A picture containing sky, screenshot, text, outdoor

Description automatically generated

Logo

Description automatically generated

**CalSAWS M&O RFP #01-2022  
VOLUME 1A – INFRASTRUCTURE BUSINESS BAFO**

**Infrastructure Understanding and Approach to the CalSAWS Integrated Multi- Contractor Environment**

August 29, 2023

Table of Contents

[I-UA1 Describe your approach to managing your scope of work and how you will coordinate with other involved CalSAWS contractors and the CalSAWS Delivery Integration Team to ensure understanding and agreement of the roles and responsibilities of each Contractor and the Consortium. 1](#_Toc143093650)

[5.2.3.1.1 Approach to Managing the Scope of Work 1](#_Toc143093651)

[5.2.3.1.1.1 Steps in our Scope Management Approach 2](#_Toc143093652)

[5.2.3.1.2 Approach to coordination with other involved CalSAWS contractors and the CalSAWS Delivery Integration Team 4](#_Toc143093653)

[5.2.3.1.3 Roles and Responsibilities for each Contractor and the Consortium 7](#_Toc143093654)

[I-UA2 Describe your approach to working and collaborating with the CalSAWS M&E Contractor to perform shared services, such as security, and supporting Application Evolution and Innovation. 9](#_Toc143093655)

[5.2.3.1.4 Approach to working and collaborating with the CalSAWS M&E Contractor to perform shared services 9](#_Toc143093656)

[5.2.3.1.5 Approach to Security Services 10](#_Toc143093657)

[5.2.3.1.6 Approach to Supporting Application Evolution and Innovation 12](#_Toc143093658)

[I-UA3 Identify major risks inherent in the Integrated Multi-Contractor Environment and your proposed mitigation strategies. 13](#_Toc143093659)

[5.2.3.1.7 Major Risks and Proposed Mitigation Strategies 13](#_Toc143093660)

Table of Figures

[Figure 1: Kyndryl’s Communication Cadence 2](#_Toc144127930)

[Figure 2: Alignment of Roles 5](#_Toc144127931)

[Figure 3: Multi-Vendor Operating Model 7](#_Toc144127932)

[Figure 4: RACI Model Example 9](#_Toc144127933)

Table of Tables

[Table 1. Scope Management Approach 2](#_Toc144127923)

[Table 2. Risks and Mitigation Strategies 13](#_Toc144127924)

5.2.3.1 Infrastructure Understanding and Approach to the CalSAWS Integrated Multi-Contractor Environment

Cross Reference: CalSAWS-MO-RFP-01-2022-Infrastructure-BAFO-1-Instructions-Final-071823.pdf, Page 2 and CalSAWS M&O RFP 01-2022 071823 Addendum 11 TC.docx Section 5.2.3.1, Pages 119-120

I-UA1 Describe your approach to managing your scope of work and how you will coordinate with other involved CalSAWS contractors and the CalSAWS Delivery Integration Team to ensure understanding and agreement of the roles and responsibilities of each Contractor and the Consortium.

## Approach to Managing the Scope of Work

Our approach to scope management starts with goal and scope definition.

The foundation of our approach is collaborative communication.

We start by establishing clear scope definition between ourselves, CalSAWS stakeholders, and our M&E partners across all delivery areas. We collaborate at the start of any effort to outline specific responsibilities and deliverables related to infrastructure support but in the context of the larger goals and scope of an effort. When it is not possible to define technical scope upfront, like when innovating on new solutions, we begin with defining the goals and outcomes of the work clearly, so that each team has a north star to guide their decisions and actions while technical scope is discovered and clarified.

Our teams meet and communicate with stakeholders and our M&E partners regularly to ensure alignment with the overall project's objectives and the specific requirements set by CalSAWS consortium.

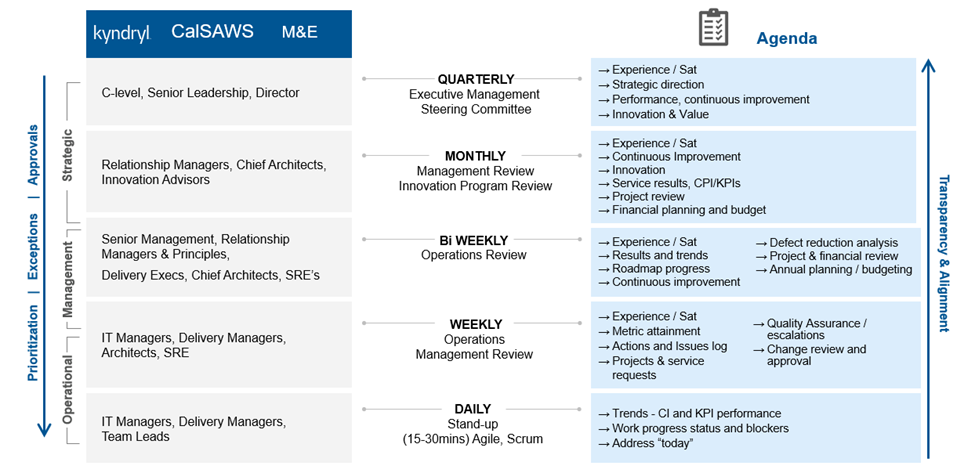
**

Figure 1: Kyndryl’s Communication Cadence

### Steps in our Scope Management Approach

The table below provides an overview of the steps involved in our scope management approach.

Table 1. Scope Management Approach

| **Description** | **Steps Involved** |
| --- | --- |
| **Collaborative Communication** | Foster open and frequent communication with all stakeholders, including the CalSAWS Consortium, other IT vendors, and our internal team members.  Regular meetings, status updates, and issue tracking mechanisms are established and maintained to provide transparency and address any potential challenges promptly. |
| **Establish and Maintain Service Level Agreements (SLAs)** | Partner to continuously define and refine SLAs to achieve expected response times, issue resolution, and performance metrics for infrastructure support.  SLAs align directly with the criticality of the services provided and the needs of the solution.  Clearly identify and gain agreement on demarcation points for multi-contractor SLAs.  Monitor and systematically collect performance and availability metrics across IT solutions from AWS environments to physical devices used by CalSAWS in the field. |
| **Risk Management** | Identify any potential risks related to infrastructure operations support and devise mitigation strategies at the start of planning.  Partner with other M&E vendors to assess the risk and devise mitigation strategies; particularly for those SLAs and service requirements that depend on multiple CalSAWS Consortium contractors for success.  Continuously update and monitor a risk log against operations and address issues and interdependencies as identified to ensure the continuity of operations. |
| **Change Management** | Follow CalSAWS’ four gates of change management practice, leading the discussion from the Infrastructure Operations perspective from Change Request submission to implementation.  Share our insights and experience with change management as a result of working with other customers to help enhance CalSAWS’ process.  Accountability, transparency, responsiveness, inclusiveness, and empowerment are the cornerstones of a successful change management practice. |
| **Security and Compliance** | Prioritize security measures and processes above all else to protect sensitive data.  Conduct Security and Architecture reviews both internally and with M&E partners to ensure compliance with relevant standards, ensuring all compliance requirements are well defined and continuously met.  Kyndryl’s Security and Resiliency practice will regularly review our current posture and recommend enhancements as the security environment evolves and changes.  Primary security goal of the M&O vendor is to establish a culture of security awareness among all teams where rapid remediation is achievable. |
| **Performance Optimization** | Continuously monitor and optimize the AWS infrastructure, Network infrastructure, and physical devices performance to ensure demands are met efficiently.  Proactively perform capacity planning and system tuning to enable seamless operations along with innovation ideas to help mature and enhance the CalSAWS products. |
| **Knowledge Sharing** | Encourage proactive knowledge sharing, collaboration, and joint training among all vendors to foster a cohesive and well-informed approach.  Cross-training and documentation are essential to not only build relationships and understanding between teams but to also ensure continuity across teams and to ensure each group has a working knowledge of each other’s capabilities and challenges. |
| **Regular Reporting** | Provide regular status reporting to CalSAWS and M&E partners following agreed upon formats ensuring to highlight key performance indicators, service achievements, and any areas for improvement for collaboration or operations  Communicate and work with the Consortium and M&E partners to continuously improve reporting information and approaches. |
| **Continuous Improvement** | Continuously seek opportunities for improvement and innovation of the CalSAWS infrastructure support services.  Enhance operational resilience and performance while maximizing the benefits of leveraging multiple vendors.  Focus on financial and security improvements from the M&O perspective. |

## Approach to coordination with other involved CalSAWS contractors and the CalSAWS Delivery Integration Team

Kyndryl’s approach to coordination with the CalSAWS Delivery Integration Team and other CalSAWS contractors revolves around building a culture and communication process that enables open and end-end collaboration with all client teams and their IT partners. We will continuously focus on building and maintaining cooperative relationships with the Delivery Integration team and other CalSAWS contractors like Gainwell, Deloitte, ClearBest, as well as any future partners which may join the program. We have successfully partnered with Gainwell and Deloitte many times in the past with other clients and feel we can do so for CalSAWS as well.

Kyndryl’s core business is Managed IT Infrastructure services, so nearly all our work for the last 30 years has been done in multi-contractor environments. We believe that in a multi-vendor IT environment like CalSAWS, relationship building is a crucial aspect that fosters collaboration, communication, and mutual understanding among all parties involved.

Here's what it looks like in practice.

Relationship management at all levels:

Kyndryl Senior management takes the lead in building relationships with key peer representatives from each M&E Partner and with Sr. Leaders of CalSAWS. Regular meetings and communication with M&E executives help set a positive tone and demonstrate a shared organizational commitment to collaboration for each organization.

At the practitioner level, Kyndryl’s Delivery Integration Manager will lead the Kyndryl teams and will own the relationship with the CalSAWS Delivery Integration office. Kyndryl’s Delivery Integration Manager will represent Kyndryl in all governance and planning discussions with the Delivery Integration Office so there is a consistent voice when speaking to CalSAWS as well as consistent leadership and direction to the Kyndryl teams.

Kyndryl’s Delivery Integration Manager will also ensure that relationship campions are identified and assigned to each M&E Partner to build relationships and facilitate communication across projects and teams. These champions act as central points of contact between engineering teams and facilitate communication, address concerns, and ensure alignment of goals at the task level. These champions build trust with the M&E partners and allow for open dialog based on a shared respect.

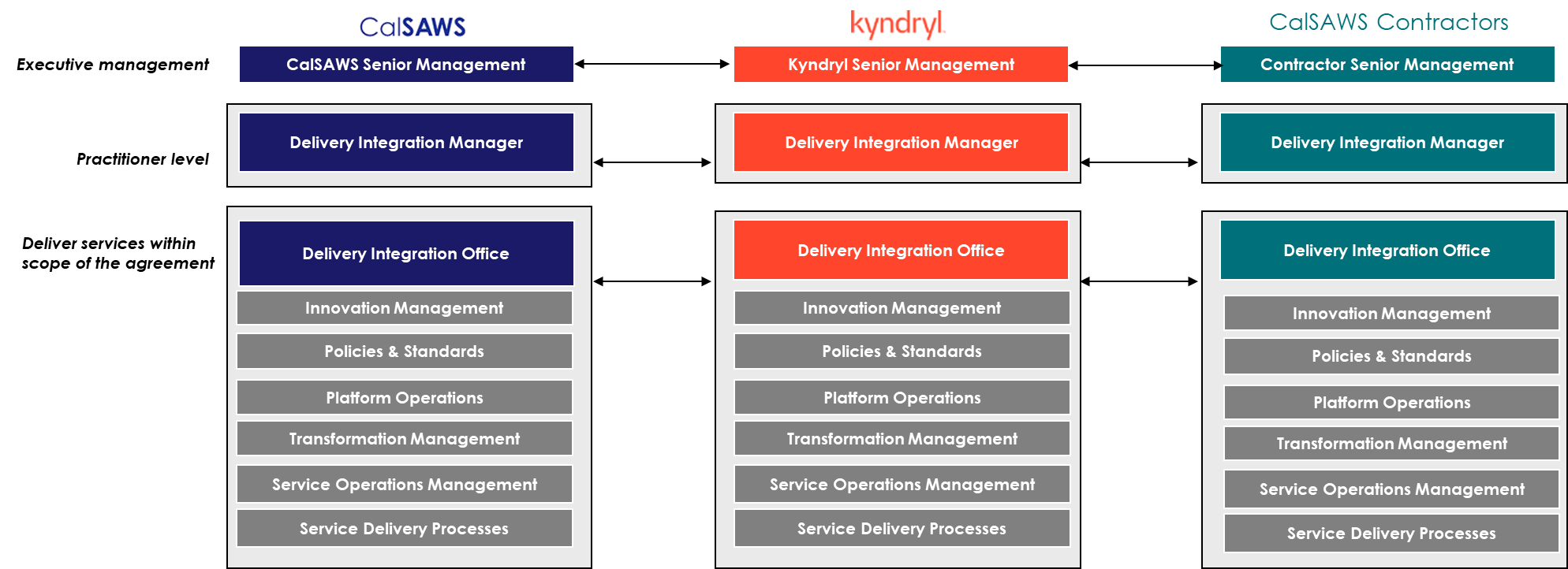
**

Figure 2: Alignment of Roles

* **Open Communication:** Kyndryl ensures essential open and transparent channels of communication through regular meetings with other partners, shared email groups, and status reports which are shared to enable discussion project updates, concerns, and communication style and approach feedback.
* **Shared Goals:**We believe that all vendors and stakeholders should align with the organization's overall goals. Kyndryl will partner with the Delivery Integration Office to design and deliver projects that span both M&E and M&O by design. We find that innovation happens when teams trust and respect each other working towards a shared objective. This often means designing projects so that teams cannot easily form silos. When everyone is working towards the same objectives, it promotes a cohesive environment that encourages teamwork. To this end we strive to ensure none of our goals are M&O specific, but instead written from the view of CalSAWS which forces the M&E perspective into M&O deliverables.
* **Trust and Respect:** Building trust and mutual respect is fundamental. All vendors need to trust that their contributions are valued, while the organization must trust the vendors to deliver quality services and products. To that end we build recognition and appreciation of other M&E partners into our own process. Recognizing and appreciating the efforts of partners when they deliver exceptional results or go beyond expectations is a positive reinforcement that strengthens our relationships. We also work to conduct shared team building exercises to build relationships outside of the core deliverable work when possible.
* **Conflict Resolution:** Inevitably, conflicts may arise. The key is to address them promptly and constructively. To achieve this, we collaborate with the Delivery Integration Office and each partner to establish a process for conflict resolution. Kyndryl relationship champions will work with their peers on their M&E team to ensure any disputes are clearly defined and effectively mitigated through conversation and negotiation. Flexibility drives resolution to most conflict, and we believe M&O vendors like ourselves should be willing to adapt to evolving requirements and provide flexibility when needed to our partners on the M&E side whenever possible. You will find we are ready to compromise on almost anything in our control except security and compliance to drive resolution and results between teams.

By nurturing these aspects of relationship building in a multi-vendor IT environment, Kyndryl and the Delivery Integration Team can create a harmonious and productive ecosystem with our M&E partners that supports the successful execution of projects and maximizes the benefits of working with multiple vendors.

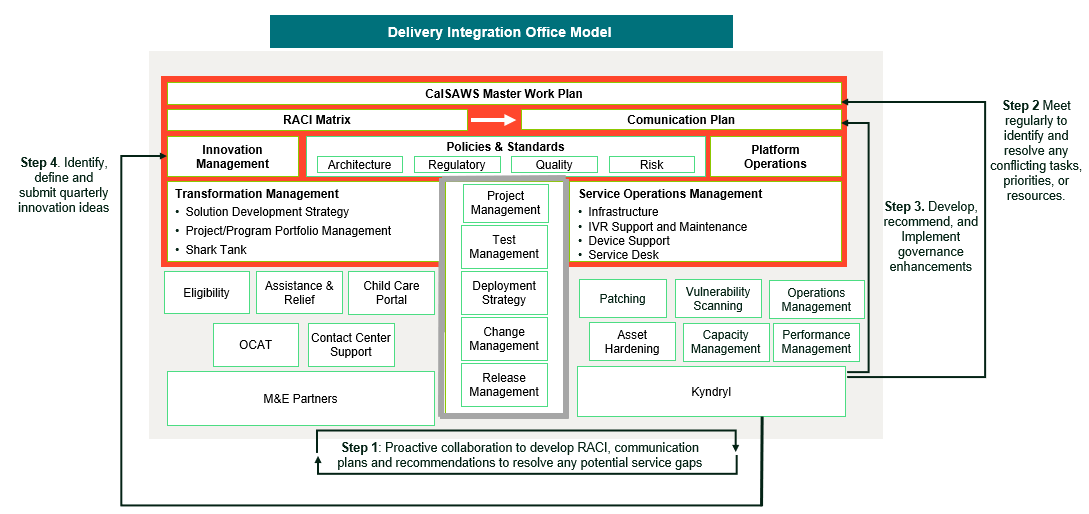


Figure 3: Multi-Vendor Operating Model

## Roles and Responsibilities for each Contractor and the Consortium

Defining roles and responsibilities with client teams and other client vendors is a well-practiced skilled here at Kyndryl. We have developed a process to guide teams through this exercise but recognize that each scenario is unique and requires adaptation and improvisation.

Establishing roles and responsibilities starts with identifying shared objectives the Consortium has for each contractor as well as independent objectives we have from our M&O and M&E perspectives for any effort. We do this to develop a shared understanding of the Consortium’s goals, desired outcomes, and implications for each vendor. We ensure designated representatives from each team who will actively participate in the role and responsibility definition process are identified and assigned the responsibility. These representatives will act as points of contact for their respective groups.

Once the team members from Kyndryl, the Consortium, and the M&E partners are assigned they kick off dialog with an initial RACI planning. During these sessions the team conducts an initial brainstorming where representatives from all three groups come together to share their understanding of the project, requirements, and their perception regarding ownership of roles and responsibilities.

We encourage open dialogue to gather different perspectives and determine an initial draft of tasks and deliverables mapped back to the owning party. The goal is for the team to collaboratively map out the tasks and deliverables required to achieve the project objectives. The team identifies areas of overlap or where they can assist each other as well as any potential gaps in responsibilities. At the end of this exercise the team completes a RACI matrix individually which is then combined as a group to clearly demarcate Responsible, Accountable, Consulted, and Informed.

During this discussion, the representatives from each team negotiate and discuss the allocation of tasks and responsibilities to ensure consensus. The goal of this is to seek alignment with skills and expertise across individual groups to ensure that each group's roles align with their areas of subject matter expertise.

Once alignment is obtained the team works together to update the documented roles and responsibilities. The finalized document is communicated to all team members involved in the project with emphasize on the importance of adhering to the agreed-upon roles but an understanding some things may need to change and be updated as more is discovered and project progress.

As work begins regular check-ins are performed to ensure any needed adjustments are made. We coach our teams to always be open to adjusting if needed due to changing project requirements, new information being identified, or to introduce process enhancements.

By following this process, all groups can work together more effectively, with clear roles and responsibilities, fostering a collaborative and productive working environment that leads to successful project outcomes.

A screenshot of a document

Description automatically generated

Figure 4: RACI Model Example

I-UA2 Describe your approach to working and collaborating with the CalSAWS M&E Contractor to perform shared services, such as security, and supporting Application Evolution and Innovation.

## Approach to working and collaborating with the CalSAWS M&E Contractor to perform shared services

Kyndryl’s approach to collaborating with M&E vendors on shared services to CalSAWS is based on a DevOps set of practices and cultural philosophies that aims to bridge the gap between application development and IT operations teams. Our process promotes collaboration, communication, and shared responsibilities throughout the solution development lifecycle. In the context of the collaboration between application development and infrastructure operations teams, DevOps becomes the foundation of how work is done in a collaborative way.

The first step in establishing DevOps is to establish a collaborative culture between engineering and development teams. This is done by breaking down traditional silos between contractor teams and forming new teams with our M&E partner resources that are aligned to a business function or project deliverable. When teams are functionally organized feedback loops between development and operations develop which enables teams to respond to issues quickly, leading to faster resolutions and product improvements. The goal is when we ask a resource what team they are on they should reply with the functional team they support not CalSAWS contractor they represent.

The second step in establishing DevOps culture is automation of repetitive technical tasks. We advocate for the automation of repetitive tasks, such as building, testing, and deploying applications through Infrastructure as Code (IaC) and Continuous Integration and Continuous Deployment (CI/CD) pipelines.

By automating these processes, it reduces errors, accelerates development cycles, and ensures consistency between development and production environments. The real benefit of automation to a collaborative culture comes when M&E developers are given access to the infrastructure automation in lower environments. This not only exposes them to operations side of solution development expanding their perspective but also allows them to deploy changes into their own environments much quicker than when relying on M&O support in ticket based traditional models. The faster a developer can release a chance the more likely they are to try new solutions and innovate.

Kyndryl uses IaC to define and manage infrastructure through code in environments that we manage. This practice allows development and operations teams to collaborate on defining and maintaining infrastructure configurations, ensuring consistency, reducing human error, and reducing manual interventions.

To elevate our DevOps practice with our M&E partners we use CI/CD. With the principle of automated repetitive tasks, we promote the implementation of CI/CD pipelines for all deployable artifacts so that both the application and infrastructure code are built together. This enables frequent and reliable code releases while reducing the effort to make changes to an environment. Kyndryl’s DevOps approach also incorporates security practices throughout the development process, ensuring that security concerns are addressed proactively rather than as an afterthought and built directly into the IaC and CI/CD automation. This approach binds Infrastructure to Development teams and ensures that code changes are thoroughly tested and automatically deployed to production, reducing the risk of deployment failures.

By embracing DevOps practices, tools, and techniques Kyndryl and our M&E partners can work together seamlessly, delivering software faster, with higher quality, and with greater reliability.

## Approach to Security Services

Kyndryl follows a DevSecOps approach for Security coordination across teams. DevSecOps is short for Development, Security, and Operations, and is an approach to software development that integrates security practices throughout the entire development lifecycle. It emphasizes collaboration between development, security, and operations teams to ensure that security considerations are addressed starting from the very beginning of the development process.

In DevSecOps, security measures and testing are integrated into the continuous integration and continuous delivery (CI/CD) pipeline. This helps identify and address security vulnerabilities early in the development cycle, reducing the risk of security breaches and making the software more resilient. It involves automating security tests, code analysis, vulnerability assessments, and compliance checks as part of the development process.

By integrating security into the DevOps workflow, DevSecOps aims to create a culture where security is not seen as a hindrance but as an integral part of the development process. This approach ultimately leads to faster, more secure, and higher-quality software deployments.

Key Pillars of Kyndryl’s DevSecOps approach:

* Early Involvement from application development, infrastructure, and security teams right from the project's inception. This promotes a shared understanding of goals and requirements throughout development and operations.
* Cross-Functional Teams that include members from each area. This helps break down silos and encourages collaboration at every stage of development.
* Shared Goals to define common objectives for the teams, focusing on delivering secure and reliable software. Align everyone's efforts towards these shared goals.
* Establish Communication Channels such as regular meetings, video conferences, and shared documentation, to facilitate transparent information exchange.
* Designate Security Champions within each team to act as liaisons between the security team and the development/operations teams, helping translate security requirements and best practices.
* Ongoing Security Training security to all team members to raise awareness about security concerns, best practices, and emerging threats.
* Automate Security testing and tools into the CI/CD pipeline to automatically scan for vulnerabilities, code flaws, and misconfigurations early in the development cycle.
* Use collaborative tools that can be accessed by all teams to manage tasks, track issues, and share information. This ensures everyone is on the same page.
* Apply the "security as code" principle, treating security configurations and policies as code that's versioned, reviewed, and tested alongside application code.
* Establish a culture of continuous feedback where teams provide input on security-related matters. Encourage open discussions about challenges and potential solutions.
* Define security metrics to track and measure the effectiveness of security practices. Establish monitoring mechanisms to quickly identify and respond to security issues.
* Regularly assess the collaboration process and look for opportunities to improve it. Encourage feedback and implement changes as needed.

Successful collaboration between teams is not just about processes and tools; it's also about fostering a culture of trust, respect, and shared responsibility for delivering secure and reliable software.

## Approach to Supporting Application Evolution and Innovation

Kyndryl’s approach to supporting application development revolves around building a DevOps culture and automation that enables developers to rapidly deploy and redeploy changes which in turn allows for innovation. When developers are faced with burdensome delays in deploying their code it changes their behavior. They try to add more code into builds, they go with what they know will work vs. what might work, and they purposely limit their number of code deployments in each development cycle. Kyndryl recognizes this and works to continuously make the developers experience better, so they are more likely to explore and take risks which are the foundation of innovation.

What this looks like in practice:

* **Deployment Automation:** Kyndryl can implement continuous integration and continuous deployment (CI/CD) pipelines, to enable the application team to quickly and reliably deploy new features, reducing manual intervention and accelerating the innovation process.
* **Scalability:** Kyndryl can collaborate with the M&E teams to design systems that can scale with the application's growing demands, ensuring that the application team can innovate without worrying about performance limitations down the road.
* **Monitoring and Alerting:** Kyndryl can set up monitoring tools and alerting systems that help the application development team identify and address any issues promptly, ensuring smooth functioning of the application and supporting a seamless innovation process.
* **Testing Environments:** Kyndryl can provide isolated AWS testing environments that mirror production conditions that allows the application team to experiment with new ideas and features without affecting the live application.
* **Performance Optimization:** Kyndryl can collaborate with the application teams to optimize system performance ensuring that the application team's innovative features run efficiently and meet user expectations.
* **Troubleshooting Support:** In case of issues, Kyndryl can assist the application team in diagnosing and resolving problems quickly, minimizing downtime and maintaining a smooth innovation process.

I-UA3 Identify major risks inherent in the Integrated Multi-Contractor Environment and your proposed mitigation strategies.

## Major Risks and Proposed Mitigation Strategies

Many of the standard risks we see in multi-contractor approaches CalSAWS has already taken steps to mitigate by establishing a Delivery Integration Office for example. Our approach will be to reinforce those mitigation strategies and support CalSAWS process with our active participation and thought leadership.

Table 2. Risks and Mitigation Strategies

| **Description** | **Risk** | **Mitigation** |
| --- | --- | --- |
| **Coordination Challenges** | Lack of synchronization among contractors leads to inefficiencies and delays. | Establish a centralized project management office (PMO) to coordinate efforts, define clear roles and responsibilities, and implement regular progress meetings. (We believe this is being accomplished with the Delivery Integration Office today.) |
| **Communication Gaps** | Inadequate communication between contractors leading to misunderstandings and misaligned objectives. | Use collaborative tools and platforms to facilitate communication, encourage regular status updates, and promote open communication channels. |
| **Inconsistent Standards** | Contractors may have varying quality, security, and performance standards, resulting in discrepancies in the delivered product or service. | Clearly define and document quality standards and expectations in each project charter and conduct regular quality audits to enforce consistent testable procedures. |
| **Security Vulnerabilities** | Contractors' differing security practices may expose the project to vulnerabilities and potential breaches. | Establish stringent security requirements defined by policy, conduct security assessments across contractors work and implement standardized security protocols across the project. Regularly test security posture and evaluate process enhancements from lessons learned. |
| **Accountability and Responsibility Tracking** | Difficulty in attributing issues to specific contractors, leading to finger-pointing and delays in issue resolution. | Clearly outline accountability and responsibility in RACI agreements between teams and maintain a centralized issue tracking system to establish a dispute resolution mechanism. (We believe this is being accomplished with the Delivery Integration Office process today.) |
| **Scope Creep and Budget Overruns** | Contractors may introduce changes that lead to scope creep and exceed the allocated budget. | Implement change management processes, require formal approval for scope changes, and regularly review project finances to prevent overruns. (We believe this is being accomplished with the Delivery Integration Office process today.) |

These mitigation strategies can help address the risks inherent in a multi-contractor IT environment and enhance the overall success of the project.