Risk Management Plan for:
Government
Citizen Helpdesk Portal

Version: 1.0

Approval date: 29/3/25

DOCUMENT CONTROL PANEL		
File Name:	Citixen Helpdesk Protal	
File Location:	E:\SE Project	
Version Number:	1.0	
	Name	**Date**
Created By:	Anamitra Bhattacharyya,Aryan Panda	29.03.25
Reviewed By:		
Modified By:		
Approved By:		

Table of Contents

List of Acronyms and Abbreviations

- **FDOT** – Florida Department of Transportation
- **ITS** – Intelligent Transportation Systems
- **MFA** – Multi-Factor Authentication
- **ITSM** – IT Service Management
- **KPI** – Key Performance Indicator
- **SLA** – Service Level Agreement
- **API** – Application Programming Interface
- **COTS** – Commercial Off-The-Shelf
- **NIST** – National Institute of Standards and Technology
- **SOC** – Security Operations Center
    -

1.Scope

1.1 Purpose

The purpose of this Risk Management Plan is to establish a structured approach for identifying,assessing, mitigating, and monitoring risks associated with the Government Helpdesk Portal. This plan ensures that risks are proactively managed to prevent disruptions, security breaches, or operational inefficiencies that could impact the portal's effectiveness.

The Government Helpdesk Portal is a critical tool that enables government employees and citizens to report issues, request support, and access relevant documentation. Given the sensitivity of the data and the high availability requirements, it is essential to implement a comprehensive risk management strategy to safeguard operations, maintain compliance, and ensure user satisfaction.

2. Applicable Documents

2.1 Florida Department of Transportation Documentation

This document references relevant Florida Department of Transportation (FDOT) guidelines, regulations, and best practices to ensure compliance and integration with existing transportation systems.

2.2 ITS Project Documentation

Intelligent Transportation Systems (ITS) documentation that may affect or integrate with the helpdesk portal, including cybersecurity policies, network infrastructure standards, and IT governance frameworks.

3. Definitions

Risk

A risk is a potential event, condition, or vulnerability that, if realized, could negatively impact the Government Helpdesk Portal's security, functionality, performance, or compliance. Risks may arise from technical failures, security breaches, regulatory non-compliance, human errors, or external threats such as cyberattacks or system overloads.

Example Risks:

- **Cybersecurity Threats:** Phishing attacks targeting helpdesk support staff.
- **Data Breaches:** Unauthorized access to sensitive user data (e.g., PII, government records).
- **System Downtime:** Infrastructure failures causing service outages for users.

Mitigation

Mitigation refers to proactive actions taken to reduce the likelihood or impact of a risk. Effective risk mitigation strategies ensure that potential threats are addressed before they escalate into major disruptions.

Mitigation Strategies Include:

- **Security Hardening:** Implementing firewalls, encryption, and multi-factor authentication (MFA) to protect sensitive data.
- **Redundancy & Failover Systems:** Ensuring backup servers and cloud storage are available to minimize system downtime.
- **Regular Security Audits:** Conducting periodic assessments to detect vulnerabilities before exploitation.

Risk Assessment

Risk assessment is the systematic evaluation of identified risks to determine their likelihood, potential impact, and priority level. The goal is to categorize risks and allocate appropriate mitigation resources.

Assessment Criteria:

- **Likelihood:** The probability of the risk occurring (Low, Medium, High).
- **Impact:** The extent of damage or disruption if the risk materializes (Minimal, Moderate, Severe).
- **Priority Level:** Based on a combination of likelihood and impact, risks are classified as **low, medium, or high priority** for mitigation.

Risk	Likelihood	Impact	Priority	Action Plan
Data Breach	High	Severe	Critical	Implement strict access controls & encryption
Server Crash	Medium	High	High	Deploy failover servers & backup recovery plans
User Error	Low	Moderate	Medium	Implement user training & automated checks

Stakeholders

Stakeholders are individuals or organizations that have an interest in the Government Helpdesk Portal and its operations. They play an essential role in risk identification, reporting, and mitigation.

Key Stakeholders:

- **Government Employees:** Use the portal for IT support and issue resolution.
- **IT Support Teams:** Manage system performance, resolve user requests, and implement security measures.
- **Project Managers:** Oversee portal development and risk mitigation strategies.
- **Regulatory Authorities:** Ensure compliance with government cybersecurity and data protection laws.
- **Vendors & Suppliers:** Provide third-party software, hardware, or IT services that integrate with the portal.

Contingency Plan

A contingency plan is a predefined set of actions designed to respond to an unexpected risk event. The purpose of a contingency plan is to minimize downtime, protect data, and restore services quickly in the event of system failure, data breach, or other major incidents.

Examples of Contingency Measures:

- **Data Breach Response Plan:** Immediate isolation of compromised systems, forensic investigation, and user notification procedures.
- **Disaster Recovery Plan:** Backup restoration procedures in case of system failure or data loss.
- **Incident Escalation Protocol:** Defined steps for notifying higher authorities and deploying emergency response teams.

Residual Risk

Residual risk refers to the risk that remains after all mitigation measures have been applied. While mitigation efforts can reduce the impact of a risk, it is often impossible to completely eliminate all risks. Residual risks must be monitored continuously and documented in the risk register for ongoing assessment.

Example of Residual Risk:

- Despite strong authentication measures, insider threats (e.g., employees leaking data) may still pose a risk.
- Even with server failover systems, a natural disaster affecting all data centers could cause downtime.

Compliance

Compliance refers to adhering to regulatory, security, and operational standards established by government and industry authorities. The Government Helpdesk Portal must comply with state and federal laws, such as:

- **FISMA (Federal Information Security Management Act):** Requires federal systems to implement strong security measures.
- **GDPR (General Data Protection Regulation):** Protects personal data of EU citizens, applicable if the portal handles EU citizen data.
- **NIST Cybersecurity Framework:** Establishes best practices for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats.

Failure to comply with regulations can result in **legal penalties, reputational damage, and financial losses**.

4 Project Summary

The Government Helpdesk Portal is a mission-critical web-based application designed to enhance efficiency in handling IT and administrative support requests from government employees and citizens. The portal serves as a centralized system for submitting and managing service tickets, accessing self-help documentation, and interacting with IT support teams.

To ensure seamless operation, the portal integrates with existing government IT infrastructure, adheres to state and federal compliance requirements, and is fortified with cybersecurity measures to protect sensitive information.

The project is driven by the need for:

- **Improved response times** for IT support requests.
- **Streamlined communication** between users and helpdesk agents.
- **Enhanced security** to safeguard government data.
- **Operational efficiency** through automation and intelligent ticketing workflows.

4.1 Project Scope

The Government Helpdesk Portal is designed to function as a secure, scalable, and user-friendly platform that enables government agencies to provide technical and administrative support efficiently. The scope of this project includes:

Core Functionalities:

Issue Tracking & Ticketing System:

- Users can submit IT-related issues, administrative requests, and general inquiries.
- Automated ticket routing based on issue type and priority.
- SLA (Service Level Agreement) monitoring to track response times and issue resolution.

Knowledge Base & Self-Service Portal:

- A repository of FAQs, troubleshooting guides, and government policies.
- AI-powered recommendations to help users find solutions before submitting tickets.
- Multi-language support for diverse government users.

Authentication & Access Control:

- **Multi-Factor Authentication (MFA)** for secure login.
- Role-Based Access Control (RBAC) to **restrict access based on user roles** (e.g., employees, IT admins, government contractors).

Integration with Other Government Systems:

- **Active Directory (AD) integration** for seamless user authentication.
- **Email & SMS notifications** to keep users updated on ticket status.
- **APIs for third-party IT Service Management (ITSM) tools.**

Automation & AI Features:

- **Chatbots for initial support requests**, reducing helpdesk workload.
- **Automated ticket escalation** for high-priority incidents.
- **AI-driven analytics** to identify recurring issues and recommend system improvements.

Compliance & Security Features:

- **Data encryption** (in transit and at rest) to protect sensitive government records.
- **Audit logs & monitoring** for tracking system activities and security events.
- **Compliance with NIST, FISMA, and GDPR** regulations for government IT security.

Exclusions from Scope:

✕ **Non-IT Service Requests:** The portal is not intended for non-technical requests (e.g., HR or payroll inquiries).
✕ **Hardware Asset Management:** This system does not track physical IT assets; it focuses on service request management.

4.2 System Description

The Government Helpdesk Portal is a web-based application hosted on a secure government cloud infrastructure with redundancy and high availability. It is designed for 24/7 accessibility and provides real-time updates on system performance and service requests.

Technical Overview:

- **Architecture:** Cloud-based, scalable, and modular.
- **Hosting:** Hosted on **government-approved cloud platforms** with geo-redundancy.
- **Database:** Encrypted **SQL/NoSQL databases** for secure data storage.
- **User Interface:** Intuitive web and mobile-friendly design.
- **APIs:** RESTful APIs for seamless integration with external systems.
- **Security Framework:** Adheres to **NIST Cybersecurity Standards**, implementing encryption, firewalls, and intrusion detection systems.

Key Components of the System

User Interface (UI):

- A **web-based dashboard** for submitting tickets, tracking issues, and accessing the knowledge base.
- **Mobile-responsive design** for ease of use on smartphones and tablets.

Backend Infrastructure:

- **Centralized database** for secure storage of ticket records and user data.
- **Load balancing and failover mechanisms** to ensure system uptime.
- **Integration with government authentication services** for seamless login.

Security & Compliance Features:

- **Data Encryption:** Uses **AES-256 encryption** to protect user data.
- **Audit Trails:** Logs and tracks all changes and interactions for security auditing.
- **Access Controls:** Implements **RBAC** to define user permissions.

Monitoring & Reporting:

- **Performance monitoring tools** to detect slow response times or system errors.
- **Real-time dashboards** for tracking issue resolution rates.
- **Automated reports** to evaluate helpdesk performance and identify areas for improvement.

Relevance to the Project

The Government Helpdesk Portal is essential for maintaining efficient IT operations within government agencies. The comprehensive ticketing system, automation, and security measures ensure that government employees and citizens receive timely support while maintaining compliance with IT governance policies.

Key Benefits:

- **Reduces downtime** by resolving technical issues efficiently.
- **Enhances user experience** with a self-service knowledge base and automated support.
- **Strengthens cybersecurity** with multi-layered authentication and data encryption.
- **Improves operational efficiency** by automating workflows and integrating with existing systems.By implementing this helpdesk portal, government agencies can streamline IT support processes, enhance data security, and improve overall service delivery, ensuring a responsive and secure digital infrastructure.

5 Risk Management Strategy

The risk management strategy for the Government Helpdesk Portal is a proactive and systematic approach to identifying, assessing, mitigating, and monitoring risks. This strategy ensures that the system operates securely, efficiently, and remains compliant with government regulations.

The key **objectives** of this strategy are:

- **Identifying and mitigating risks** before they disrupt operations.
- **Ensuring compliance** with cybersecurity and data protection laws
- **Minimizing service downtime** and maximizing portal availability.
- **Enhancing security measures** to prevent cyber threats and data breaches.
- **Maintaining continuous monitoring and improvement** of risk controls.

5.1 Risk Management Framework

The risk management framework follows a continuous cycle of risk assessment, response, and monitoring. It includes:

Step 1: Risk Identification

- Conduct risk analysis through **stakeholder interviews, system audits, and security assessments.**
- Categorize risks into **technical, security, operational, compliance, and external risks**.
- Maintain a **Risk Register** to document and track all identified risks.

Step 2: Risk Assessment

- Evaluate risks based on **Likelihood (Low, Medium, High)** and **Impact (Minimal, Moderate, Severe)**.
- Assign a **Risk Priority Score** to focus on **high-risk** areas.

Step 3: Risk Mitigation & Handling

- Develop risk response strategies: **Avoidance, Mitigation, Transfer, or Acceptance**.
- Implement **security controls**, **data protection measures**, and **system redundancies**.

Step 4: Risk Monitoring & Reporting

- Use **automated monitoring tools** to detect security threats and system failures.
- Conduct **periodic risk reviews** and update the **Risk Register**.
- Generate **compliance reports** to track **risk mitigation effectiveness**.

6.1 Risk Identification

This is the first step where potential risks are identified, categorized, and documented.

Key Aspects of Risk Identification:

Risk Sources:

- **Internal**: Server failures, software bugs, lack of trained personnel.
- **External**: Cyberattacks, natural disasters, third-party vulnerabilities.

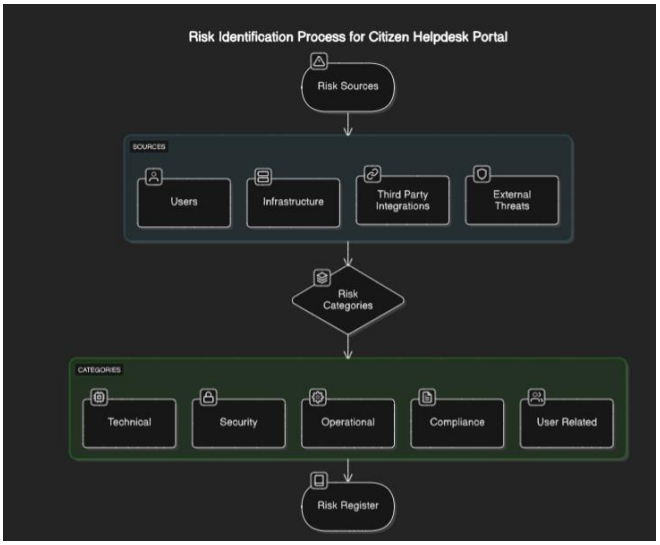
Categorize Risks:

- **Technical Risks**: Server crashes, API failures, integration issues.
- **Security Risks**: Unauthorized access, data breaches, phishing.
- **Operational Risks**: Downtime, lack of staff availability
- **Compliance Risks**: Data privacy violations, regulatory non-compliance.
- **User-Related Risks**: Fraudulent complaints, system misuse.

Document Risks in a Risk Register:

- **Risk ID** (Unique Identifier)
- **Risk Description**
- **Potential Impact**
- **Likelihood of Occurrence**

Diagram: Risk Identification Process



6.2 Risk Assessment

Once risks are identified, they need to be analyzed and prioritized.

Risk Assessment Parameters:

- Likelihood:
- Low (Rare)
- Medium (Possible)
- High (Likely)

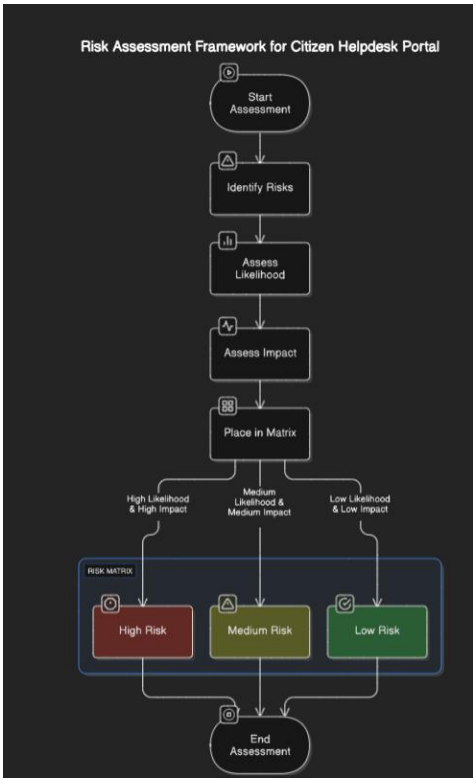
Impact:

- Minor (Minimal effect)
- Moderate (Some disruption)
- Critical (Severe consequences)

Risk Matrix:

- A **5x5 matrix** or **3x3 matrix** plots **Likelihood vs. Impact**
- High likelihood & high impact = **Critical Risk (Needs Immediate Action)**
- Low likelihood & low impact = **Minimal Concern**

Diagram: Risk Assessment Framework



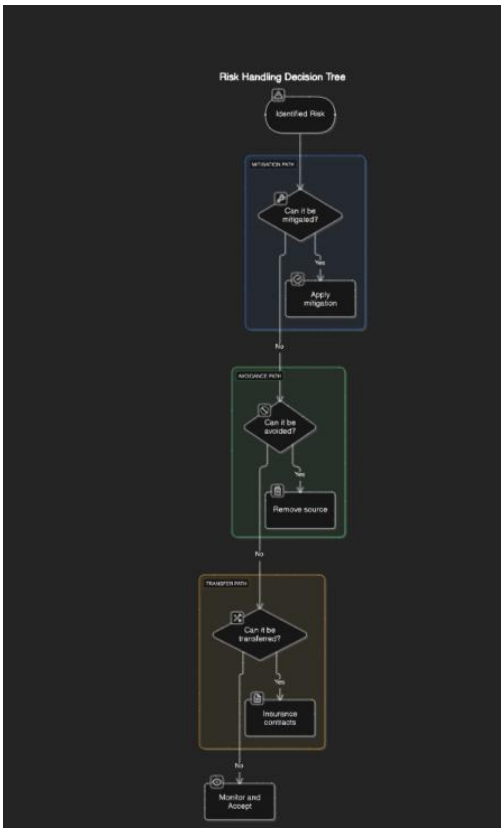
6.3 Risk Handling

Now, we decide what actions to take to reduce or eliminate risks.

Risk Response Strategies:

- **Mitigation** – Reducing risk impact (e.g., Firewalls, Regular Backups).
- **Avoidance** – Eliminating the risk source (e.g., Restricting access to critical systems)
- **Transfer** – Shifting risk responsibility (e.g., Cybersecurity insurance, third-party monitoring services).
- **Acceptance** – Acknowledging the risk but monitoring it.

Diagram: Risk Handling Decision Tree



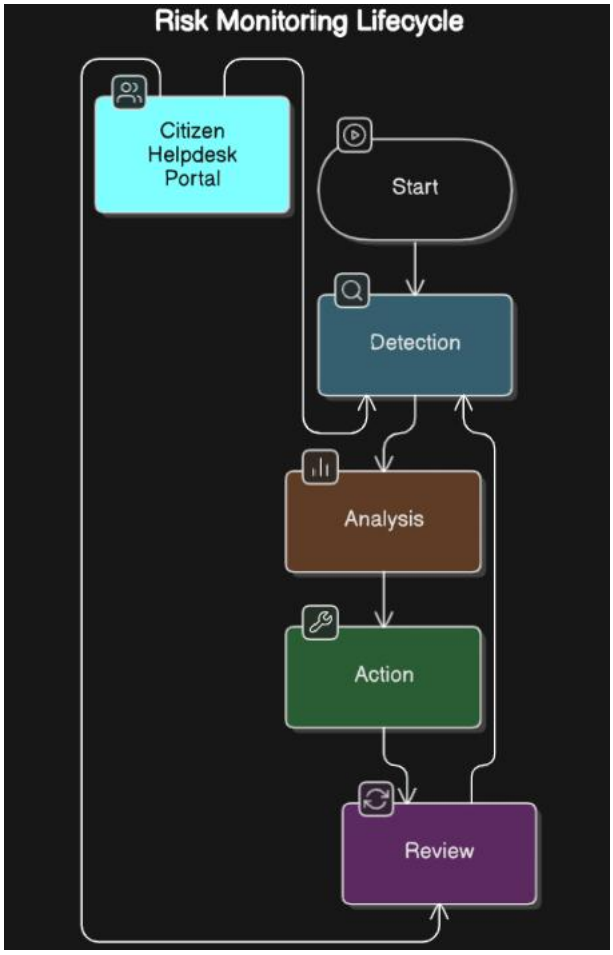
6.4 Risk Monitoring

Risks need to be tracked continuously to prevent issues from escalating.

Key Activities:

- **Automated Logs & Alerts** – Monitor system vulnerabilities.
- **Periodic Audits** – Monthly/Quarterly security assessments.
- **Incident Response Plan** – Steps to handle security breaches.
- **User Feedback Mechanism** – Allow users to report issues.

Diagram: Risk Monitoring Lifecycle



7. Risk Management Roles and Responsibilities

Risk management requires the involvement of multiple stakeholders, each with a clear role in identifying, assessing, and mitigating risks. Below is a structured breakdown of key roles, responsibilities, and their interactions.

7.1 Project Manager

Role: The Project Manager (PM) oversees the entire risk management process and ensures that risk-handling measures align with project goals.

Responsibilities:

- Establishing risk management policies and framework.
- Assigning responsibilities to team members.
- Ensuring risk mitigation measures are implemented.
- Reviewing risk reports and approving corrective actions.
- Communicating risks to higher management and stakeholders.

7.2 Risk Manager

Role: The Risk Manager specializes in identifying, analyzing, and mitigating risks.

Responsibilities:

- Maintaining the **Risk Register** (document listing all identified risks)
- Conducting **risk assessment and prioritization**.
- Coordinating with teams to implement mitigation strategies
- Reporting potential risks to the Project Manager.
- Ensuring compliance with **government regulations** on security and IT governance.

7.3 Project Engineer

Role: The Project Engineer is responsible for identifying and addressing technical risks.

Responsibilities:

- Evaluating vulnerabilities in **software, hardware, and integrations**.
- Developing **technical solutions** for risk mitigation.
- Collaborating with the Risk Manager to ensure compliance with security protocols.
- Implementing failover mechanisms to minimize system downtime.

7.4 Risk Individual Contributor

Role: Team members who actively contribute to risk identification, documentation, and resolution.

Responsibilities:

- Reporting **any identified risks** to the Risk Manager.
- Documenting **incidents, system failures, and near-misses**.
- Assisting with **testing and validation** of risk mitigation strategies
- Providing feedback on risk management policies and suggesting improvements.

7.5 Customer and Stakeholder Participation

Role: Includes **government bodies, external agencies, and end-users** who influence risk decisions and ensure compliance.

Responsibilities:

- Reviewing security **policies and risk assessments**.
- Ensuring the system meets **government standards** (GDPR, ISO 27001, etc.).
- Participating in audits and feedback loops.
- Requesting modifications based on evolving security threats.

7.6 Supplier Participation

Role: External vendors providing cloud services, security software, and other third-party tools.

Responsibilities:

- Ensuring **third-party security compliance**.
- Providing **system updates and patches**.
- Responding to risk incidents affecting vendor-supplied services.
- Collaborating with the Risk Manager on integration risks.

8. Opportunity Management

While risk management focuses on minimizing threats, **opportunity management** identifies ways to enhance the system.

8.1 Identifying Opportunities

Key opportunities in the Government Help Desk Portal include:

- **Enhancing Security** – Implementing AI-based fraud detection.
- **Automation** – Using chatbots for automated ticket resolution.
- **User Experience Improvements** – Adding self-service features.
- **Data Analytics** – Predictive analysis of service requests.

8.2 Evaluating Opportunities

Each identified opportunity is assessed based on:

- **Feasibility** – Can it be implemented within budget and time?
- **Benefit Analysis** – Does it improve efficiency, security, or compliance?
- **Risk vs. Reward** – Does it introduce new risks?

8.3 Executing Opportunities

- **Pilot Programs** – Test features before full deployment.
- **Resource Allocation** – Assign teams and budget.
- **Implementation Strategy** – Define timelines and milestones.

8.4 Monitoring & Reviewing

- To ensure opportunities are effective:
- Track **KPIs (Key Performance Indicators)**.
- Conduct **user feedback surveys**.
- Adjust strategies based on **results and evolving risks**.

User Definitions

A clear definition of system users ensures a shared understanding of roles.

User Role	Definition
End-User	General public or government employees using the help desk portal.
Administrator	IT personnel managing system performance, access, and security.
Auditor	Government officials reviewing security, compliance, and risk reports.
Developer	Engineers responsible for system updates, patches, and security enhancements.

DOCUMENT REVISION HISTORY			
Version Number	**Approved Date**	**Description of Change(s)**	**Created/ Modified By**
1.0	29.03.2025	vAdded Risk Management Plan for Government Helpdesk Portal	Anamitra