Statement of Work
4

1. PROJECT OVERVIEW

test

2. SCOPE OF WORK

This Statement of Work outlines the deliverables and services to be provided for the 4 project. It includes detailed requirements, implementation tasks, acceptance criteria, timeline, and costs.

3. REQUIREMENTS

Requirement 1: Intuitive Ticket Creation Process

The target system's user interface for creating service tickets must be intuitive and streamlined, mirroring the workflow demonstrated in the 'Product Team Meeting - 2019-07-09.mp4' video. This includes clear labeling of fields, logical grouping of related information, and intelligent form pre-population based on user context and previous entries. The navigation flow should guide users through the process with minimal clicks and clear progress indicators. The user experience should be enhanced with features like auto-suggestions for common fields, real-time validation of inputs, and the ability to easily attach relevant files. The target system should also support various input methods, including keyboard shortcuts and voice-to-text, to cater to diverse user needs and improve efficiency in ticket creation.

Requirement 2: Seamless Ticket Search and Filtering

The target system must provide a robust search and filtering functionality for service tickets, replicating the capabilities observed in the source system video. Users should be able to search by keywords, ticket ID, customer name, assigned agent, status, priority, and other relevant criteria. The search interface should offer advanced filtering options, including date ranges, custom fields, and logical operators (AND, OR, NOT). The search results should be displayed in a clear and organized manner, with customizable columns and sorting options. The user experience should prioritize speed and efficiency, providing real-time search suggestions and displaying results as the user types. The system must also support saved searches and filters for frequently used queries, improving user productivity and reducing repetitive tasks.

Requirement 3: Responsive Design for All Devices

The target system's user interface must be responsive and adapt to different screen sizes and devices, ensuring a consistent user experience across desktops, laptops, tablets, and smartphones. This includes adjusting layout, font sizes, and interactive elements to optimize usability on each device. The navigation flows should remain intuitive and efficient regardless of screen size, with clear visual cues and touch-friendly controls on mobile devices. The responsive design should prioritize performance and minimize loading times across all devices, ensuring a seamless user experience. This requirement is essential for supporting field technicians and remote workers who access the service management system on various devices.

Requirement 4: Accessible UI for All Users

The target system's user interface must adhere to accessibility guidelines (e.g., WCAG 2.1) to ensure usability for all users, including those with disabilities. This includes providing alternative text for images, keyboard navigation for all interactive elements, sufficient color contrast, and support for assistive technologies like screen readers. The navigation flows should be designed with accessibility in mind, providing clear and consistent landmarks and keyboard shortcuts for common actions. The user experience should be inclusive and cater to diverse needs, ensuring that all users can access and interact with the service management functionality effectively. This is crucial for compliance and inclusivity.

Requirement 5: Consistent UI with Project Context 4

The target system's user interface and navigation flows for service management functionality must maintain consistency with the overall design and branding guidelines established for Project Context 4. This includes using consistent color palettes, typography, iconography, and interaction patterns across all modules and workflows. The user experience should be cohesive and familiar, minimizing cognitive load and facilitating seamless transitions between different parts of the system. This consistency is crucial for building a strong brand identity and ensuring a positive user experience across the entire platform, as highlighted in the 'Product Team Meeting - 2019-07-09.mp4' video's discussion on user adoption and training.

Requirement 6: Service Request Approval Workflow

The target system must replicate the service request approval workflow demonstrated in the 'Product Team Meeting - 2019-07-09.mp4' video. This includes replicating the conditional approval paths based on request type, priority, and estimated cost. For service requests exceeding $500, two levels of managerial approval are required: the direct manager and a department head. For requests below $500, only direct manager approval is necessary. The system must enforce these rules and automatically route requests to the appropriate approvers. The workflow must also include provisions for rejecting requests, with clear communication to the requestor including the reason for rejection. Finally, an audit trail of all approvals, rejections, and modifications to the request must be maintained for reporting and compliance purposes within project context 4.

Requirement 7: Automated Service Ticket Routing

The target system must implement the automated service ticket routing logic observed in the source system video. This includes routing tickets based on service category, assigned team, and availability of support personnel. The routing rules must consider the skillset of the support team members, prioritizing tickets to agents with the appropriate expertise. If no agent with the required skills is available, the ticket should be escalated to a secondary support team as demonstrated in the video. The target system must also maintain a queue management system with clear visibility into ticket status, assigned agent, and time spent in each stage of the workflow within project context 4.

Requirement 8: SLA Management and Escalation

The target service management system must incorporate SLA management functionality equivalent to the source system, including automated escalation procedures for breached SLAs. The video 'Product Team Meeting - 2019-07-09.mp4' showcases specific SLA timelines based on service priority. The target system must adhere to these timelines and trigger automated notifications to relevant stakeholders upon breach. Escalation procedures must involve notifying higher management levels and potentially re-assigning the ticket to a specialized team. The system should also provide reporting capabilities to track SLA performance and identify areas for improvement within project context 4.

Requirement 9: System Performance and Response Times

The target service management system must demonstrate acceptable performance and response times under expected load conditions, comparable to or better than the source system as observed in the video. This includes page load times, search query response times, and workflow execution times. Performance testing should be conducted to ensure that the system can handle the anticipated volume of service requests and user interactions within project context 4. Target response times for key operations, such as creating a service request or retrieving ticket information, should be defined and validated during testing to ensure a satisfactory user experience.

Requirement 10: Secure Data Migration and Access Control

Data security is paramount during the migration process. All data transmitted between the source and target systems must be encrypted using secure protocols. Access to migration data should be restricted to authorized personnel only. The target system must enforce appropriate access controls to ensure data confidentiality and integrity. Audit logs should be maintained to track all data access and modifications during the migration process. The migration process should comply with all relevant security policies and regulations. Post-migration, data validation checks should be performed to ensure data integrity and identify any potential security breaches.

Requirement 11: Data Masking and Anonymization

The target system must implement data masking and anonymization techniques to protect sensitive customer information within service records. This includes masking or redacting personally identifiable information (PII) such as names, addresses, phone numbers, and email addresses when accessed by unauthorized personnel. The system must also support data anonymization for reporting and analytics purposes, allowing aggregated data analysis without compromising individual customer privacy. This functionality is crucial for complying with data privacy regulations like GDPR and CCPA and maintaining customer trust. The masking and anonymization rules should be configurable and auditable, ensuring transparency and accountability in data handling practices.

Requirement 12: Compliance with Service Management Regulations

The target system must be designed and implemented to comply with relevant service management regulations and industry standards, such as ITIL, ISO 20000, and any applicable industry-specific regulations. This includes adhering to best practices for service request management, incident management, problem management, and change management. The system should provide features and functionalities that support compliance reporting and documentation, enabling the organization to demonstrate adherence to regulatory requirements. This includes the ability to generate reports on key performance indicators, service level agreements, and security controls. Maintaining compliance is essential for minimizing legal and operational risks, enhancing customer trust, and ensuring the quality and reliability of service delivery.

Requirement 13: Knowledge Base Article Integration

The target system must integrate with the existing knowledge base system. This integration should enable users to access relevant knowledge articles within the service management workflow. The data structure for knowledge articles in the target system must be compatible with the existing knowledge base. Field mappings should be defined for key attributes like article ID, title, content, keywords, and related categories. The integration point should allow for real-time searching and retrieval of knowledge articles based on keywords or context from within the target system. This will enable agents to resolve incidents and fulfill service requests more efficiently.

Implementation Tasks:

- Configure Knowledge Object and Field Mappings (8 hours)
- Develop Oracle Knowledge Base Integration API (8 hours)
- Create Knowledge Search Component for Service Console (8 hours)
- Implement Contextual Knowledge Suggestion Feature (8 hours)
- Develop Knowledge Article Formatting and Display Handler (8 hours)
- Implement Comprehensive Integration Testing Suite (8 hours)

Acceptance Criteria:

• Given I am logged in as a service agent
And I am working on an incident ticket
When I search for knowledge articles using the keyword "network outage"
Then the system should display a list of relevant...

• Given I am logged in as a service agent
And I am viewing a service request with category "password reset"
When I click on the "Find Knowledge" button
And I select a knowledge article titled "Standard ...

• Given I am logged in as a service agent
And I am working on a ticket
When I search for knowledge articles with the keyword "nonexistent topic"
And no matching articles exist in the knowledge base
Then...

• Given I am logged in as a knowledge manager
And I create a new knowledge article in the existing knowledge base with:
| Field | Value |
| ID | KB001023...

• Given I am logged in as a service agent
And I am updating an incident with the description "User cannot access shared drive"
When I type in the resolution field
Then the system should automatically su...

Requirement 14: Data Integrity and Validation Rules

The target system must enforce data integrity and validation rules consistent with the source system, as observed in the 'Product Team Meeting - 2019-07-09.mp4' video. This includes input validation for fields such as request type, priority, description, and contact information. Specific validation rules, such as mandatory fields, data type restrictions, and format requirements, must be implemented to prevent invalid data entry. The system should also incorporate error handling mechanisms to provide clear and informative error messages to users in case of validation failures. This is crucial for maintaining data quality and ensuring the reliability of the service management processes within project context 4.

Requirement 15: Incident Data Migration and Mapping

The target service management system must seamlessly migrate all incident data from the source system, including incident number, creation date, priority, status, assigned technician, description, resolution notes, and related configuration items. Field mappings between the source and target systems must be precisely defined and validated to ensure data integrity. Transformation rules must handle any data format discrepancies, such as date formats or priority codes. The integration point for incident data migration should leverage a secure API or data export/import mechanism. Data validation checks must be implemented in the target system to ensure data accuracy and completeness after migration.

Requirement 16: Service Request Data Transformation

Service request data from the source system requires transformation before loading into the target system. This includes mapping service categories, subcategories, and request types to the equivalent structures in the target system. Custom fields from the source system must be evaluated and either mapped to existing fields in the target system or new custom fields created. The integration process should handle data type conversions where necessary. For instance, if the source system uses a text field for priority and the target uses a numerical value, a transformation rule needs to be defined. Any dependencies between service request data and other data entities, such as users or CIs, should be preserved during the migration.

Requirement 17: Data Migration Performance Requirements

The data migration process must meet specific performance requirements to minimize downtime and ensure business continuity. The migration of incident and service request data should be completed within a defined timeframe, for example, within a weekend maintenance window. The integration process must be optimized to handle large volumes of data efficiently. Performance testing should be conducted to validate the migration process and identify any potential bottlenecks. Metrics such as data throughput and processing time should be monitored and reported. Any performance issues identified during testing must be addressed before the final migration.

Requirement 18: Role-Based Access Control for Service Data

The target service management system must implement role-based access control (RBAC) to restrict access to sensitive service data based on user roles and responsibilities. Each role should have clearly defined permissions for viewing, creating, modifying, and deleting service records, ensuring that users only have access to the information necessary for their job function. This includes granular control over specific fields within service records, preventing unauthorized access to confidential customer data, internal notes, or financial information. The RBAC system must be configurable and auditable, allowing administrators to easily manage roles and permissions and track changes over time. This is critical for complying with data privacy regulations and maintaining the security of sensitive service data. The system should support integration with existing identity providers for seamless user management and authentication.

Requirement 19: Comprehensive Audit Trail for Service Actions

The target system must maintain a comprehensive audit trail of all service-related actions, including record creation, modification, deletion, and access attempts. The audit trail must capture the user identity, timestamp, action performed, and any changes made to the data. This information should be securely stored and readily retrievable for auditing and investigation purposes. The audit trail must be tamper-proof to ensure data integrity and provide evidence of compliance with regulatory requirements. Furthermore, the system should provide reporting capabilities to analyze audit data and identify potential security breaches or unauthorized activities. This is essential for maintaining accountability and demonstrating compliance with industry regulations.

Requirement 20: Secure Data Retention and Disposal Policy

The target system must adhere to a secure data retention and disposal policy that aligns with industry best practices and relevant regulations. This policy must define the retention period for different types of service data, ensuring that data is retained for the necessary duration for business operations, legal compliance, and audit requirements. The policy must also specify secure data disposal methods, such as secure erasure or encryption, to prevent unauthorized access to deleted data. The system should automate data retention and disposal processes, minimizing manual intervention and reducing the risk of human error. This is crucial for minimizing data storage costs, mitigating legal risks, and protecting sensitive information throughout its lifecycle.

4. TIMELINE AND MILESTONES

Project Start: 4/20/2025
Estimated Completion: 7/19/2025

Key Milestones:
• Requirements Finalization: 5/4/2025
• Development Phase: 6/4/2025
• Testing and QA: 7/4/2025
• Final Delivery: 7/19/2025

5. COSTS AND PAYMENT

Item	Amount
Total Estimated Hours	48 hours
Hourly Rate	$150/hour
Total Estimated Cost	**$7,200**