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  
System Performance**

August 29, 2023

Table of Contents

[I-UA4 Describe your approach to proactively monitoring and managing SLAs to ensure performance requirements and appropriate security measures are met. 1](#_Toc144142356)

[5.2.3.2.1 Proactively monitoring and managing SLAs for Performance 2](#_Toc144142357)

[5.2.3.2.1.1 CalSAWS AWS Environment 2](#_Toc144142358)

[5.2.3.2.1.2 AWS Native Services Tools: 2](#_Toc144142359)

[5.2.3.2.1.3 CalSAWS Physical Network 3](#_Toc144142360)

[5.2.3.2.1.4 CalSAWS User Devices 4](#_Toc144142361)

[5.2.3.2.1.5 Kyndryl Bridge 4](#_Toc144142362)

[5.2.3.2.2 Proactively monitoring and managing SLAs to ensure appropriate security measures are met. 9](#_Toc144142363)

[5.2.3.2.2.1 Managed Security Information Event Management 11](#_Toc144142364)

[5.2.3.2.2.2 Kyndryl’s Endpoint Detection and Response (EDR) Services 11](#_Toc144142365)

[5.2.3.2.2.3 Kyndryl Vulnerability Management Service 12](#_Toc144142366)

[5.2.3.2.2.4 Cloud Security Posture Management 12](#_Toc144142367)

[I-UA5 Describe your approach to proactively assessing CalSAWS system performance, and how you will optimize and continually improve system performance. 13](#_Toc144142368)

[Based on your experience, describe how your past system performance and SLA management processes delivered improved system performance and measures and the extent to which you met or exceeded stated SLAs. 13](#_Toc144142369)

[5.2.3.2.3 Approach to proactively assessing CalSAWS system performance and continually improve system performance. 13](#_Toc144142370)

[5.2.3.2.3.1 Kyndryl’s Service Components 16](#_Toc144142371)

[5.2.3.2.4 How we will optimize and continually improve system performance 19](#_Toc144142372)

[5.2.3.2.5 How our past system performance and SLA management processes delivered improved system performance and the extent to which we met or exceeded stated SLAs. 20](#_Toc144142373)

[I-UA6 Identify major risks inherent in multi-contractor system performance requirements and your proposed mitigation strategies. 21](#_Toc144142374)

[5.2.3.2.6 Major Risks and Proposed Mitigation Strategies 22](#_Toc144142375)

Table of Figures

[Figure 1: Overview of CalSAWS and Kyndryl Tools 6](#_Toc144127803)

[Figure 2: Environment Example 8](#_Toc144127804)

[Figure 3: SOC Team 10](#_Toc144127805)

[Figure 4: Integrated AIOps Dashboard 15](#_Toc144127806)

[Figure 5: Case Study - California based national not-for-profit integrated healthcare and delivery network 21](#_Toc144127807)

Table of Tables

[Table 1. Major Risks and Proposed Mitigation Strategies 22](#_Toc143935917)

5.2.3.2 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

I-UA4 Describe your approach to proactively monitoring and managing SLAs to ensure performance requirements and appropriate security measures are met.

Proactively monitoring and managing SLAs (Service Level Agreements) and ensuring performance requirements and security measures are met is the top priority for Kyndryl.

Kyndryl’s Performance Management methodology assesses the health, efficiency, and effectiveness of overall IT operations. It tracks the various metrics including system performance, ticket analysis, SLA compliance, and identifies any opportunities for improvement. The focus is on identifying incident and problem trends, system performance, and user satisfaction.

Tools and services we use may vary from your AWS environment, physical network, call center, and device management but the underlying methodology is consistent.

Kyndryl’s Approach:

* Define clear SLAs
* Establish monitoring tools
* Set metric based alarms
* Implement centralized logging and auditing
* Implement security measures based on best practices
* Continuous testing and simulation
* Automated remediation
* Regular review and continuous incremental improvements
* Incident response plans (for when SLAs are breached, or security incidents occur)
* Regular communication with partners and stakeholders
* Design for scalability

By following this approach, we establish a proactive and systematic approach to monitoring and managing SLAs, performance, and security in your AWS environment, helping to ensure smooth operations, high availability, and data protection.

## Proactively monitoring and managing SLAs for Performance

We begin by establishing clear and well-defined SLAs in collaboration with M&E Partners and the CalSAWS Consortium stakeholders which can be measured and enforced systematically through tooling and reports. These SLAs outline response times, uptime targets, and performance metrics to create a common understanding of expectations. These are well documented and maintained in our standard operating procedures and service contracts.

### 5.2.3.2.1.1 CalSAWS AWS Environment

To effectively monitor these established SLAs, Kyndryl leverages many tools and techniques including AWS native services, 3rd party tools, and Kyndryl’s proprietary monitoring system we call Bridge. Collecting and tracking key performance indicators (KPIs) across the CalSAWS environment is built into all project and operational work we perform.

During the transition period we will review the existing monitoring and services established to ensure necessary operational services and functionality are in place. If anything requires immediate attention, we will work with the incumbent providers to resolve any potential gaps immediately. Our goal is to not to impact existing processes and tools that teams have grown accustomed too so we will maintain established tools and behaviors but after our transition in period we will further enhance CalSAWS posture by establishing additional tools, configuration, and monitoring that meet our high bar for operational excellence we have established across our 4,000+ managed services clients around the world.

### 5.2.3.2.1.2 AWS Native Services Tools:

Amazon provides many services which allow us to create custom metrics to measure specific aspects of your environment and set up automated alarms that trigger notifications and automated actions when predefined thresholds are crossed. These alerts and monitors will act as proactive warnings, enabling our teams to swiftly address issues and prevent SLA violations. Kyndryl will continuously develop and adjust these alarms and corresponding automation trigger iteratively improve the performance management posture of the CalSAWS ecosystem.

To define optimal performance, we will establish performance baselines for each business function or service consumed by CalSAWS and our M&E partners. Automation regularly compares real-time metrics against these baselines to detect deviations and potential problems early. This baselining approach helps identify and define anomalies and deviations, allowing for timely intervention before any impact to SLAs.

Next, we work to build intelligent auto healing mechanisms into operations. For example, by implementing auto-scaling on AWS infrastructure that is triggered by Amazon Cloud Watch alerts we can often prevent issues from occurring before any SLA are at risk. In addition to auto-scaling we build simple, but powerful Lambda functions that perform tasks an operational engineer normally would. This allows us to automate performance management tasks, schedule activities, and remove human error. Activities like ensuring a data file is made available to a system at a certain time every day or revoking a user’s permission instantly when off boarded are some examples of tasks we have recently automated in AWS for other clients.

It is easily said but the key to achieving this posture is a close partnership with the M&E partners to ensure they understand how to architect their applications to support these infrastructure functions. Kyndryl has successfully helped clients with both modern and legacy workloads achieve this performance posture and do not believe every application has to be containerized to have modern operational scaling and performance functionality. Our goal is to iteratively build an intelligent system that can selfheal by adjusting resource allocation dynamically based on demand to ensure consistent performance during sudden spikes in traffic and lower operating costs during slower periods of performance.

### 5.2.3.2.1.3 CalSAWS Physical Network

We start by reviewing existing monitoring tools in place today to monitor network devices, bandwidth utilization, and connectivity. We will recommend enhancements to the current posture during transition in and set up alerts for critical events agreed upon between CalSAWS and our M&E partners as we assume ownership of operations.

On the Network Security front, we will review and implement any required changes to secure the environment from a firewall, intrusion detection systems (IDS), and intrusion prevention systems (IPS) perspective to safeguard the network against unauthorized access and cyber threats.

We conduct regular audits and vulnerability assessments to identify and address weak points in the physical network infrastructure. We focus on patch and update management to ensure network devices (routers, switches, firewalls) are regularly patched and updated to mitigate vulnerabilities. If there is not a robust resilient solution in place today this will be a focus of conversation with CalSAWS during and post transition in period. Finally, regarding redundancy and failover we will work with CalSAWS to ensure redundant network paths and failover mechanisms and hardware are in place and tested regularly to ensure network availability in case of hardware failures or localized disasters to the physical infrastructure.

### 5.2.3.2.1.4 CalSAWS User Devices

CalSAWS User devices follow a similar methodology for SLA adherence but with different focal points. We again start with a review and audit of existing key focal areas to understand posture against SLA’s and areas for improvement.

Device Focal Points for SLA Management

* End Point Security
* Monitoring and Management Tooling
* Data Backup functionality
* Device support and replacement
* End User Training
* Patch Management
* Access Controls
* Encryption

We ensure endpoint security software has been deployed to all user laptops for real-time malware detection, data encryption, and intrusion prevention. We also review and audit which Remote Monitoring and Management tools are in place. These tools are critical for our operational support and to monitor user laptops, install software updates, and enable troubleshooting of issues remotely. To ensure data backup and recovery functionality we review data backup solutions implemented to understand how data is regularly backed up and how it can quickly it can be restored in case of data loss or hardware failure. User Training also helps drive better performance management by informing users about security best practices, such as avoiding suspicious links and using strong passwords, to minimize and avoid security risks which can drive SLA breaches.

### 5.2.3.2.1.5 Kyndryl Bridge

Kyndryl Bridge is an open integration platform that has been built based on Kyndryl’s decades of experience and lessons learned managing critical infrastructure and operations for clients. It provides enterprise visibility across AWS, commercial products, and custom-built solutions to enable actionable insights at the ecosystem level comprising all the topics above. This helps operational and development teams understand, predict, and act to maintain SLA and drive better business outcomes.

By centralizing all performance monitoring metrics from and operational services into one place with custom reports and dashboards Bridge allows for new insights not possible at the individual service level. AWS Cloud Watch may tell you system performance regularly degrades at a certain time each week; Bridge can help you understand why.

At the heart of Bridge is a set of continuously growing anomaly detection mechanisms and logic that leverage machine learning to identify unusual patterns or behaviors in your IT ecosystem. Bridge analyzes historical data to identify trends and patterns that guide improvements and enable insights. Kyndryl centralizes our lessons learned across clients into Bridge’s machine learning library so that CalSAWS gets benefits of our M&O experience across a wide range of customer environments.

An example of one of the tools that form our Kyndryl Bridge is the Tivoli NetCool/OMNIbus product which performs the following functions:

* Centralized Service Level Agreement management to deliver real-time monitoring of complex networks and IT domains in a single location.
* SLA information presentation to the Kyndryl service desk team.
* Trigger for automated responses to operational events.
* Consolidation point for information from other network management tools.
* Intelligent processing and management of SLA alerts for operations teams.

Graphical user interface

Description automatically generated

Figure 1: Overview of CalSAWS and Kyndryl Tools

Documenting monitor configurations, incident resolutions, and SLA performance is the foundation of our SLA management approach. Regularly analyzing SLA breaches or near-miss incidents to identify root causes and patterns drives continuous improvement. Using these insights, we work with CalSAWS and our M&E partners to refine SLA management approach, ensuring your IT environment on AWS evolves to consistently meet or exceed SLA expectations. Generating periodic reports to keep stakeholders, developers, and operators informed about the health of the IT environment and SLA compliance helps foster a culture of continuous improvement. Several different scenarios are described below for Kyndryl our M&E Partners to collaborate on and execute the optimal service delivery for the CalSAWS which lays the foundation for SLA and Performance management through automation and machine learning.

The figure below depicts an overall example.

**A picture containing timeline

Description automatically generated**

Figure 2: Environment Example

1. M&E or Kyndryl users invoke the provisioning of resources using either code pipelines or IAC approaches such as Terraform or CloudFormation.
2. AWS Services are provisioned with resource tags. Tags used by Kyndryl are documented and defined but M&E partners can also apply tags specific to their use cases.
3. AWS Config service is used to deploy services with agreed upon harden configuration to ensure each deployment meets security and operational requirements.
4. Play books defined within AWS Systems Manager automate common and repetitive deployment across CalSAWS accounts consistently.
5. During the deployment process, AWS CloudWatch monitors are automatically created to monitor all services deployed as part of the System Manager playbook.
6. AWS CloudWatch alerts trigger notification and automation (like auto scaling or lambda functions) based on AWS Service performance.
7. Cloud Watch alarms trigger Incidents in AWS Systems Manager Incident Manager.
8. AWS ServiceNow connector passes these Incidents to CalSAWS’ ServiceNow instance for consolation.
9. AWS Config service passes details of deployed resources to ServiceNow CMDB.
10. The AWS ServiceNow connector also synchronizes other elements like AWS Service Catalog to ServiceNow Service Catalog on a regular schedule.
11. Kyndryl implements multiple cloud-native security solutions like AWS Security Hub, Guard Duty, Inspector, and Audit Manager to manage the security and compliance posture of resources within a customer AWS account.
12. Kyndryl manages backups and patching of resources within a customer AWS account.

## Proactively monitoring and managing SLAs to ensure appropriate security measures are met.

Kyndryl’s cyber security solution for CalSAWS provides both physical and logical controls to protect all assets and systems based on Kyndryl’s established comprehensive security and compliance program which is tailored to meet CalSAWS specific requirements. Our standards and processes will reflect CalSAWS security requirements, which include, but are not limited to procedures for security monitoring, end point protection and vulnerability management. Kyndryl will develop, implement, and maintain a comprehensive System Security Plan (SSP) that guides security efforts throughout the organization.

Kyndryl will deliver advanced threat detection and vulnerability management as part of our solution. Kyndryl approach includes establishing a Security Operations Center (SOC) to provide 24x7x365 monitoring and a response team for any alerts or incidents. Our team continuously identifies risks and vulnerabilities as well as any irregular behavior of users. They quickly respond and remediate Security Incidents and Events and ensure compliance of impacted systems through remediation efforts.

Kyndryl will provide a physical Command Center to host the nearshore SOC team. The goal of the Command Center is to break down tower silos and create a unified, multi-disciplinary team with a consolidated “single pane of glass” view of security operations. Our solution physically locates the nearshore teams all in the same room with monitors displaying key metrics to establish a control room which maintains security posture and is available to quickly respond to incidents.

Diagram

Description automatically generated with medium confidence

Figure 3: SOC Team

The Kyndryl SOC team will be made up of security specialists with the skillsets to manage and administer the security tech-stack to maintain the health and currency of supporting systems. Kyndryl SOC team will also provide support functions to the on-going maintenance and operations teams, this includes the following general support activities:

* Application Support
* Monitoring (Health Checks, Capacity, etc.)
* Application Administration (L2 activities, User administration, Configuration, Log source updates, etc.)
* Updates and upgrades
* End User Support (ticket assignment from service desk)
* Platform Support
* Agent updates
* Troubleshooting performance
* System/Platform down
* Security Advisory Support
* Inform, Evaluate, Assess, Plan and Act on security alerts
* Security Policy and Controls

### 5.2.3.2.2.1 Managed Security Information Event Management

Kyndryl’s Security Information Event Management (SIEM) methodology brings CalSAWS a holistic management of their security logs. We support implementing various SIEM systems for the CalSAWS selected vendors and solutions of choice. Managed SIEM is designed to help plan, implement, manage, and monitor a based on CalSAWS identified business requirements.

Our services also include best practices to implement log enrichment which simplifies management of increasingly complex architectures encompassing more and more remote endpoints using a mix of operating systems and deployment.

### 5.2.3.2.2.2 Kyndryl’s Endpoint Detection and Response (EDR) Services

* A team of senior security professionals identify, investigate, prevent, and stop the most sophisticated and advanced cyberattacks.
* Protects endpoints by detecting malware, including ransomware variants, zero-days, non-malware, and file-less attacks by leveraging the tool of choice and by configuring and managing it in accordance with industry best practices and CalSAWS business needs.
* Continuous review and tuning of Policy design in accordance with best practices and CalSAWS requirements.
* System and Agent health status tracking and management
* 24/7 monitoring, incident alerting, investigation, and remediation services

Managed Endpoint Protection Services protect CalSAWS servers, workstations, and mobile devices by implementing endpoint security features.

* Anti-virus (Workstations, Servers & Network Attached Storage)
* Host Intrusion Protection (HIPS) (Workstations and Servers) (Networking/NOC interlock)
* Console technology upgrades co-ordination as applicable
* Signature file updates available for download, as applicable
* Health and availability of management console

### 5.2.3.2.2.3 Kyndryl Vulnerability Management Service

* End-to-end vulnerability management lifecycle
* Risk based approach to detect vulnerabilities and orchestrate their remediation
* Remediation of critical assets and actively exploitable threats
* Custom made reports & dashboard
* Discovery Scans/External Scans/Internal Scans (Authenticated/Non-authenticated scans) and Compliance Scans
* Recommendations based on vulnerability assessment reports
* Periodic review of processes and policy requirements
* Security Baseline configuration scanning
* False Positive analysis
* Active exploitation intelligence
* Critical Vulnerabilities Vs Assets
* Trigger requests for remediation on service management tool
* Track remediation progress
* Document exception management

### 5.2.3.2.2.4 Cloud Security Posture Management

Kyndryl’s Cloud Security Posture Management (CSPM) service is designed to identify and manage misconfiguration and compliance issues in Public Cloud environments. Our CSPM services enable organizations to leverage the benefits of Public Cloud native services, activating continuous posture assessment, non-compliance identification and classification, non-compliant workloads and services management and remediation according to industry best practices and standards. Kyndryl’s CSPM delivery team is tightly integrated with CalSAWS M&E Contractor team with incident, alert, investigation, and response services.

Key Capabilities:

* Cloud Native Security Policy development based on Industry and Regulatory Standards
* Services architecture design, activation, and configuration
* Kyndryl Public Cloud Continuous Compliance framework implementation
* Public Cloud Risk and Compliance Reporting
* Deviations remediation guidance

Kyndryl’s CSPM Managed Service includes:

* Console Management
* Continuous Policy review and tuning in accordance with Industry standard changes and cloud technology evolution
* Remediation guidance with detailed ticketing, required actions and management system to track noncompliance issues
* Continuous fine tuning and suppression
* Continuous fine tuning and suppression
* Monthly compliance reporting and audit support
* Users and privilege monitoring
* Threat detection
* Upgrade and patch co-ordination
* Policy configuration

I-UA5 Describe your approach to proactively assessing CalSAWS system performance, and how you will optimize and continually improve system performance.

Based on your experience, describe how your past system performance and SLA management processes delivered improved system performance and measures and the extent to which you met or exceeded stated SLAs.

## Approach to proactively assessing CalSAWS system performance and continually improve system performance.

Our approach to monitoring and managing system performance is designed to meet several key objectives:

* **Minimizing business disruption:** From our experience across hundreds of transitions globally, Kyndryl has developed an approach that includes steps to establish management, planning, and control processes that transition from the existing vendor while minimizing business disruption and maintaining operational continuity.
* **Infrastructure optimization:** We will deliver continuous improvements to the services through cloud tools automation, cloud operation optimization, service request automation, infrastructure software, hardware consolidation, and year-on-year productivity.
* **Consistent experience:** Drive quality, agility, and delivery consistency across infrastructure services full lifecycle in the support center by implementing Kyndryl delivery framework.
* **Accountability for outcomes:** Take accountability for Infrastructure service support and maintenance across the Consortium AWS Cloud, hardware, and software.
* **Innovation:** We will bring Infrastructure insights, best practices, and innovations that will allow CalSAWS to best utilize its assets to meet changing customer requirements.

The key to optimizing and improving system performance is access to timely and accurate data about the assets in the managed environment, the connections and relationships among the assets, and the ability to glean useful insight from, and execute actions based on, this data.

Kyndryl M&O services includes:

* Perform AWS services and monitoring
* Monitor 24x7 and auto generate support tickets in Service Now
* Validate and update KPI
* Perform operation management of environments
* Perform component service change and incident management
* Perform health check and compliance management
* Perform regular patching and maintenance
* Perform backup and restore of system data
* Continuous capacity monitoring
* Continuous cost management and cost optimization

At the core of our system performance management approach is Kyndryl’s Integrated AIOps service which is a component of Kyndryl Bridge platform. AIOps combines data gathering and analytics with a delivery model designed to facilitate the highest levels of automation and defect prevention. Integrated AIOps will become the foundational support of a predictive proactive responsive model.

Kyndryl will start by enhancing and augmenting existing monitoring tools to collect additional relevant and correlated data, which will allow us to bring proactive, actionable insights and automation opportunities while leveraging DevOps and Site Reliability Engineering.

Next, we will use robust data insights and correlation techniques to examine and cross-reference data from a variety of sources (for example, hardware and software currency, configuration, performance, capacity, and availability) and begin watching for anomalies and deviations from the target operating baseline and correlating those for proactive digital root cause determination.

We will proactively monitor the environment and manage and configure alerts. This will allow us to use dashboards and actionable insights to provide proactive support before an incident occurs. Monitoring will be enterprise-wide and will include all infrastructure and network, as well as user device monitoring. Site Reliability Engineers will use trending and analysis to prevent outages and performance/capacity issues before they occur. They will have the tools and data to build a highly automated, self-healing ecosystem. The additional actionable insights will feed incremental automation.

Integrated AIOps will also support rapid response and incident resolution. Robust monitoring with correlated data provides additional insights into problem determination of issues and root causes. This will improve the meantime to resolve along with automation.

Integrated AIOps combines data with visualizations (dashboards, data science tools) and collaboration technologies to reduce friction between insights and actions. The result is both proactive and responsive and will improve the performance and availability of CalSAWS systems, which will result in a better user experience.

The Integrated AIOps Dashboard takes a totally different approach than other operational dashboards. It does not exhibit the typical IT landscape, like 95% patch compliance and/or 80% health check compliance, but instead focuses on those areas where actions need to be taken to address an area of concern or improvement.

Text

Description automatically generated

Figure 4: Integrated AIOps Dashboard

The dashboard is divided into three key areas, which represent different perspectives of the environment:

1. The Alerts section on the left top provides observability of what is actively occurring. It shows ticketed events sorted by severity and mapped to business applications impacted. Other observability information coming from solutions like Dynatrace are also displayed here. This gives the view of which business application is impacted, how many CI s are involved as well and when the issue first occurred. As such, it is a near real-time view of what is currently happening within the CalSAWS environment.

2. The Actionable Insights section on the bottom left is where it gets interesting. This shows actionable insights. It uses patterns and AI/machine learning models across all available data to define areas of concern and areas of improvement with a link to the next best action to take to start resolving it. These actionable insights can be seen as answers to questions derived from the underlying data. The system learns from similar occurrences from other customer environments and leverages these learnings to recommend insights when encountering similar observations in CalSAWS environment. In essence each root cause analysis should result in an actionable insight with the next best action defined. An example of an actionable insight determination is described below. Each actionable insight is an answer to a question asked to the underlying data.

Each actionable insight comes with 4 key areas of information.

Top 10 objects which are impacted and benefit from the actions provided.

Recommended actions taken to address the area of concern or area of improvement.

Derive observations from the data. Identify the devices that are impacted based upon the observations.

Graphs of utilization information vs. memory consumption. (It has the capability to show alternative insights using incident information instead.)

3. IT Health Indicators on the top right of the landing page operate like the dashboard light in your car. Because you know when the engine light comes on something requires attention and action is to be taken. When an indicator is gray, it means that it is within normal range and does not require attention, however you can still drill down into the details.

### 5.2.3.2.3.1 Kyndryl’s Service Components

Successfully managing service performance requires the orchestration of many service components, which span architecture, engineering, operations, administration, asset management, and not least, service desk management. Kyndryl’s service component include:

#### 5.2.3.2.3.1.1 Call Management

The Kyndryl Service Desk will provide a call management service to answer and respond to support calls regarding the infrastructure services in scope of the service. The service Desk will be the single point of contact for the CalSAWS. A Services Coordinator will be assigned incident to resolver group for incident resolution.

#### 5.2.3.2.3.1.2 Service Request Management

Kyndryl will support a service request process. Requests for services received via the CalSAWS Service Desk will be routed to the respective resolver group. An agreed set of services will be defined as Service Requests within the catalog, examples including:

* Project services
* Report maintenance
* Report batch status query
* User assistance
* Provision a cloud infrastructure component
* Execute and ad-hoc backup or restore
* Modify a backup plan
* Customize a virtual machine image
* Information for audit request
* Generate custom reports

#### 5.2.3.2.3.3 Incident Management

CalSAWS-aligned incident management process will be followed, and all incidents will be recorded in CalSAWS’ ServiceNow, which will be used to log, track, analyze, resolve, and report incidents. The scope of the service includes:

* Mobilization and facilitation of resolver groups (Kyndryl, CalSAWS and third parties) in the event of major incidents / high impact severity 1s.
* Progress checks and reporting appropriate to the severity of the incident.
* Escalation management of incidents to 2nd and 3rd level support, including 3rd parties.
* Production of incident summary reports in preparation for status meetings.
* Referring to issues from third parties.

#### 5.2.3.2.3.4 Problem Management

The problem management service will be integrated with the incident management process. Problems will be raised in accordance with the service agreement and will be recorded in the service management tool. The scope of the service includes:

* Problem determination and source identification for incidents that affected business services.
* Identification and implementation of remedial action to resolve the root cause of incidents.
* The coordination of resolution or workaround activities with third party service providers.
* Root cause analysis of infrastructure problems
* Identification, development, testing and implementation of infrastructure fixes, including maintenance of solution documentation
* Management and reporting of problem fix activity.

#### 5.2.3.2.3.5 Change Management

Changes to the Infrastructure will be governed by an CalSAWS-aligned change management process. Changes will be raised, assessed, and implemented according to agreed policies and will be reviewed by a Change Advisory Board. Changes will be administered via the Change Control tool, which will refer to a forward schedule of change.

Changes will be categorized into various types (emergency, standard) and will be pre-assigned with associated levels of approval accordingly. Maintenance windows will be predetermined and built into the forward schedule of change.

Environment demand and provisioning will collate and maintain information on production and non-production environment demand and will use this information to provide resource utilization forecasts as input into Capacity Management.

Hardware and cloud resource demand data will be maintained centrally and will provide a basis for modelling resource usage and providing forecasting reports for management purposes, for example as an input to budget preparation.

#### 5.2.3.2.3.6 Capacity Management

Capacity management will focus on monitoring cloud instance and server system performance and capacity to ensure that the infrastructure meets current and future business needs. The Kyndryl service operations team will extract data using the cloud and datacenter management tool set. The system capacity and performance metrics will be produced and documented in preparation for presentation during the service reviews. Infrastructure capacity metrics collected will include CPU usage, memory usage, disk space utilization.

M&E provider will review Application Performance Management and Services business demand (user usage).

Demand and Provisioning Management – Environment demand and provisioning will collate and maintain information on production and non-production environment demand and will use this information to provide resource utilization forecasts as input into Capacity Management

Hardware and cloud resource demand data will be maintained centrally and will provide a basis for modelling resource usage and providing forecasting reports for management purposes, for example, as input to budget preparation.

#### 5.2.3.2.3.7 Configuration Management

* Update CI/CD pipeline and a GitOps pull-based workflow model, to deploy configuration definition files to cloud infrastructure resources.
* Create and record configuration change requests.
* Validate configuration change records for completeness and accuracy.
* Implement the configuration change.
* Perform post implementation review and update the configuration change status
* Documentation Management
* Maintain and update the Infrastructure Services Operational Working Documents (OWDs) for the activities and processes as per infrastructure scope
* Perform gap analysis, working in conjunction with the Consortium, identify changes (additions and deletions) and enhancements to the documents
* Submit changes and improvements to the documents through Deliverable Expectation Documents (DEDs)

## How we will optimize and continually improve system performance

Innovation and Continuous Improvement are key aspects associated with assuring the future viability of and extending the overall system life. Kyndryl will apply a structured approach for continually improving the infrastructure and supporting processes through innovative technologies and methods aligned with CalSAWS integration delivery office processes.

We view Kyndryl’s operating model initiative as an ongoing journey of continual improvement.

1. Regular Monitoring and Analysis: Continuous monitoring of the system's components and performance metrics to identify bottlenecks, anomalies, and trends that might affect performance.
2. Scalability Planning: Designing the system alongside our M&E partners with scalability in mind, allowing it to handle increased workloads as the user base grows. This might involve using cloud resources, load balancing, and efficient database structures.
3. Optimized Code and Infrastructure: Continuously improving code to be efficient and simple to minimize resource usage, and ensure the infrastructure is properly configured and optimized for the specific workload and requirements.
4. Performance Testing: Conduct regular performance and security testing to simulate different levels of user activity and stress-test the system to identify its limits and potential failure points.
5. Response Time Optimization: Focus on reducing the system's response time to user requests. This involves optimizing database queries, minimizing network latency, and employing caching mechanisms to deliver faster and more efficient responses to users.

Kyndryl is focused on providing a cloud native framework that is aligned to AWS Well Architected Framework and best practices for Modernization of Application Infrastructure. Kyndryl’s approach is composable and will help CalSAWS transform and align their cloud deployments and operations to a cloud native framework.

## How our past system performance and SLA management processes delivered improved system performance and the extent to which we met or exceeded stated SLAs.

Case Study:

Kyndryl assumed M&O responsibility of IT infrastructure for a California based national not-for-profit integrated healthcare and delivery network. Client required assistance stabilizing their IT ecosystem supporting a 39-hospital systemwhose IT real estate environment contained 57K servers and 32PB storage.

We started out as an IT managed services partner with a focus on services availability, solution quality, and continual improvement of operations but we have grown into their primary partner for IT innovation and modernization of their systems.

Scope of Kyndryl services include SLA management in the following areas:

* Security and compliance
* Disaster recovery and cyber resiliency
* Data center operations
* Private cloud services
* Compute and storage services
* Modernization and new ways of working
* Applications – Citrix and middleware
* Critical environments – EPIC, Cerner, Pharmacy
* Service management and quality
* Cost optimization

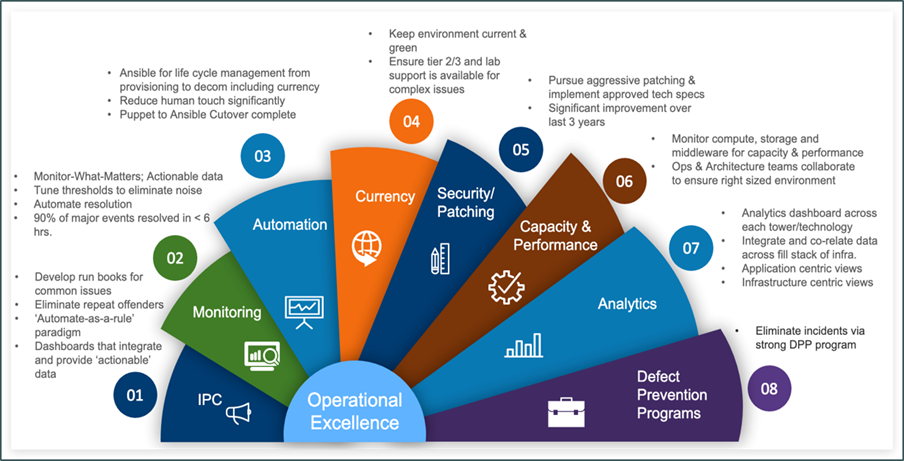


Figure 5: Case Study - California based national not-for-profit integrated healthcare and delivery network

Measurable Client SLA and Performance Outcomes:

* Between 2015 and 2021 when measurements where last refreshed it was demonstrated that M&O incidents decreased by 96%
* Client was able to move to an OPEX model based on consumption of Kyndryl provided infrastructure vs. their traditional CAPX investment model of all physical infrastructure reducing operating costs.

I-UA6 Identify major risks inherent in multi-contractor system performance requirements and your proposed mitigation strategies.

## Major Risks and Proposed Mitigation Strategies

Table 1. Major Risks and Proposed Mitigation Strategies

| Potential Risk | Proposed Risk Mitigation Plan |
| --- | --- |
| Poor service performance and missed Service Level Agreements (SLAs) | Immediately establish a quality assurance/quality control process by confirming that all devices are monitored.  Work to make certain that incidents are tracked and closed as rapidly as possible.  Multiple incidents based on the same issue become a problem that requires root cause analysis to be documented within the existing knowledge management system for common reference.  For major outages, open an immediate bridge managed by a “problem manager;” stakeholders, vendors, and technicians on the bridge will prioritize restoration of service.  Continually monitor and manage performance.  Skills continuous development for the staff assigned to keep supporting CalSAWS network with high level performance and quality.  Review root cause analysis reports and service performance parameters on a regular basis and provide recommendations for continual improvement |
| Attrition of key CalSAWS employees and incumbent resources required to support knowledge transfer | Identify key resource pool and name critical SMEs upfront to develop appropriate retention plans and prepare for availability of Kyndryl skilled resources as contingency to fill gaps.  Communicate and set correct expectations early and reinforce them honestly and in a timely manner.  Hire and re-hire key skills and resources in critical areas if needed.  Empower and motivate staff to provide critical requirements and information.  Develop detailed desk documentation for processes as early as possible in the event new employees are hired and require training. |
| Environment not fully documented | Identify gaps with knowledge transfer; we will add tasks to project plans and quality checkpoints to verify complete documentation during the agreed transition periods.  Kyndryl’s analytics capabilities will be implemented to assist in knowledge transfer.  Record Knowledge transfer sessions to create a training repository. |
| Communications | Communicate and set correct expectations early and reinforce them honestly and in a timely manner.  Develop trust between CalSAWS stakeholders, colleagues, and our M&E partners. |