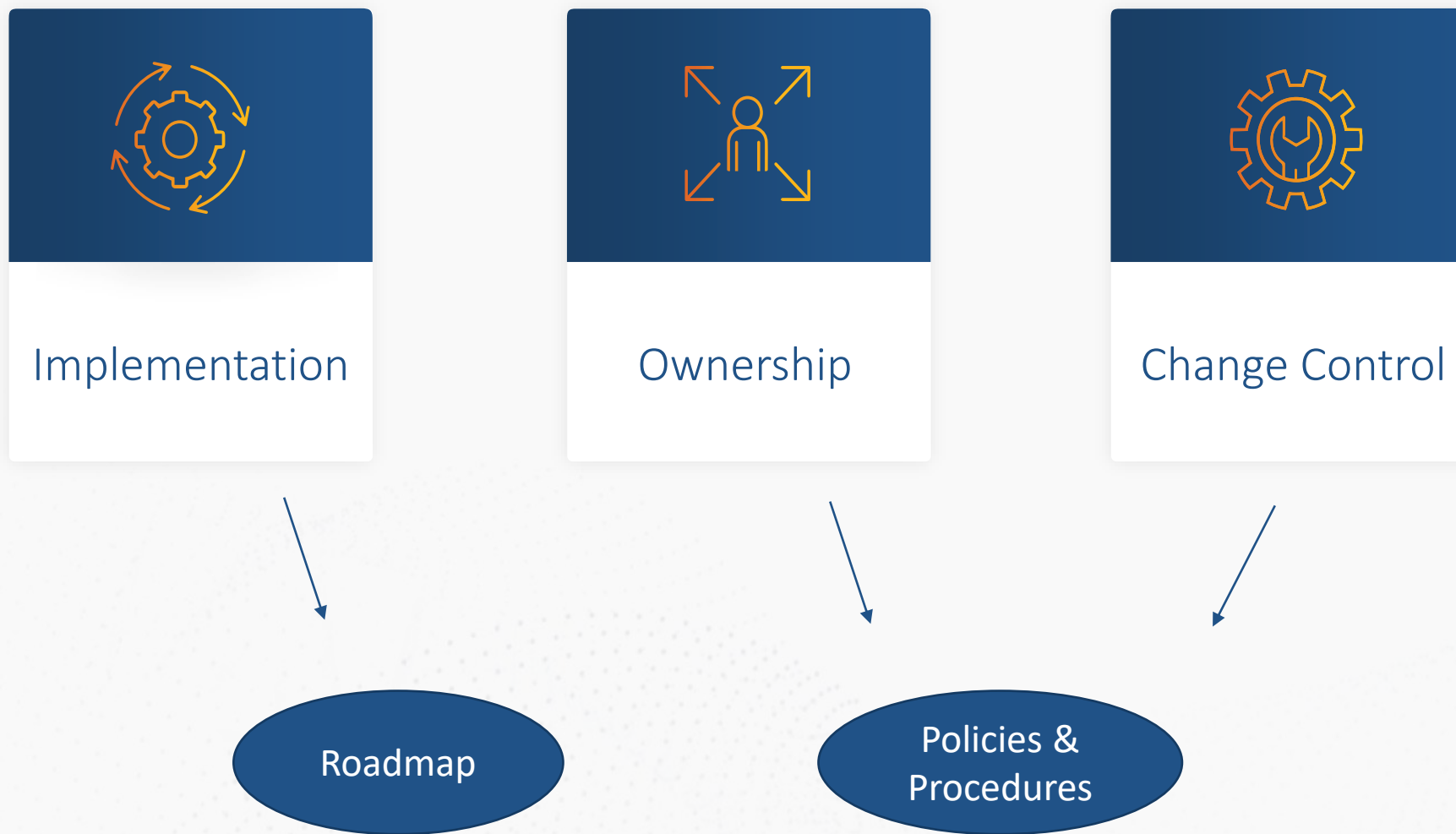
Takeaways



- ▶ View your GRC holistically
- ▶ Clearly define Policies and Procedures
- ▶ Define a GRC Roadmap



Takeaways



Thank you