

Delivering Security and Access Control Implementations at the Speed of Light with Crescent Energy

Juan Garza, Director, Crescent Energy
Mariah Jeffreys, Senior Property Accountant, Crescent Energy

Las Vegas

2024

SAPinsider



In This Session

- Prioritize key design criteria for both GRC Access Control and Security Role Design to focus your project scope to those necessary for system deployment
- Coordinate with the system implementation team to identify design requirements as efficiently as possible
- Tailor your project timeline to fit within an agile implementation approach
- Create the foundation of a governance framework within your SAP environment that will be scalable over time



What We'll Cover



Crescent Energy Background



Implementation Project Overview & GRC / Security Alignment



Project Challenges



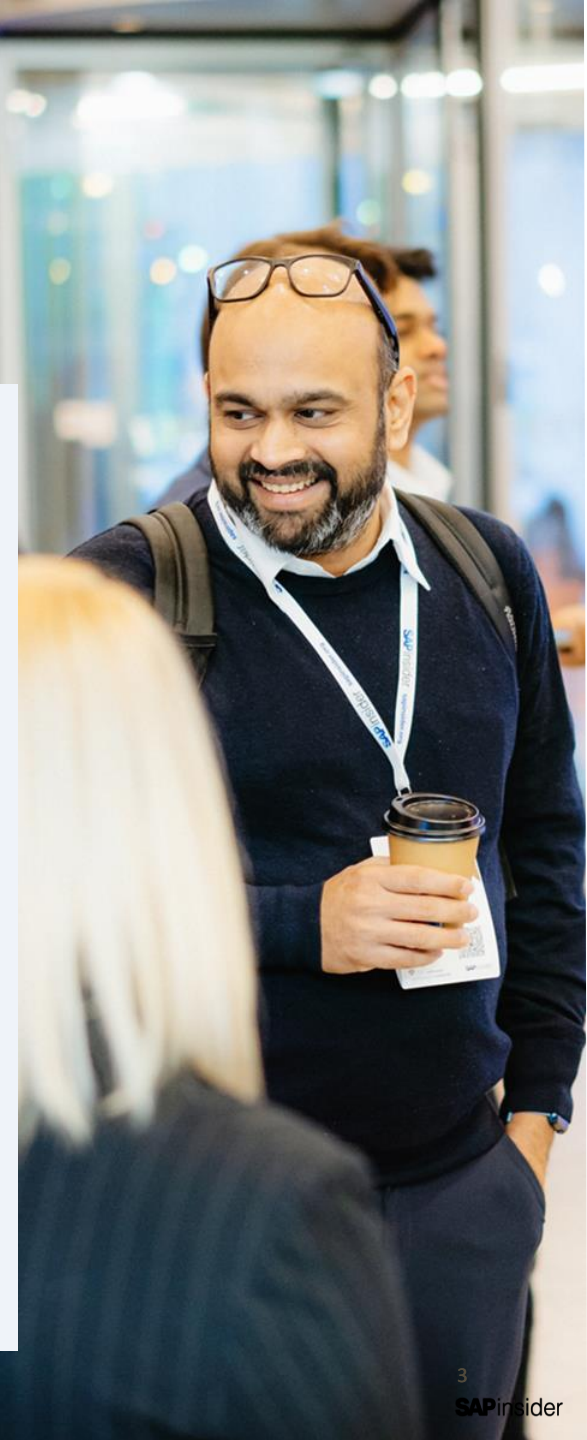
Project Successes



Lessons Learned



Wrap-Up



Project Drivers

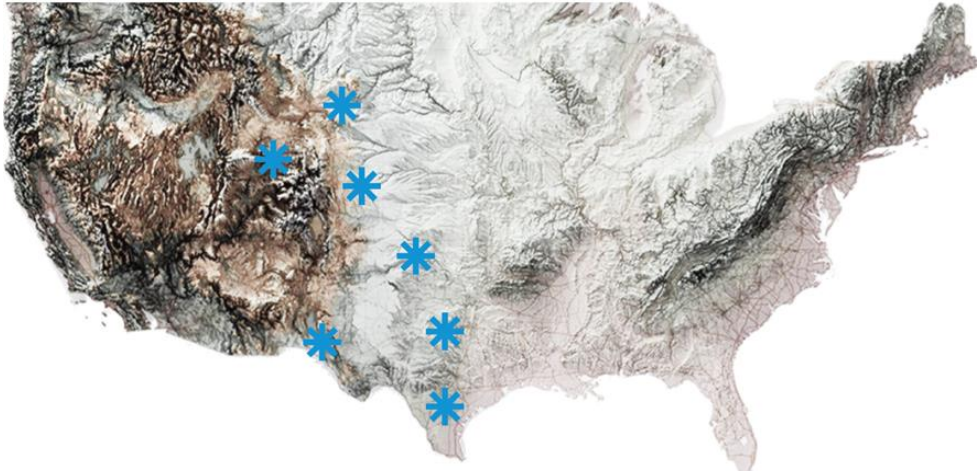
Acquisitions and Divestitures Model

Sustainable Growth and Scalability

IPO

Security, Audit and Traceability

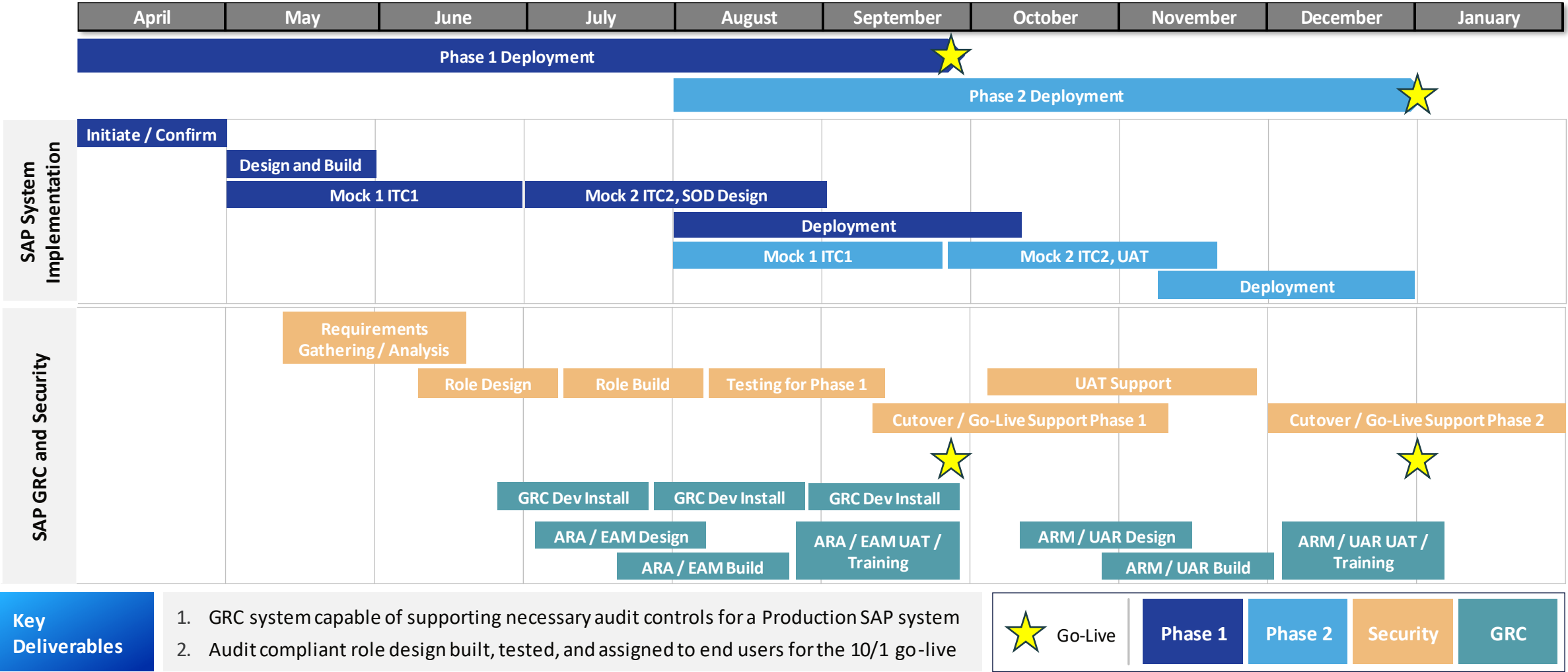
Governance, Risk, and Compliance



Crescent Energy:

- Operated Well Count: 14,000
- Non-Operated Well Count: 15,000
- Company Codes: 98+
- MBOED: 164
- Operating States: California, Texas, New Mexico, Oklahoma, Colorado, Utah, Wyoming

Implementation Project Overview & GRC / Security Alignment



Project Challenges

Risks Due to Timeline

Insufficient Time for Full Deployment of GRC

Compliance Concerns During Interim Period Between Go-Lives

Compressed Timeline for Role Design, Build, and User Assignment

Limited Availability of Implementation Team and Business Resources

Mitigation Plan

Risk Details

- Accelerated timeline meant the team could not configure and deploy all in-scope functionality of the GRC AC Module prior to the 10/1 go-live.

Solution

- Prioritized functionality in GRC that would support audit and compliance functions in Q4 2022 while remaining functionalities were configured for Q1 2023 deployment.
- Aligned with internal audit to ensure temporary gaps in functionality to be released in phase 2.

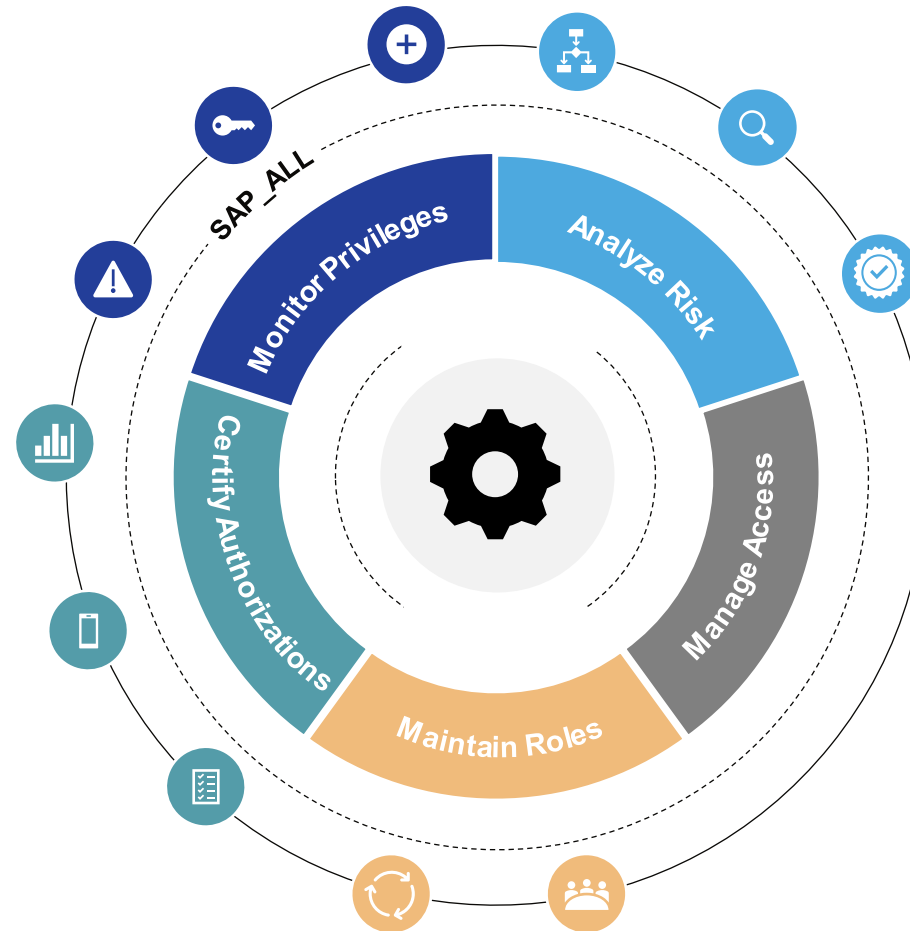
Project Challenges - SAP Application Security Controls

Firefighter (EAM)

Monitor emergency access and transaction usage

User Access Reviews (UAR)

Certify access assignments are still warranted



Access Risk Analysis (ARA)

Find and remediate Segregation of Duties (SoD) risks at the time of provisioning new or changed access

Access Request Management (ARM)

Automate approval and access assignment workflows within SAP for both new and changed access

Business Role management - Maintain role owner delegation for access approvals

Project Challenges

Risks Due to Timeline

Insufficient Time for Full Deployment of GRC

Compliance Concerns During Interim Period Between Go-Lives

Compressed Timeline for Role Design, Build, and User Assignment

Limited Availability of Implementation Team and Business Resources

Mitigation Plan

Risk Details

- Due to the decision to de-scope of ARM (Access Request Management) and UAR (User Access Review) for phase 1 go-live (10/1), the ability to leverage GRC to facilitate these processes wouldn't be available until phase 2 go-live (1/2)
- Assignment of sensitive access to perform cutover activities for the phase 2 go-live (1/2) in a live production environment.

Solution

- Established governance processes around user access management, SOD review, and FF log reviews to be used on Day 1.
 - Supplemented with temporary manual processes for user access management and SOD review to ensure audit compliance during Q4 2022.
- Created temporary elevated access ids (Firefighter) to be used by implementation support teams to execute cutover activities, while remaining audit compliant.

Project Challenges – Compliance Concerns During Interim Period Between Go-Lives

Firefighter ID/ROLE - All

View: [Standard View] [Open] [Assign] [Copy] [Reassign] [Delete]

Firefighter ID	System	Owner ID	Owner	Comments
<input type="checkbox"/> FF_ABAP_01	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	
<input type="checkbox"/> FF_ABAP_02	PS4CLNT100	JGARZA	Juan Garza	
<input type="checkbox"/> FF_ABAP_03	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Updated per approval on 3.31.23 by MB
<input type="checkbox"/> FF_ABAP_05	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	
<input type="checkbox"/> FF_BASIS_01	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Approved per INC34541 on 1.9.24 by MB and JG
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Extended per INC-25009
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Approved as part of the FFID consolidation 7.20.23
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	
<input type="checkbox"/> FF_BASIS_02	PS4CLNT100	JGARZA	Juan Garza	Approved per INC34541 on 1.9.24 by MB and JG
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	JGARZA	Juan Garza	Extended per INC-25009
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	JGARZA	Juan Garza	Approved as part of the FFID consolidation 7.20.23
<input type="checkbox"/> PS4CLNT100	PS4CLNT100	JGARZA	Juan Garza	
<input type="checkbox"/> FF_BASIS_05	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Updated per approval on 3.31.23 by MB
<input type="checkbox"/> FF_BASIS_06	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	
<input type="checkbox"/> FF_BUS_SUP01	PS4CLNT100	MBRACAMONTEZ	Michael Bracamontez	Provisioned through CUP for request number 699

Emergency Access Management

Firefighter	System Name	Firefighter ID Ow...	Status	FF ID Used By	Description	Logon Using FFID
FF_IT_BAS_01	DS4CLNT100	FFTESTOWNER	OC			Logon
FF_FIN_SUP01	DS4CLNT100	FFTESTOWNER	OC			Logon

Multiple Selection

Analysis Criteria

System: IS PS4CLNT100
Object ID: EXCLUDE SAPSUPPORT
Rule Set ID: IS HGRBRISK
Risk Level: IS

Object Type: User
Offline Date: NO
User Type: Dialog
Type: Permission Level

Include Mitigated Risks: X
Consider Obj Rules in the Risk Analysis:
Show All Objects in Risk Analysis Report: X
Show descriptions in Risk Analysis Report: X
Report Format View Type: Business View


Analysis Results

Result Set: [Result Set 1] [Go] [Previous] [Next] [Export Result Sets]

Result

View: [Standard View] [Display As: Table] [Print Version] [Export] [Type: Permission Level] [Format: Management Summary] [Mitigate Risk]

User Group	Access Risk ID	Risk Description	Control	Monitor	Monitor Name	Business Process	Business Process Description
<input type="checkbox"/>	F002	Alter a cost center and process unauthorized cost transfers	FIN_02	MGASPARINI	Matteo Gasparini	F002	Finance
<input type="checkbox"/>	PRAD9	Access to maintain check input master data AND enter checks (via manual or CDEX) is segregated	FIN_02	MGASPARINI	Matteo Gasparini	PRAD9	Production Revenue Accounting
<input type="checkbox"/>	S015	Risk of Sales Prior modifications for Sales Invoicing	OTC_01	MGASPARINI	Matteo Gasparini	S000	Order to Cash (Accounts Receivable, Receiving, Sales)
<input type="checkbox"/>	S026	Maintain an invoice and enter or change payments against it	OTC_02	MGASPARINI	Matteo Gasparini	S000	Order to Cash (Accounts Receivable, Receiving, Sales)
<input type="checkbox"/>	S029	Create a credit memo then clear the customer to prompt a payment.	OTC_02	MGASPARINI	Matteo Gasparini	S000	Order to Cash (Accounts Receivable, Receiving, Sales)
<input type="checkbox"/>	S033	Process Customer Invoices & Clear Customer Balance	OTC_02	MGASPARINI	Matteo Gasparini	S000	Order to Cash (Accounts Receivable, Receiving, Sales)
<input type="checkbox"/>	F002	Alter a cost center and process unauthorized cost transfers	FIN_02	MGASPARINI	Matteo Gasparini	F002	Finance
<input type="checkbox"/>	JV02	Joint Venture Master Data & Joint Venture Processing	JVA_06	MGASPARINI	Matteo Gasparini	JV00	Joint Venture
<input type="checkbox"/>	JV03	Joint Venture Master Data & Process Customer Credit Memos	JVA_01	MGASPARINI	Matteo Gasparini	JV00	Joint Venture
<input type="checkbox"/>	JV04	Joint Venture Master Data & Clear Customer Balance	JVA_02	MGASPARINI	Matteo Gasparini	JV00	Joint Venture



With the GRC implementation priorities set to include Firefighter and Access Risk Analysis, interim controls were set up between Go-Lives

- **Access Risk Analysis**

- Ad-hoc risk analysis performed on a monthly basis
- For access request tickets, these continued to be processed manually with a step included an SOD simulation using ARA
- Mitigating controls were assigned for any SOD risks that could not be remediated

- **Firefighter**

- Firefighter IDs required for supporting the first go-live and for cutover during the second go-live were manually assigned
- FF log review was implemented for the first go-live, ensuring the process was in place from the start, avoiding manual FF log review challenges

Project Challenges

Risks Due to Timeline

Insufficient Time for Full Deployment of GRC

Compliance Concerns During Interim Period Between Go-Lives

Compressed Timeline for Role Design, Build, and User Assignment

Limited Availability of Implementation Team and Business Resources

Mitigation Plan

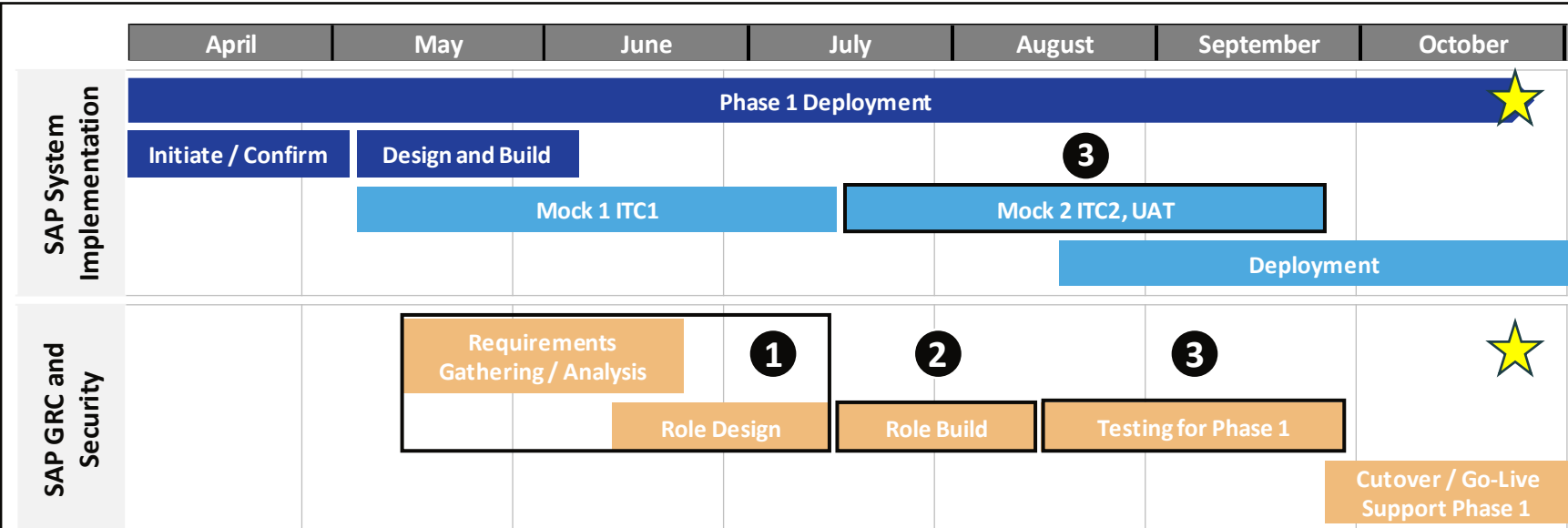
Risk Details

- Due to the complexity of SAP security, ample time is needed to understand the business operations and system customizations, which are crucial for designing and implementing a security role design that aligns with business needs.

Solution

- Utilized leading practice template role design as baseline and leveraged Protiviti's industry expertise to focus on specific customizations needed for the role design.
- Utilized accelerators to expedite role building and quality assurance activities, ensuring readiness for the 10/1 go-live.
- Conducted security testing phases concurrently with system integration testing, accelerating the overall testing process.

Project Challenges – Role Design Timeline



- Leveraged Protiviti Leading Practice role design and focused attention on specific functional restrictions:
 - Task-based role design enabled future enhancements and provided scalability.
- Utilized accelerators to complete build and QA activities:
 - SAP GUI Scripting.
 - Custom Org Program.
 - Role QA Tool.
- Conducted Security UAT for phase 1 in parallel with system UAT to ensure no delays in overall timeline.



Task	Description	Priority	Status
Task 1	...	High	Complete
Task 2	...	Medium	In Progress
Task 3	...	Low	Not Started



Project Challenges

Risks Due to Timeline

Insufficient Time for Full Deployment of GRC

Compliance Concerns During Interim Period Between Go-Lives

Compressed Timeline for Role Design, Build, and User Assignment

Limited Availability of Implementation Team and Business Resources

Mitigation Plan

Risk Details

- Project team and business resources had conflicting priorities due to the simultaneous implementation of S/4 HANA, with primary focus being the implementation of the S/4 system.

Solution

- Prioritized GRC and Security tasks to address competing priorities, focusing on the highest ROI while efficiently utilizing time from business and project stakeholders.
- Leveraged off-shore resources in a “follow-the-sun” model to optimize productivity across different time zones.

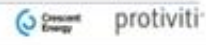
Project Challenges – Resource Availability

User ID	User Name	Description	Start Date	End Date	Mapping Status
3025NM_WFM-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_CUST-SIN-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_CUST-SIN-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025LUM_JMI-GRD-SIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PF_DTS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PF_RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_DTS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_SAX-ACRHP-ENR_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PS_I1-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PS_P1-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_MID-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_PO-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_PO-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_PP-ORL_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_PP-Q-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025QMS_DTS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025QMS_RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025WMT_DTS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025WMT_RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PVT_RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025IM_CDRNGRC-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025IM_RPT-ADM_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025IT_CA_CDRNG-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025IT_CA_SABLS-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025IT_SEC-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_CDR-REV-REC-RPT_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_CDR-REV-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PMA_RIS-RPT-ADM_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File
3025PUR_SEC-ADR-DIS_SUBL	Juan Garcia		10/5/2022	12/31/9999	Excellent File

DETAILED SOD RULESET REVIEW WORKSHOP

- The ruleset review will be performed by process area and feedback will be captured by the team within the detailed review document.
- Decisions will be captured at the risk level by reviewing the conflicting functions that make the risk.

Business Process	Role ID	Function 1	Function 2	Risk Detail	Default SAP Risk Level	Risk Level	Index
Process to Pay	PE07	Release Requisitions	Registration	Risk of the same person-responsibility on item and then issuing a requisition for purchase following the authorization process.	Medium	Medium	Active
Process to Pay	PE08	AP Payments	Bank Reconciliation	Users may conceal payments by adjusting the bank reconciliation account. This can result in overstating the financial statements withing their transaction financial reporting and misrepresentation of the account.	High	High	Active
Process to Pay	PE09	Process Under Invoice	Service Acceptance	A user with the ability to accept the invoice and process the subsequent invoice could either state that they have accepted the invoice when in fact they had not or over-accept and create payment through the processing of the invoice. This is a problem not where the vendor is a one time vendor or alternative payee is allowed.	Medium	Medium	Active

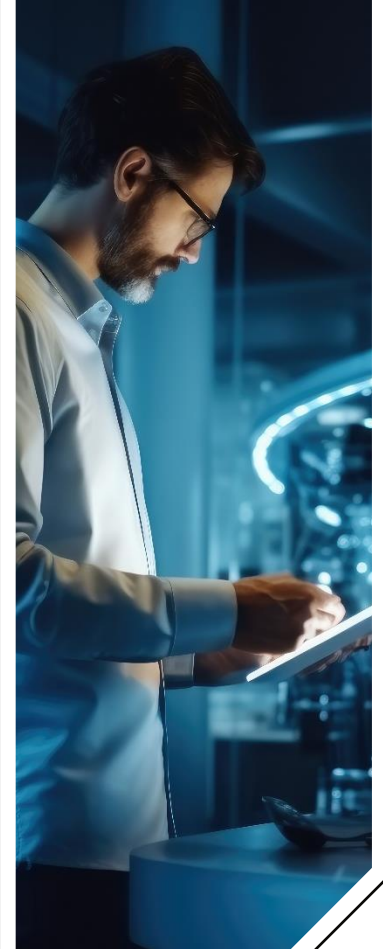


Role Name	Role Description	User Name	User Status	Admin Function	Status	User Role	User Status	User Role	Security Profile	Security Profile	Security Profile	Comments
...
...
...

- Reduced the time needed from implementation team and business stakeholders to key decision points:
 - GRC
 - Facilitated offline ruleset review / approval.
 - Leveraged standard GRC workflows with minimal customization.
 - Security
 - Focused attention on Functional Restrictions and User Mapping.
- Deployed a blended team of on-shore and off-shore resources:
 - “Follow-the-Sun” approach.
 - Majority of security testing executed by off-shore team.

Project Successes

- Successfully met both scheduled Go-Live timelines with minimal business disruption between the first and second Go-Lives.
- Out of Box solution from Protiviti fulfilled over 80% of our requirements, enabling the accelerated timeline.
- Knowledge transfer sessions allowed business to take over without major disruptions.
- Efficiently prioritizing key design criteria for GRC Access Control and Security Role Design, leading to a focused project scope and streamlined deployment process.
 - Effectively coordinating with the system implementation team to identify design requirements promptly, ensuring smooth collaboration and timely decision-making.
- Adapting the project timeline to fit within an agile implementation approach, fostering flexibility and responsiveness to evolving requirements.
 - Meeting demanding implementation timeline objectives.
- Creating a robust governance framework providing a scalable foundation for ongoing management and compliance.
 - Usable from day one of the initial go-live ensuring compliance with audit requirements and regulations.



Lessons Learned

- Significance of tailoring project timelines to fit within an agile implementation approach, allowing for flexibility and adaptability.
- Importance of prioritizing key design criteria for GRC Access Control and Security Role Design to ensure project focus and efficiency.
 - Access Risk Analysis (ARA) and Emergency Access Management (EAM) modules from GRC to cover many compliance requirement (with less automation than ARM and UAR).
 - Designing Controls for accessing data.
 - Defining a scalable security role design solution from day one.
- Security change management during transition period (carefully handling of impact on current live users and future users).
- Consistent communication between Business and SI is essential for this type of agile project, enabling quick responses to testing and issues, ensuring they are addressed quickly.



Wrap Up

- Importance of prioritizing SAP Security and Controls during an S/4 implementation to ensure compliance and safeguard of your system's integrity.
- Selecting the right partner for SAP transformation is crucial, considering long-term value and cost savings over mere cost-effectiveness.
- Best-in-class security architecture includes scalable design, mitigating audit findings for cost efficiency, and enhancing productivity through streamlined access.
- Independence from systems integrators (SIs) ensures unbiased perspectives on SAP requirements, leading to optimal outcomes and effective project governance.



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/>

- Blog post discussing considerations for selecting vendors to implement Security and Controls during an SAP S/4HANA implementation

Mohammed Abdullahi, “System Integrator or Security Specialist: Who Should Be Responsible for Implementing S/4HANA

<https://www.sap.com/products/erp/rise.html>

- Additional information on RISE with SAP, which was used for the rapid deployment of SAP at Crescent

<https://www.protiviti.com/us-en/whitepaper/erp-system-implementation>

- White Paper detailing the various responsibilities across an ERP System Implementation

Carol Raimo and John Harrison, “Understanding the Responsibilities of the Business During an ERP System Implementation” (SAP Implementation and Transformation Leaders)

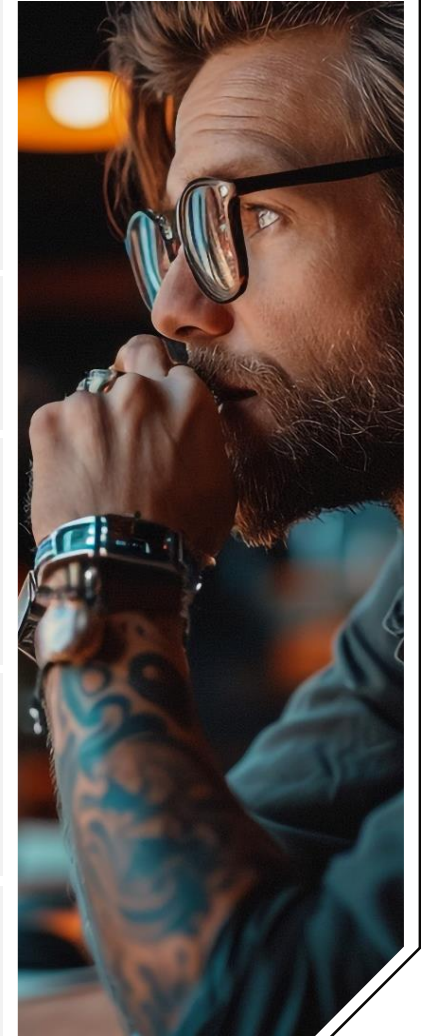
<https://sapblog.protiviti.com/2023/10/04/risk-management-essentials-for-sap-s-4hana-projects/>

- Blog post discussing the importance of risk management during SAP S/4HANA projects

Chris Hanson, “Risk Management Essentials for SAP S/4HANA Projects” (SAP Transformation Expert, October 2023)

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

- Subscribe to SAP Insights featuring SAP blogs and monthly newsletters



Key Points to Take Home

- Creating a project timeline that aligns with an agile implementation approach for flexibility and adaptability.
- Prioritizing SAP Security and Controls during an S/4 implementation.
- Choosing the appropriate partner for SAP transformation.
- A top-tier security architecture involves scalable design.
- Maintaining independence from systems integrators (SIs).



Thank you! Any Questions?



Juan Garza

Director of Business Solutions

Juan.Garza@crescentenergyco.com

[Linkedin.com/in/juan-j-garza/](https://www.linkedin.com/in/juan-j-garza/)



Mariah Jeffreys

Senior Property Accountant

Mariah.Jeffreys@crescentenergyco.com

[Linkedin.com/in/mariah-jeffreys/](https://www.linkedin.com/in/mariah-jeffreys/)

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.**
