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 Hardware and Software Management**

August 29, 2023

Table of Contents

[I-UA7 Describe your approach for providing CalSAWS Software maintenance services, including CalSAWS Software upgrades and patches, and ensuring appropriate security measures are continually addressed. 1](#_Toc144149486)

[Describe how Infrastructure staff will be allocated and/or shared to support Hardware/Software Maintenance as well as with Operations and Innovation Support. 1](#_Toc144149487)

[5.2.3.3.1 Software maintenance services 1](#_Toc144149488)

[5.2.3.3.1.1 Corrective Maintenance 1](#_Toc144149489)

[5.2.3.3.1.2 Preventative Maintenance 2](#_Toc144149490)

[5.2.3.3.1.3 Perfective Maintenance 2](#_Toc144149491)

[5.2.3.3.1.4 Adaptive Maintenance 3](#_Toc144149492)

[5.2.3.3.2 Software upgrades and patches 3](#_Toc144149493)

[5.2.3.3.3 Security Measures 3](#_Toc144149494)

[5.2.3.3.3.1 Security Patch Management 4](#_Toc144149495)

[5.2.3.3.3.2 Customer Security Document 4](#_Toc144149496)

[5.2.3.3.4 Infrastructure staff allocation approach to support Hardware/Software Maintenance and Operations 6](#_Toc144149497)

[5.2.3.3.4.1 User Experience 7](#_Toc144149498)

[5.2.3.3.4.2 Geographic Coverage Model 7](#_Toc144149499)

[5.2.3.3.5 Innovation Support 10](#_Toc144149500)

[I-UA8 Describe your approach for providing central and remote CalSAWS Hardware maintenance services for the Project Offices and CalSAWS Managed Hardware located in the Counties. 11](#_Toc144149501)

[Describe your depot location(s), where and how equipment will be staged for deployment, and which staff will be deployed, along with the manner of deployment, to support Central Project Office support and remote County support. 11](#_Toc144149502)

[Describe your approach for technology refresh efforts and incident/issue support. 12](#_Toc144149503)

[5.2.3.3.6 Approach to providing central and remote CalSAWS Hardware maintenance services for the Project Office and Counties 12](#_Toc144149504)

[5.2.3.3.7 Depot locations, staging and deployment 12](#_Toc144149505)

[5.2.3.3.8 Technology Refresh Approach 13](#_Toc144149506)

[5.2.3.3.12.2 Refresh Process 13](#_Toc144149507)

[5.2.3.3.12.1 Refresh Schedule 14](#_Toc144149508)

[5.2.3.3.9 Incident/Issue Support 14](#_Toc144149509)

[I-UA9 Describe challenges and risks to providing CalSAWS Hardware and CalSAWS Software management for CalSAWS and how you will mitigate the risk. 15](#_Toc144149510)

[5.2.3.3.10 Challenges and risks to providing CalSAWS Hardware and CalSAWS Software management 15](#_Toc144149511)

Table of Figures

[Figure 1. Customer Security Document 6](#_Toc144197682)

[Figure 2. Regional Coverage Examples 8](#_Toc144197683)

[Figure 3. Dispatch Tracker 9](#_Toc144197684)

Table of Tables

[Table 1. Corrective Maintenance 1](#_Toc144149545)

[Table 2. Preventative Maintenance 2](#_Toc144149546)

[Table 3. Perfective Maintenance 2](#_Toc144149547)

[Table 4. Adaptive Maintenance 3](#_Toc144149548)

[Table 5. Equipment Refresh Schedule 14](#_Toc144149549)

[Table 6. Hardware and software management services risks and mitigation strategies 15](#_Toc144149550)

5.2.3.3 Infrastructure Understanding and Approach to Hardware and Software Management

Cross Reference: CalSAWS-MO-RFP-01-2022-Infrastructure-BAFO-1-Instructions-Final-071823.pdf, Page 3 and CalSAWS M&O RFP 01-2022 071823 Addendum 11 TC.docx Section 5.2.3.3, Page 120

I-UA7 Describe your approach for providing CalSAWS Software maintenance services, including CalSAWS Software upgrades and patches, and ensuring appropriate security measures are continually addressed.

Describe how Infrastructure staff will be allocated and/or shared to support Hardware/Software Maintenance as well as with Operations and Innovation Support.

## Software maintenance services

CalSAWS will benefit from our well-established software maintenance approach, which has been shaped over 30 years of valuable client collaborations. This extensive experience has allowed us to refine and perfect templates that support our methodologies, guaranteeing the optimal operation, security, and adaptability of software systems. Our suite of maintenance methods—Corrective, Preventative, Perfective, and Adaptive—has been fine-tuned through practical implementation and continuous client input, underscoring their efficacy and versatility.

Each one of these methods is described below.

### 5.2.3.3.1.1 Corrective Maintenance

Corrective maintenance involves identifying and fixing defects, errors, and bugs in the software to restore it to its intended functionality. The table below described the process.

Table 1. Corrective Maintenance

|  |  |
| --- | --- |
| Corrective Maintenance Step | Description |
| **Issue Identification** | Gather information from users, testers, and monitoring tools to identify the issue's nature and scope |
| **Issue Reproduction** | Attempt to reproduce the issue in a controlled environment to understand its underlying causes |
| **Issue Diagnosis** | Analyze the code, logs, and system behavior to pinpoint the root cause of the problem |
| **Bug Fixing** | Develop a fix for the identified issue, addressing the root cause and ensuring it doesn't introduce new problems |
| **Testing** | Test the fix thoroughly to verify that it resolves the issue without causing regressions |
| **Deployment** | Deploy the fix to the affected software systems and verify that it works correctly in the production environment |

### 5.2.3.3.1.2 Preventative Maintenance

Preventative maintenance aims to identify and address potential issues before they lead to defects or system failures as illustrated in the table below.

Table 2. Preventative Maintenance

|  |  |
| --- | --- |
| Preventative Maintenance Step | Description |
| **Performance Analysis** | Monitor system performance and identify bottlenecks or areas where performance could degrade over time |
| **Security Audits** | Conduct security assessments to identify vulnerabilities and address them before they are exploited |
| **Documentation Updates** | Keep documentation up-to-date to help future maintenance efforts and reduce confusion |

### 5.2.3.3.1.3 Perfective Maintenance

Perfective maintenance is the most common maintenance activity and focuses on enhancing the software's functionality, user experience, and performance. Perfective software maintenance aims to adjust software by adding new features as necessary or removing features that are irrelevant or not effective in each software we support. This process keeps software relevant as user needs and software functionality change. Here's how we perform perfective maintenance:

Table 3. Perfective Maintenance

|  |  |
| --- | --- |
| Perfective Maintenance Step | Description |
| **Requirements Analysis** | Gather feedback from users and stakeholders to understand their evolving needs and expectations |
| **Feature Review** | Review new software features to ensure they meet user needs and function correctly with existing configurations and other software dependencies |
| **Performance Optimization** | Identify areas where the software's performance can be improved and implement optimizations |
| **Testing and Validation** | Thoroughly test the new enhancements to ensure they meet the expected quality standards |

### 5.2.3.3.1.4 Adaptive Maintenance

Adaptive maintenance involves making changes to the software to adapt to changes in the environment, platforms, or technologies. The table below illustrates how we perform adaptive maintenance.

Table 4. Adaptive Maintenance

|  |  |
| --- | --- |
| Perfective Maintenance Step | Description |
| **Environmental Changes** | Identify changes in hardware, operating systems, or third-party components that may affect the software |
| **Platform Upgrades** | Modify software configurations to work with newer versions of underlying platforms or technologies |
| **Regulatory Compliance** | Make necessary adjustments configuration and deployment practices to ensure the software remains compliant with changing regulations |
| **Data Format Changes** | Update software configuration to handle changes in data formats or external interfaces |

## Software upgrades and patches

We begin the Software patch life cycle with an inventory assessment during the Transition In period to create an updated inventory of all existing devices and their software configurations. We will assess the software versions, patches, and security settings currently in place and develop a plan to patch and remediate any non-compliant systems.

To keep devices in compliance we will implement a patch management system to regularly update operating systems and software applications. We use ServiceNow to maintain inventory and track patch compliance across software and devices.

We use Microsoft System Center Configuration Manager (SCCM) as a centralized software tool to manage software, updates, and configurations across a variety of devices. It allows for automated simultaneously deployment, patch management, and software distribution. We schedule automated updates during non-disruptive times to keep laptops up to date without impacting users during core business hours.

## Security Measures

Kyndryl will install and maintain robust security software, including antivirus, anti-malware, and firewall solutions to keep CalSAWS devices and software secure. We establish and enforce security policies for all software and devices we support. This for example includes password complexity requirements, screen locking, and limitations on software installations.

We also implement automated backups to protect user data should a failure occur, or a device become compromised. We regularly test the backup restoration process to ensure data can be recovered in case of data loss. We enable full-disk encryption to protect sensitive data in case a laptop is lost or stolen. We have checks built into our management processes to ensure encryption solutions are properly configured and keys are securely managed. We implement solutions for remote wiping of laptops in case they are lost or stolen to ensure that sensitive data is not compromised.

All devices are configured to receive automatic operating system updates and we regularly check for and install security patches to address vulnerabilities. We implement remote monitoring and management tools to monitor device health, performance, and security status. This allows for proactive issue detection and resolution.

The cornerstone to our security approach is to educate users and provide them with a support system where they can report issues and receive immediate assistance from our technical experts. We take steps to educate end users about safe browsing practices, the importance of not clicking on suspicious links or downloading unknown files, and how to recognize potential security threats.

### 5.2.3.3.3.1 Security Patch Management

The patch management solution includes the following activities:

* Analyze the vendor security alerts as released by software and hardware vendors.
* Evaluate, test, and post, upon CalSAWS approval, the applicable security alerts to the existing Microsoft Software Update Services or equivalent servers where applicable.
* Integrate the security alerts into the workstation image elements by working with the M&E Contractor to update the production master image repository during the next image refresh.
* Management and distribution of regular Windows monthly security patches
* Management and distribution of Windows feature updates

Patches will be tested on the CalSAWS image and follow the distribution process prior to any mass software distribution. Kyndryl understands CalSAWS’ business environment and does not want distributions to have any impact.

### 5.2.3.3.3.2 Customer Security Document

Kyndryl uses a central, proprietary Customer Security Document (CSD) for every managed services customer. This records IT system security responsibilities, standards, and policies so we can demonstrate agreement on the required policies and controls. The CSD also documents the mutually agreed upon specific protection requirements for individual platforms (operating systems and subsystems).

The CSD uses an international standard, *(ISO/IEC 27002:2005, Information technology - Security techniques Code of practice for information security management*), as a framework for protecting customer information.

The CSD outlines the security services and processes provided by Kyndryl. This document includes the CalSAWS and Kyndryl areas of responsibilities for each service area. It also documents the mutually agreed specific protection requirements for individual platforms (operating systems and subsystems).

This document will be used to review the initial security controls on your systems and advise where they differ from your requirements. Mutually agreed settings are recorded and then used by the support teams to maintain the systems, the compliance teams who perform system security checks, and the Kyndryl internal audit and business controls teams who are ensuring delivery against the infrastructure agreement.

The Customer Security Document can be used with your internal and external auditors and is a useful way of demonstrating that we have discussed and agreed to the system security controls.

We begin with a set of foundations, or basic security controls, and then tailor the program by adding additional services or controls specific to your environment. The applicable security controls are selected in conjunction with Kyndryl based on CalSAWS’ assessment of risk, business principles, and objectives, and legal and regulatory obligations.

The CSD is created during Transition and will require involvement from CalSAWS to ensure we are documenting the appropriate controls that support your policies. A gap analysis will be performed to sample the environment and validate the deployed controls to match what is expected. The document is formally reviewed on an annual basis and informally reviewed as part of the change management process. The CSD is tailored to each client’s controls and policies and changes as the environment changes or new threats emerge.

Once the CSD document is developed for CalSAWS, it will be used to deliver the contracted services according to the specific security requirements CalSAWS has identified for their environment.

The CSD can be used with your internal and external auditors and is a useful way of demonstrating that we have discussed and agreed to the system security controls.

Kyndryl will review the CSD document on a regular basis with CalSAWS to compare against CalSAWS’ requirements.

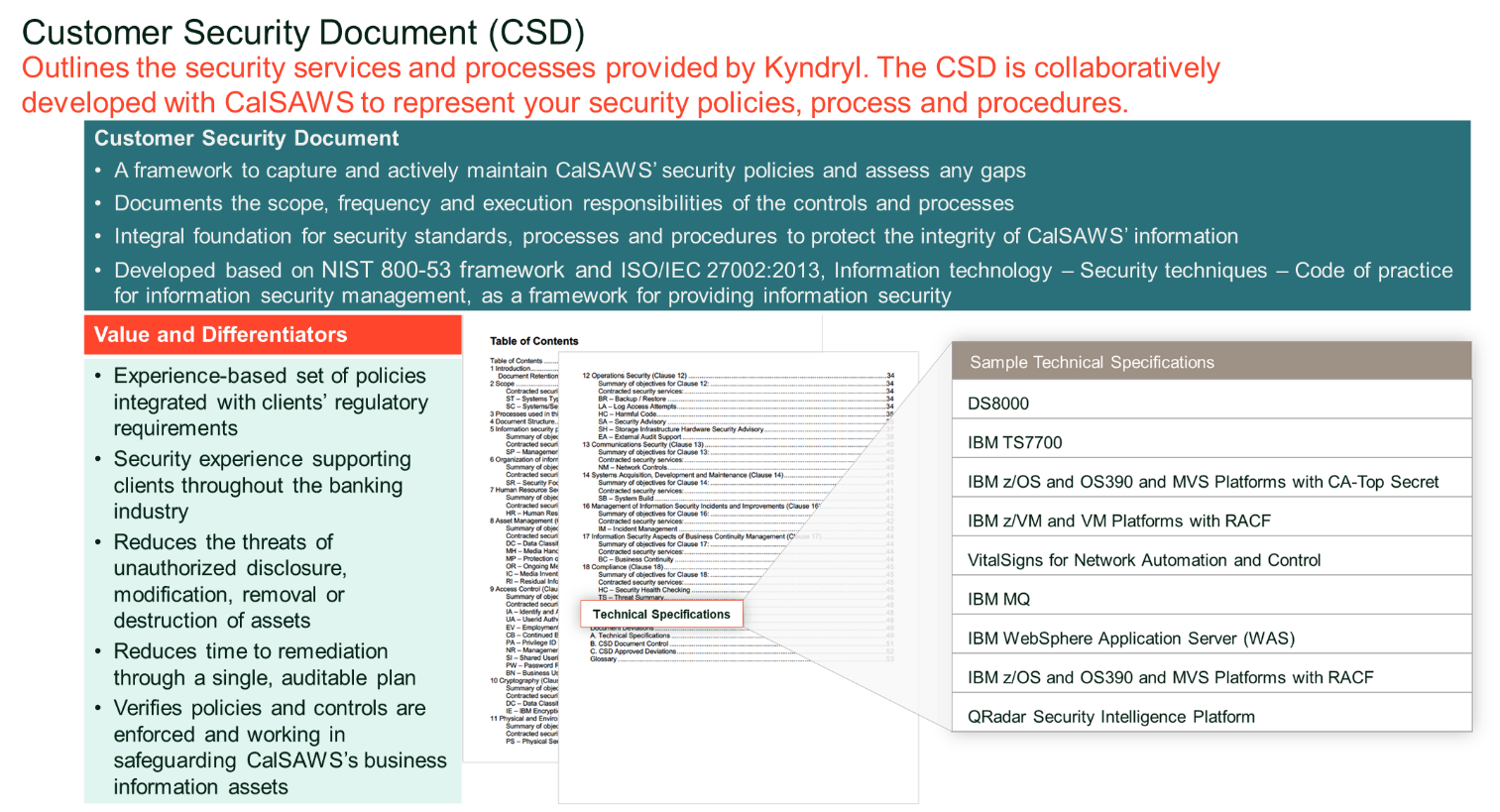


Figure 1. Customer Security Document

## Infrastructure staff allocation approach to support Hardware/Software Maintenance and Operations

Our proposal currently models our end-to-end staffing model to support the following teams:

1. **Remote Support Team (Service Desk):** (18) Kyndryl Technicians are assigned to Hardware and Software support for all County and CalSAWS users remotely from our Service Desk. Kyndryl will support CalSAWS users using an 8:00 am to 5:00 pm Monday to Friday operating model.
2. **Deskside Support Team:** (12) Kyndryl Support Technicians working in pairs are assigned to provide deskside support to users in each geographic region. These resources rotate between CalSAWS, County, and Kyndryl provided offices following an 8:00 am to 5:00 pm Monday to Friday operating model. When urgent desk side support is needed in a particular location at a particular time technicians are dispatched by the Service Desk based on criticality and a first in first out support model. Idel technicians in nearby regions also lend support during peak times.
3. **Depot support team:** (4) Kyndryl Support Technicians dedicated to device imaging, break-fix, disposal, asset management logistics, and warehouse management at two primary locations near CalSAWS project offices.

We will make continuous updates to this model’s resource allocation as more information becomes available on user and device density across the state as well as user preferences between remote and deskside support.

### 5.2.3.3.4.1 User Experience

Users will first contact the Kyndryl Service Desk to register the issue and receive remote support. Our remote support technician will work with the user during the initial call to troubleshoot the problem through discussion and screen share. Everything between the agent and User is captured as a case in ServiceNow. This allows agents to understand prior issues and enables device management for the life of that piece of hardware. If the issue is not correctable over the phone, the ticket will be assigned to a deskside support technician nearest the user. The support technician will call the user to provide tier 2 support remotely. If the issue is still not resolvable the user and deskside support technician will determine where to meet at the closest location to the user, either a CalSAWS office, County office, or Kyndryl provided office space. The closest Kyndryl technician will bring replacement hardware in the event the issue cannot be resolved so that the CalSAWS user is able to return to work with a new device quickly. The Kyndryl technician will return defective devices to our major depots for repair or return to the manufacture.

### 5.2.3.3.4.2 Geographic Coverage Model

Our Infrastructure staffing model and approach for CalSAWS will be designed based on our similar model with Arizona’s DMV. We have helped AZ DMV transform and modernize their end user devices and support process over the last few years and are currently managing over 50,000 physical devices for them remotely and in their offices across the entire state. We have learned from Arizona DMV that it is critical to have local technicians who rotate between client offices on a schedule so that relationships can be built, response times are efficient, costs are reduced, and our clients get to see and interact with us every day.

We recognize that there will be varying CalSAWS user concentrations across California, that each County will have unique requirements, and that these may change over time. To meet this support requirement, we will work with CalSAWS prior to Transition In to understand exact user location densities so we can break California into logical geographic regions that a support technician or small team of individuals can physically manage from both a travel and user demand perspective.

After initial implementation of the remote and desk side model we will continue to monitor the user demand for remote and deskside support and change allocations to technician types and staff levels accordingly. This strategy will allow Kyndryl to provide CalSAWS tailored support and specialized assistance for each county’s diverse needs while also optimizing technician allocation and response times.

The key to our geographic deskside approach is to hire local technician talent within a given region so that our support experts live in the communities they support. This reduces costs for transportation and increases response time vs. hosting technicians only out of large metropolitan areas. Local technicians are better positioned to understand the specific technology landscape and potential issues faced by users in these regions. This regional talent approach not only improves the quality of support but also fosters a more personalized and localized user experience.

We will also implement a technician rotation structure to allow technicians to collaborate and share expertise with other technicians in nearby regions. This can be particularly helpful for resolving complex or uncommon technical problems where you need to phone a friend for help. This rotation approach provides opportunities for knowledge sharing and cross-training while enhancing the overall skill set of our support teams.

**Examples of possible regions a team could cover** are illustrated in the figure below**:**

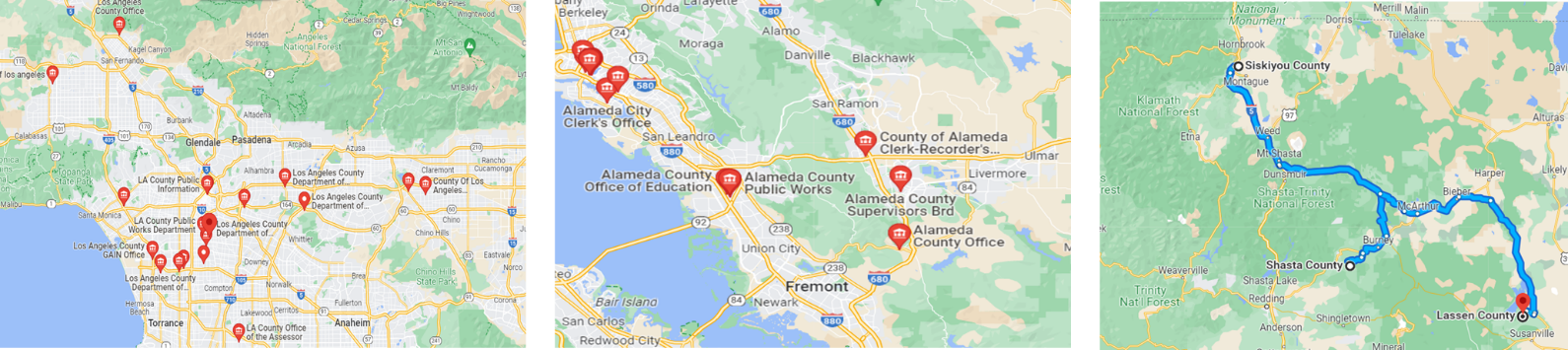


Figure 2. Regional Coverage Examples

Additionally, we will implement a comprehensive ticketing on ServiceNow for tracking system to enable us to monitor support requests, response times, and issue resolutions across all regions so continuous improvement to the coverage models can be made.

When a Deskside Technician is dispatched to a user, the user will be able to track the technician's progress using Dispatch Tracker.

* Technician tracking software integrated with ServiceNow for end user detail and ticket updates.
* Web based tracking platform no need for dedicated software.
* CalSAWS end user receives invite link via email and/or SMS to track the deskside technician
* Real time location of technician on live map
* ETA provided based on traffic data
* Technician name and button to call provided on live map
* Automatic notification to CalSAWS end user upon detection of arrival at service address

A screenshot of a mobile application

Description automatically generated

Figure 3. Dispatch Tracker

We recommend that our technicians work in CalSAWS or County offices alongside users whenever possible so that our technicians can be seen as part of the team and build relationships. Our technicians will float between locations on a schedule within their region so that our teams are recognizable and CalSAWS users feel they have a support team available to them. In areas where we need to provide our own support locations, we will provide secured rented office space where CalSAWS users can travel to meet in person with our technicians to receive support.

Benefits of our regional coverage model include:

* **Faster Response Times:** Local technicians can respond to support requests quicker since they are already in close proximity to the users they serve. This reduces downtime and frustration for users facing technical issues.
* **Increased Availability:** Local technicians are more likely to be available for on-site visits at shorter notice. This is particularly important for critical issues that require immediate attention.
* **In-depth Community Understanding:** Local technicians are familiar with the unique technology landscape, challenges, and preferences of the community they serve. This localized knowledge helps them provide more relevant and effective support.
* **Personalized Support:** A local technician can offer personalized support by understanding the specific needs and expectations of users within the community.
* **Community Relationships:** A local technician can build relationships with users and stakeholders in their support community. This can foster trust and a sense of reliability, which is essential for long-term support success.
* **Efficient Problem Solving:** Local technicians are well-acquainted with the local infrastructure, potential connectivity issues, and other region-specific factors. This knowledge enables them to troubleshoot and resolve problems more efficiently.
* **Minimized Travel Costs and Time:** Having technicians live in the community eliminates the need for long commutes from large cities, reducing travel costs and time. This can lead to better work-life balance and improved job satisfaction for technicians.
* **Resource Allocation Efficiency:** By placing technicians where they are needed most, you can optimize resource allocation. Larger cities can still have technicians to handle high-density areas, while local technicians can cater to specific needs in the countryside.
* **Reduced Environmental Impact:** Less commuting by technicians results in a smaller carbon footprint and contributes to environmental sustainability.
* **Prevention of Commuting Fatigue:** Long commutes can lead to fatigue and reduced productivity for technicians.

## Innovation Support

Kyndryl embraces the need for innovation and enables our support experts to stay ahead of evolving user needs and technological advancements through dedicated time to perform proof of concepts. These side projects also give them something to work on during occasional periods of low user support demand. We work with our technicians to create coverage models that allow them to balance their user support responsibilities with innovation work so that they have at least 8 hours a month to explore innovative ideas or learn new skills to improve service while a peer provides coverage to their region.

We believe that innovation is pivotal for any hardware and software support service as it directly impacts the long-term efficiency, effectiveness, and user experience of technical assistance. We have helped many clients implement innovative solutions that empowers their users with self-help resources, real-time collaboration features, and personalized solutions, enhancing their ability to troubleshoot problems independently and fostering a sense of empowerment.

By continually exploring new avenues of innovation, our support services can offer seamless, innovative assistance that not only meets but exceeds customer expectations, driving greater user satisfaction and loyalty in an increasingly competitive market. Below is a list of innovative enhancements in the hardware software support domain we are working with other clients to implement:

* **AI-Powered Troubleshooting:** Integrating AI chatbots and virtual assistants that can help users self-diagnose and troubleshoot common issues, providing users with quick solutions and reducing the need for human intervention.
* **Remote Diagnostics:** Developing tools and techniques that allow support teams to remotely diagnose and fix problems on users' devices, minimizing downtime and the need for physical visits.
* **Self-Help Resources:** Create an extensive knowledge base with step-by-step guides, video tutorials, and Frequently Asked Questions (FAQs) that empower users to resolve minor issues independently.
* **Predictive Maintenance:** Utilize sensors and data analytics to predict when a device might encounter problems, allowing users to address issues before they become critical.

I-UA8 Describe your approach for providing central and remote CalSAWS Hardware maintenance services for the Project Offices and CalSAWS Managed Hardware located in the Counties.

Describe your depot location(s), where and how equipment will be staged for deployment, and which staff will be deployed, along with the manner of deployment, to support Central Project Office support and remote County support.

Describe your approach for technology refresh efforts and incident/issue support.

## Approach to providing central and remote CalSAWS Hardware maintenance services for the Project Office and Counties

Our Geographic Coverage Model detailed in 5.2.3.3.4 above outlining software support through deskside support technicians who rotate between CalSAWS and County sites within a geographic region also applies to hardware support as well. CalSAWS and Country offices are supported within geographic region by a team of deskside support technicians who either rotate between offices or are dedicated to support offices full time when demand allows their full utilization.

If space is not available in the CalSAWS Project or County offices for Kyndryl technicians to continuously be present in, we will provide secured office space near the office locations where users can bring their laptop devices for support. For devices like desktops, printers, scanners, kiosks, network, and video conferencing devices that are physically in CalSAWS and County offices our deskside support technician will be dispatched to the building with replacement parts to restore service.

The foundation of our hardware maintenance approach is to replace equipment rapidly, so productivity is restored as soon as possible with a break-fix performed later at our depot site after service is restored to CalSAWS. To do this we will maintain depos that have spare devices for every piece of equipment we support. When our technicians cannot fix a device, we will return it to the manufacturer through warranty support and restock the replacement in the depos to maintain the spare capacity support for the future.

## Depot locations, staging and deployment

Kyndyl's solution has modeled two large depots located near the Roseville and Norwalk CalSAWS offices. These depots will contain equipment for all hardware assets like laptops, desktops, local printers, scanners, kiosk equipment, video conferencing devices, and network devices. These depots will be used to perform break-fix work and to ship defective hardware back to manufacturers. The depot locations will also serve as a staging facility for pre-configuration of devices like user laptops. Innovation activities like proof of concepts will also be conducted at these depot locations.

Smaller regional depots will be strategically located in each geographic region, so our deskside support technicians have quick access to devices when supporting regions not close to CalSAWS offices. These smaller depots will be secure, climate-controlled facilities but will only have devices needed in that region, primarily laptop devices for end users. The exact depot solution in each geographic region (ex. secure Kyndryl office or Kyndryl acquired climate-controlled locker facilities) will vary based on the specific needs of the county offices in that region. The exact location details of how these smaller depots are deployed will be confirmed once Kyndryl has analyzed the CalSAWS user and device density enabling us to build a tailored geographic support plan. We have learned from supporting the AZ DMV devices across the state that depo location and geographic allocations for support technicians is a very nuanced process which requires continuous adjustment overtime, so we have budgeted in our solution to meet a wide range of possibilities.

## Technology Refresh Approach

### 5.2.3.3.12.2 Refresh Process

The refresh process is a full lifecycle process that includes both joint planning and scheduled refresh project execution activities that are designed to periodically refresh the infrastructure environment in a planned, cost-effective manner that minimizes disruption.

Refresh coordination for equipment and software requires centralized coordination of the refresh perform activity, and includes the scheduling, coordination, and administrative completion.

To assist with equipment and systems software refresh coordination, Kyndryl will:

* Leverage lessons learned from our past infrastructure experience with refresh activities to suggest approaches and techniques
* Work with CalSAWS to review and provide input into the refresh plan, schedule the refresh perform date, communicate the plan to stakeholders, and resolve any refresh issues
* Assist CalSAWS with the development and execution of testing plans
* Execution of the refresh campaigns

The refreshment of software will include application upgrades, releases, and new application software. Kyndryl will follow the CalSAWS Change Management Process prior to introducing a refresh into the CalSAWS environment.

Kyndryl will:

* Leverage Kyndryl’s past refresh experience (upgrades, release and new application software) activities
* Review and obtain approval of the refresh plan and schedule from CalSAWS
* Coordinate the refresh perform date with CalSAWS
* Communicate to CalSAWS the effect and impact of the refresh
* Resolve refresh issues
* Obtain signoff from CalSAWS prior to the refresh being implemented into production
* Conduct a post-change review which includes lessons learned

### 5.2.3.3.12.1 Refresh Schedule

Kyndryl will collaborate with CalSAWS to maintain the technical currency of the in-scope equipment in line with the agreed refresh timeframes:

Table 5. Equipment Refresh Schedule

| Equipment | Refresh Schedule |
| --- | --- |
| PC (Desktop/Laptop) | 3 years |
| Non-production Servers | 5 year |
| Network Equipment (excluding Switches) | 4 years |
| Network Switches | 5 years |
| Video Conferencing Equipment | 5 years |
| Uninterruptible Power Supply (UPS) Devices | 5 years |

## Incident/Issue Support

Our approach to incident and issue support on ServiceNow follows a comprehensive and structured methodology designed to swiftly identify, address, and resolve IT challenges while maintaining seamless communication and collaboration across teams.

Our process begins with a meticulous assessment of the reported incident's scope and severity. We employ ServiceNow's incident management module to categorize incidents based on their impact and urgency, ensuring that the appropriate resources are allocated for swift resolution.

Upon incident classification, we initiate an immediate triage involving our dedicated incident response team. This team, comprised of seasoned technicians and subject matter experts, can evaluate an incident’s criticality, and categorize it accurately.

ServiceNow's collaboration tools serve as the backbone of our communication strategy. Our teams engage in real-time discussions, leveraging shared insights and diagnostic data. Regular updates are provided to stakeholders through ServiceNow's integrated communication channels, maintaining transparency throughout the incident's lifecycle.

Root cause identification is a cornerstone of our approach. By leveraging ServiceNow's incident history and knowledge base, we identify patterns and potential underlying problems that contribute to the incident. This enables us to address the root cause and prevent recurrences.

Our skilled team implements the solution following established procedures and leveraging ServiceNow's automation capabilities. Each step of the resolution process is meticulously documented within the platform, ensuring a comprehensive incident record for future reference.

Prior to closure, our resolution undergoes rigorous testing to validate its effectiveness. A subset of end-users is engaged to confirm that the issue has been satisfactorily resolved. This approach ensures a seamless user experience post-resolution.

Upon resolution confirmation, the incident ticket is closed. We schedule a post-incident review, leveraging insights gained to enhance our incident response strategy continuously.

Our documentation extends to updating the knowledge base with incident details, root cause analysis, and resolution steps. This facilitates knowledge sharing, enabling our team and others to learn from each incident and contributes to a growing repository of expertise.

I-UA9 Describe challenges and risks to providing CalSAWS Hardware and CalSAWS Software management for CalSAWS and how you will mitigate the risk.

## Challenges and risks to providing CalSAWS Hardware and CalSAWS Software management

The following table identifies potential challenges/risks and mitigation approaches that we have identified for CalSAWS at this time based on our experience delivering hardware and software management services to similar clients.

Table 6. Hardware and software management services risks and mitigation strategies

| Potential Challenge/Risk | Category | Proposed Risk Mitigation Plan |
| --- | --- | --- |
| Unforeseen disruptions in the supply chain, such as component shortages or manufacturing delays. | Hardware | Maintain a diverse network of suppliers and maintain backup sources for critical components in our depot locations. |
| During hardware repairs, sensitive data stored on devices could be at risk of exposure, potentially leading to data breaches or privacy violations. | Hardware | Provide technicians with training and clear guidelines on data security procedures. We implement strict data handling protocols for all devices, including data encryption, secure wiping of storage devices, and adherence to relevant HIPPA and NIST data protection regulations. |
| Unpredictable Workload Peaks. Hardware failure incidents might experience sudden spikes, overwhelming available resources and causing delays in response times. | Hardware  /Software | Maintain a scalable workforce by collaborating with external service providers and other Kyndryl delivery teams during peak periods or large system refreshment efforts. We develop a clear incident prioritization strategy to ensure critical issues are addressed promptly within established SLAs. |
| Lack of clear and consistent communication with customers regarding repair status, estimated timelines, and any potential delays can lead to dissatisfaction and frustration. | Hardware  /Software | Implement automated notifications to users that provides regular updates to customers throughout the repair process. We establish a dedicated customer support channel for inquiries through our Service Desk and provide self-service options for customers to track their repair status. |
| Updates or new software installations might lead to compatibility issues with existing applications or hardware, causing disruptions or system instability. | Software | Establish a comprehensive testing environment to assess new updates or software installations before deployment to end users. We maintain a database of known compatibility issues from across our Kyndryl worldwide managed service operations and provide guidelines for software procurement to our delivery teams. |
| Software updates or system changes can inadvertently lead to data loss or corruption, impacting business operations and data integrity. | Software | Implement comprehensive data backup procedures prior to any significant changes and conduct thorough testing before deploying updates and changes to devices. |
| Inaccurate software licensing or non-compliance with software usage terms could result in legal and financial consequences. | Software | Maintain a comprehensive inventory of our client’s software licenses and ensure compliance with each vendor’s terms. We regularly audit software deployments to identify and address any compliance gaps. |