7808ICT T1 Project and Cyber Security Management

Assessment 2 – Project Execution Plan (Option 2)

ZeroDay Response Tackles Phishing with ServiceNow

FIGHTING PHISHING FAST WITH ServiceNow
servicenow
Detect. Respond. Protect. All in Record Time.

Prepared by

ZeroDay Response Team, Nathan Campus

Henry Ng, s5423376, (Project Manager and Team Leader)

Minhaj Ahmed, s5419774, (Security Architect)

Ansaf Althaf, s5405482, (Security Engineer)

Sherina Lu, s2717884, (Security Analyst)

02/06/2025

Table of Contents

List of Figures

List of Tables

Section 1. Project Executive Summary

1.1 Project Title and Description

ZeroDay Response Tackles Phishing with ServiceNow

The purpose of this project is to determine how to effectively and efficiently, reduce successful email phishing attacks by at least 50% in the FeatherDrive Flying Car Company.

Within this project, comprehensive and effective technical solutions have been proposed, which include measures such as the implementation of ServiceNow with other security features such as Multi-Factor Authentication (MFA) using Microsoft Authenticator, incident response management and role –based access controls (RBAC). From the non-technical perspective, ZeroDay Response will be seeking to implement more robust and frequent staff training in phishing email detection, utilising a program sourced from KnowBe4. These measures will aim to strengthen the organisation's overall cybersecurity posture as well as increase staff awareness regarding phishing email detection.

1.2 Problem Definition

According to Bhasavar et al. (2018), phishing is defined as malicious actors sending emails that surface-wise seem legitimate and trustworthy to acquire sensitive information and login credentials through various electronic communication platforms including payment services, online or auction sites and social media applications. For this project, ZeroDay Response are specifically focusing on email phishing, which is defined as a cyberattack in which victims are coerced into revealing login credentials or providing sensitive data through emails and malicious links, resulting in outcomes such as password compromise and data theft (Basit et al., 2020).

1.3 Issues and Findings

The proposed solutions of MFA and RBAC entail some issues. MFA presents usability challenges, as users may experience fatigue, due to the complexity of authentication procedures, potentially leading to forgotten credentials or the adoption of weaker, less secure passwords for the sake of convenience (Mukherjee, 2023). Remote access controls are hindered by their limited scalability, particularly as organisational structures evolve (McCarthy, 2025). Likewise, misalignment of roles and permissions can occur, and the ongoing maintenance of access privileges is resource-intensive (McCarthy, 2025). Regarding ServiceNow, there may be some compatibility issues when undertaking the process of integration with existing information technology (IT) systems. Finally, an important factor that bears consideration is that some of the measures proposed may incur significant costs related to software licensing, system integration, ongoing support, and staff training (Halyday, 2022).

1.4 Decision Sought

As a result of the initial project proposal, a decision was made by FeatherDrive Flying Car Company to grant ZeroDay Response permission to proceed with the next phase of the project, implementing ServiceNow with a host of other solutions to reduce email phishing attacks within the organisation.

Section 2. Project Scope and Solution Proposal

2.1 Security Requirement

For this project, it is imperative that the technical measures and solutions for combating email phishing in the organisation firstly meet the triad of security requirements, namely confidentiality, integrity and availability. According to the National Cybersecurity Centre of Excellence (NCCOE) and the National Institute of Standards and Technology (NIST) (2020), confidentiality is defined as ensuring only authorised persons and entities can access and utilise sensitive information. The second part of the triad, integrity, is defined as the process of safeguarding sensitive information against alteration or destruction by unauthorised persons, as well as ensuring the data and systems are trust-worthy, complete and reliable (NCCE & NIST, 2020). Lastly, availability is defined as systems and data being reliably accessible to staff members whenever required, irrespective of circumstances (Hashemi-Pour, 2023, NCCE & NIST, 2020).

Another important security requirement for this project is access control, which is defined as a security mechanism that is designed to restrict and manage access to information and resources in a computing system (Wright, 2024). It is important to note that there are two categories of access control. Firstly, there is physical access control, which, according to Wright (2024), is defined as physically restricting entry to buildings, rooms and IT hardware. Secondly, there is logical access control, which is more commonly defined as restricting access to computer networks, system files, and data (Wright, 2024).

Compliance is the next security requirement for this project. The definition of compliance used herein, is the adherence of an organisation to an established legal, regulatory, and industry-specific standard aimed at safeguarding data privacy (Cyber Management Alliance, 2023). Compliance in a cybersecurity context entails the implementation of technical, operational and administrative controls designed to safeguard data and enhance risk management (Cyber Management Alliance, 2023).

The final security requirement for this project is assurance, which is defined here as the degree of certainty that the design and implementation of an information systems security controls aligns with the prescribed security policy (National Institute of Standards and Technology, 2025).

Adherence to the aforementioned security requirements ensures that the technical measures and solutions implemented to mitigate email phishing incidents within FeatherDrive Flying Car Company are robust, sustainable, and resilient over time, thereby supporting the organisation's continued growth and long-term operational success.

2.2 Conceptual Models of the Solution Proposal

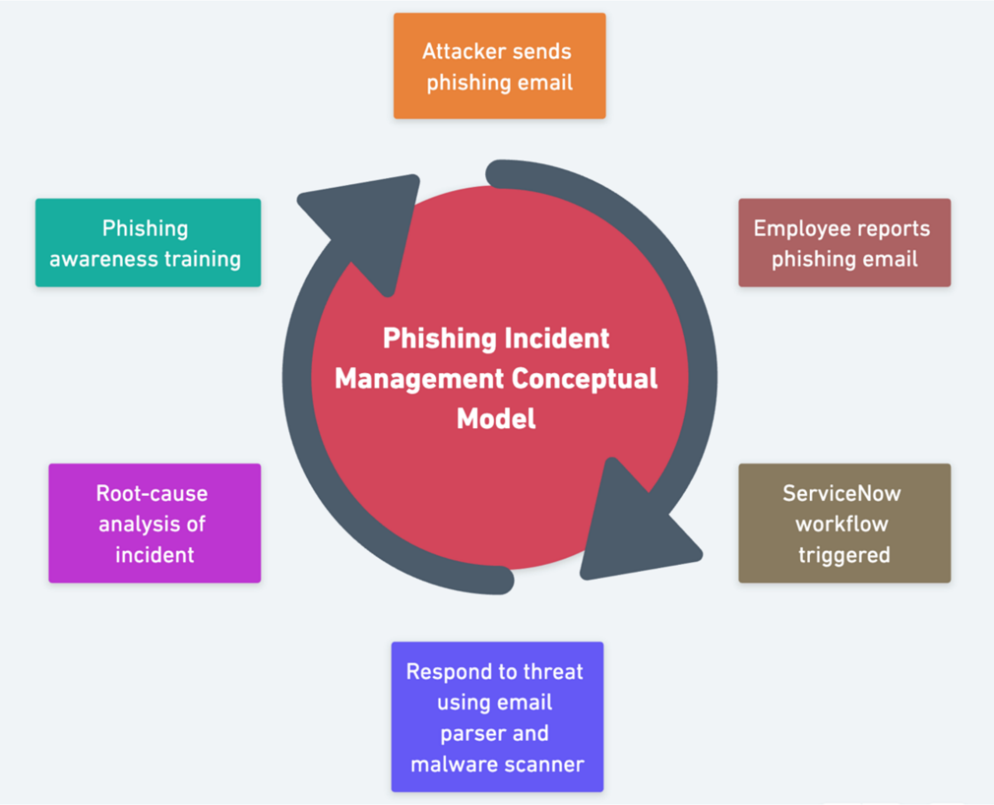

Attacker sends phishing email
Employee reports phishing email
ServiceNow workflow triggered
Respond to threat using email parser and malware scanner
Root-cause analysis of incident
Phishing awareness training
Phishing Incident Management Conceptual Model

Figure 1: Phishing Incident Management Conceptual Model Using ServiceNow

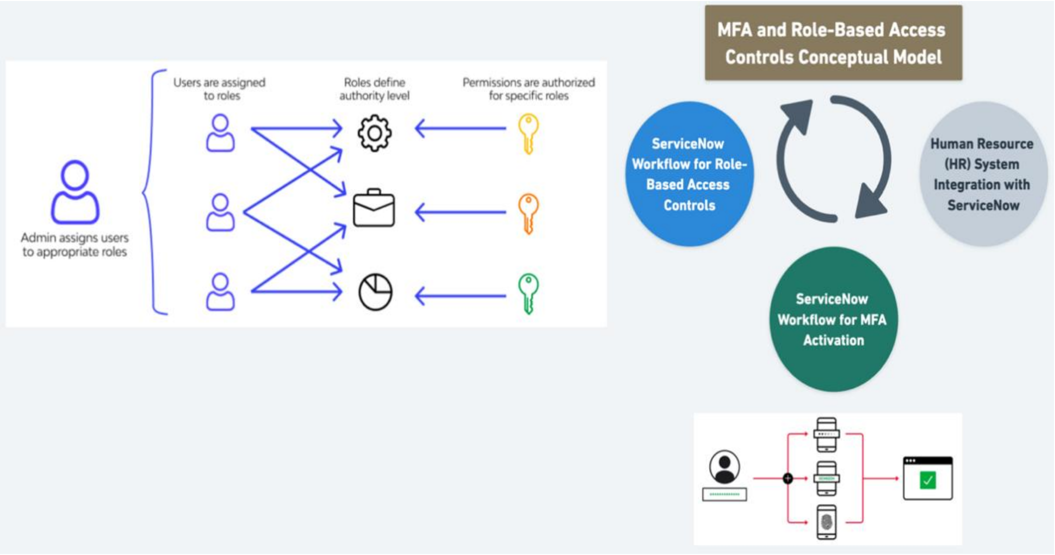

MFA and Role-Based Access Controls Conceptual Model
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles
ServiceNow Workflow for Role-Based Access Controls
Human Resource (HR) System Integration with ServiceNow
ServiceNow Workflow for MFA Activation

Figure 2: MFA and Role-Based Access Controls Conceptual Model Using ServiceNow

2.3 Technologies Underpinning the Solutions Proposed

The technological components that make up the proposed malware scanner are multi-engine scanning, dynamic analysis with sandboxing and cloud infrastructure (VirusTotal, 2024). Multi-engine scanning entails the simultaneous utilisation of multiple anti-malware engines to examine files or systems for potential security threats (Phillips, 2025). Dynamic analysis with sandboxing consists of executing software within a secure, isolated environment (known as a sandbox) to monitor its behaviour and detect potentially malicious activity (Collier, 2022). Cloud infrastructure comprises the integrated hardware, software, and networking components that constitute a cloud computing environment, serving as the foundational framework for the deployment and delivery of cloud-based services (Robinson, 2024).

Email parser is another tool that will be adopted for the project. This is underpinned by Artificial Intelligence (AI), Machine Learning (ML) and Natural Language Processing (NLP) algorithms (McDaniel, 2022). AI denotes the design and development of computer systems capable of executing tasks that traditionally require human intelligence, such as learning, problem-solving and decision-making (Bowman, 2024). ML is a sub-discipline of AI whereby computer systems learn from large datasets and enhance their performance over time to autonomously identify patterns, generate predictions and make informed decisions, without being explicitly programmed (Chen, 2024). NLP is another subfield of AI focused on enabling computer systems to understand, generate, and manipulate human language in a meaningful and contextually appropriate manner (Eppright, 2021).

ServiceNow (integrated with Microsoft MFA and RBAC) is the principal tool to be adopted at FeatherDrive Flying Car Company. The technological foundation of ServiceNow is that it is a primarily cloud-native AI driven platform engineered for enterprise IT service management (ITSM) and workflow automation (ServiceNow, 2025). A cloud-native platform denotes a software development paradigm that capitalises on the core benefits of cloud computing such as scalability, malleability and flexibility to facilitate the design, deployment, and management of contemporary applications (Yasar, 2024).This approach typically incorporates technologies such as microservice architectures, containerisation, and container orchestration frameworks, enabling the development of applications that are resilient, highly scalable, and capable of adapting dynamically to changing demands (Yasar, 2024).

The technology behind Microsoft Authenticator MFA consists of one-time passwords (OTP) or time-based, one-time passwords (TOTP) and push notifications (Terekhov, 2024). OTPs are generated using algorithms that typically rely on event counters (as in HMAC (Hash-based Message Authentication Code) One Time Password (HOTP) or synchronised timestamps (as in Time-based One-Time Password (TOTP) (Gundeti, 2024). Regarding the process of push notifications in MFA, the user is prompted via their registered mobile device to approve or deny authentication requests triggered by login attempts or security-critical operations (Singh, 2025).

RBAC is enabled by technologies such as Identity Governance and Administration (IGA) systems and role definitions tailored to specific applications or systems (Rubeck, 2019). IGA are policy-based solutions that provide a systematic framework for managing digital identities and access rights within organisations (Rubeck, 2023). The IA (Identity Administration) component involves automating user access changes through Human Resource (HR) integration, supporting self-service password management, and enabling federated identity for cross-system access (Rubeck, 2023). Identity Governance (IG) then focuses on enforcing access policies, conducting periodic access reviews, and generating audit reports (Rubeck, 2023).

In regard to role definitions tailored to specific applications, Rubeck (2023) states that it refers to the process of determining a set of assigned permissions that determine the actions a user is authorised to perform in a system or application, a process usually performed by an administrator.

2.4 Techniques and Methods Used

	Techniques	**Methods**
1. Multi-Engine Scanning Implementation	Use several anti-malware engines to find threats (Phillips, 2025).	Set up a system that checks files with different engines to make sure nothing is missed (Phillips, 2025).
2. Dynamic Analysis and Sandboxing	Run suspicious software in a safe environment. Execute potentially malicious	Create a sandbox that observes how the software behaves, looking for harmful actions like changes to files

	software in a controlled environment (Collier, 2022).	or unusual network activity (Collier, 2022).
3. Cloud Infrastructure Utilisation	Use cloud computing for flexibility and storage (Robinson, 2024).	Store and process data in the cloud, keeping malware definitions updated across all scanning engines (Robinson, 2024).
4. AI-Driven Email Parsing	Use AI and language processing to analyse emails (Bowman, 2024; Eppright, 2021).	Train models to assess emails for risks, using language understanding to identify potential threats (Eppright, 2021).
5. ServiceNow Integration	Automate IT service tasks (ServiceNow, 2025d).	Use ServiceNow to streamline the handling of security incidents, connecting it to the malware scanner for quicker responses (ServiceNow, 2025g).
6. MFA with Microsoft Authenticator	Enhance security through MFA (Gundeti, 2024).	Use OTPs and push notifications to ask users for approval when they log in (Gundeti, 2024). This includes using hardware tokens and time-based

		passwords to confirm identity (Gundeti, 2024).
7. RBAC	Control user access based on roles (Rubeck, 2023).	Set specific permissions for what users can do in different applications (Rubeck, 2019). Connect this system to HR tools to automatically adjust access when users change roles (Rubeck, 2023).

Table 1: Techniques and Methods Associated with the Proposed Solutions

2.5 Measurable Outcomes

Strengthened Cybersecurity Posture: Enhance the organisation's cybersecurity stance by reducing vulnerability to email phishing by 50% by the end of 2025, and by 90% by the end of 2026, while also aiming to reduce associated costs by 30%.

Incident Reporting: Produce a detailed report of all phishing incidents encountered by the company, documented in ServiceNow for management review and to identify areas for improvement. Ensure that all incidents from the previous 30 days are displayed on the dashboard for easy access and monitoring.

Streamlined Incident Management: Develop a tailored cyber incident management workflow using ServiceNow to minimise response time to incidents to under a stretch target of 30 minutes as well as quickly restore operations thereafter.

Upgraded Security Infrastructure: Enhance the security infrastructure by integrating new and compatible systems within existing IT frameworks, including the implementation of MFA and RBAC to improve network security through ServiceNow. Aim for 100% resolution of integration bugs by the end of the project.

On-going Training Program: Implement a quarterly training program for all staff that includes phishing simulation tests and refresher courses to reduce the risk of email phishing and other cybersecurity threats.

Section 3. Proof of Concept Demonstrator

3.1 Software to be Used (Name of AI Tools and all Open Sources)

Software Name	**Description**
ServiceNow	A cloud-based ITSM platform that automates and manages incident response, requests, and workflow processes (ServiceNow, 2025f). This will serve as the essential system for tracking phishing and other employee-reported issues by integrating MFA with the company’s existing Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) and Internet of Things (IoT) platforms.

Microsoft Authenticator	An MFA application, in sync with Azure Active Directory (AD) to access accounts securely (Microsoft Support, 2025). It improves login security by requiring users to validate their identity through push notifications, OTP codes, or biometric verification (Microsoft Support, 2025).
Zapier	An automation tool which connects with ServiceNow phishing workflow to automate email parsing from mailboxes (Zapier, 2025). It enables swift responses to incidents by extracting and sending structured data to ServiceNow for analysis and further action/s (Zapier, 2025).
VirusTotal	An open-source threat intelligence service which scans email content, such as files, URLs and IPs, for malicious indicators using antivirus engines and behavioural analysis tools (Microsoft, 2025h). It performs malware scans and threat classifications and extracts reputation data, further enhancing the retaliation process (Microsoft, 2025h).

Table 2: List of Software for the Project Proposal

3.2 Proof of Concept Prototype – Faceplate

ZeroDay Response proposes a prototype design using a combination of security tools and automation to handle phishing incidents and support MFA. The ServiceNow platform incorporates Microsoft Authenticator to facilitate secure access for users using MFA, and workflows have been implemented to enable new users to access MFA and manage troubles accessing MFA. Workflows have been developed to efficiently respond to phishing incidents, integrating Zapier and VirusTotal for enrichment and rapid incident response. The prototype is empowered by these smart and responsive workflows to respond to phishing threats and MFA problems with minimal human involvement. The faceplate designs in this section visually present the integrated workflows and automated processes for handling phishing incidents and MFA support.

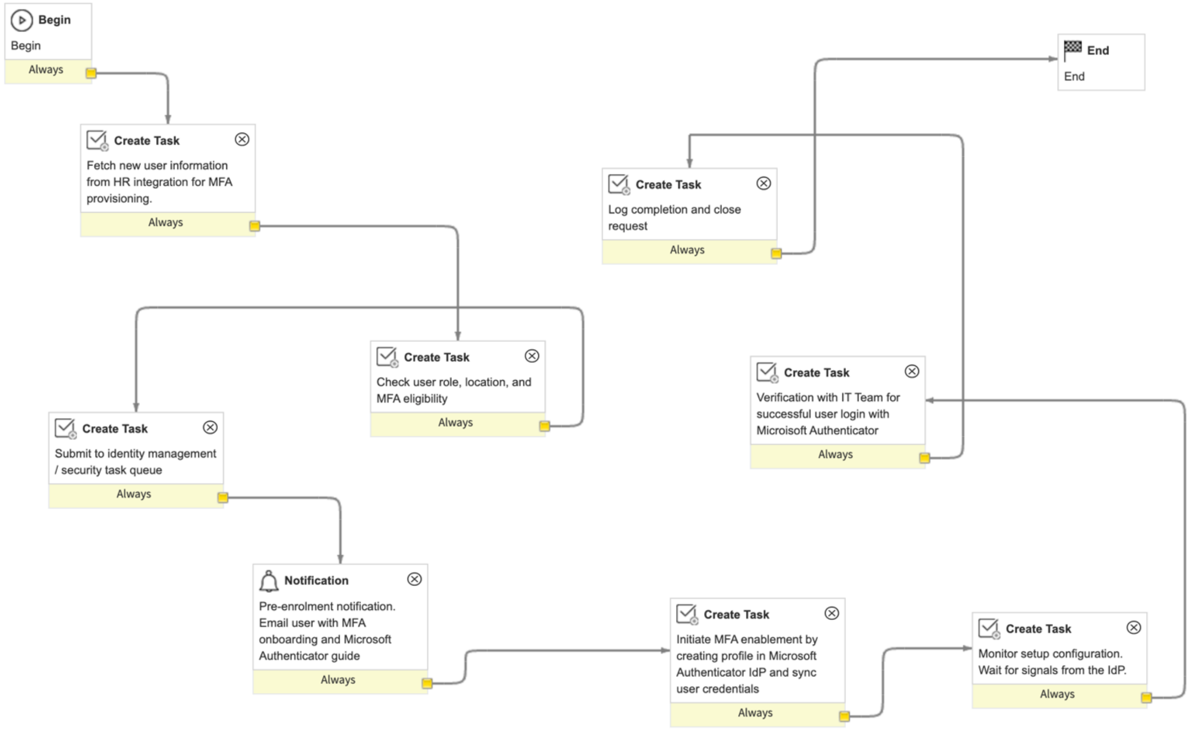

Begin
Begin
Always
Create Task
Fetch new user information from HR integration for MFA provisioning.
Always
Create Task
Check user role, location, and MFA eligibility
Always
Create Task
Submit to identity management / security task queue
Always
Notification
Pre-enrolment notification. Email user with MFA onboarding and Microsoft Authenticator guide
Always
Create Task
Initiate MFA enablement by creating profile in Microsoft Authenticator IdP and sync user credentials
Always
Create Task
Monitor setup configuration. Wait for signals from the IdP.
Always
Create Task
Verification with IT Team for successful user login with Microisoft Authenticator
Always
Create Task
Log completion and close request
Always
End
End

Figure 3: ServiceNow Workflow - Enabling New User with Microsoft Authenticator MFA

Figure 3 demonstrates the workflow in ServiceNow which manages the comprehensive process of enabling Microsoft Authenticator MFA access to a new user. To begin with, the new user's information is extracted from the HR system, and the user's role and eligibility is verified for MFA provisioning. Next, an email notification is automatically sent to the new user, providing the MFA instructions and guide for Microsoft Authenticator. After this, the user profile is created in Microsoft Authenticator Identity Provider (IdP) and the user login credentials are synced with the profile. Subsequently, the confirmation signals in the IdP for the profile setup are monitored and the verification of a successful login is performed by the IT team. Finally, the process details are logged, and the workflow ends by closing the request.

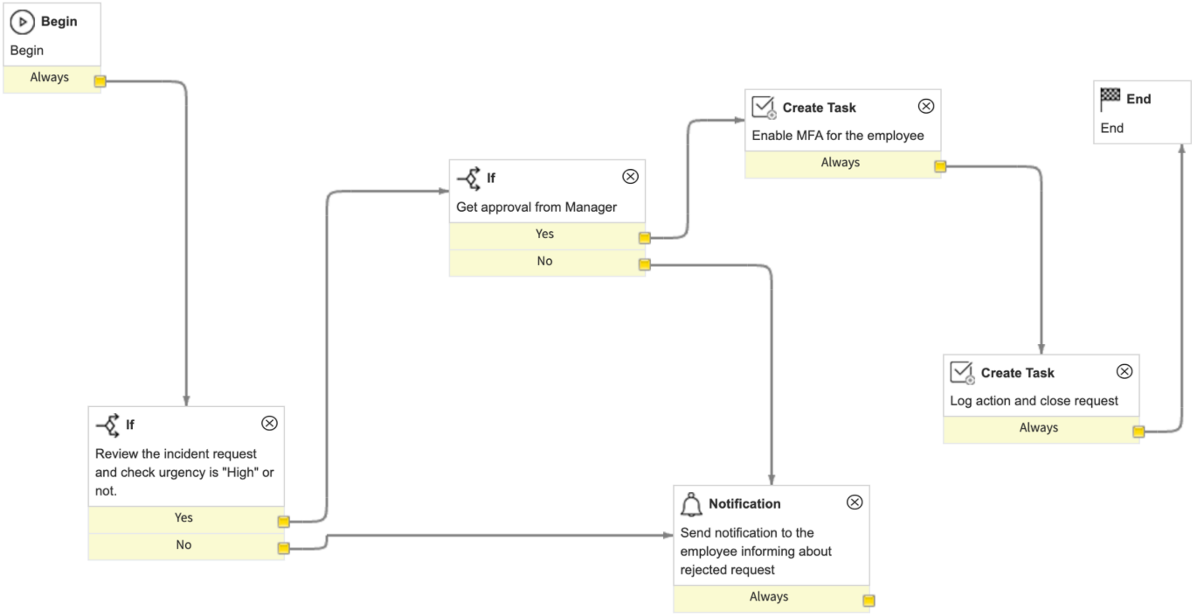

Begin
Begin
Always
If
Review the incident request and check urgency is "High" or not.
Yes
No
If
Get approval from Manager
Yes
No
Create Task
Enable MFA for the employee
Always
Notification
Send notification to the employee informing about rejected request
Always
Create Task
Log action and close request
Always
End
End

Figure 4: ServiceNow Workflow - Employee Unable to Access Systems for an Urgent Task Due to Disabled MFA During the Weekend

Figure 4 illustrates the ServiceNow workflow for responding to urgent requests when an employee cannot access systems as the MFA is disabled during the weekend for security purposes. The workflow begins by reviewing the request and checking whether the urgency has been set to "High" or not. If not, then an automated email is sent to the employee notifying them that their request has been rejected. If the urgency is “High”, then their direct manager’s approval is requested. If their manager disapproves, then the rejection email is sent to the employee. Otherwise, the workflow triggers the action to enable MFA for the employee, facilitating their access to the systems. The workflow concludes by logging the actions and closing the request, ensuring urgent actions and necessary validations are handled during the entire process.

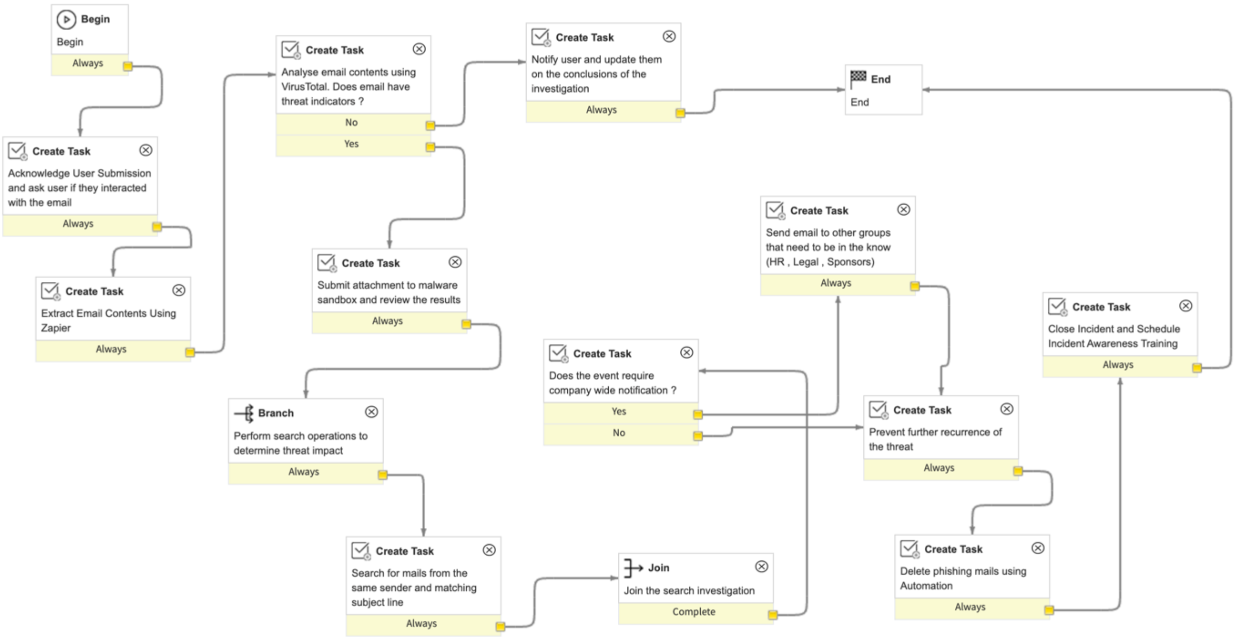

Begin
Begin
Always
Create Task
Acknowledge User Submission and ask user if they interacted with the email
Always
Create Task
Extract Email Contents Using Zapier
Always
Create Task
Analyse email contents using VirusTotal. Does email have threat indicators ?
No
Yes
Create Task
Submit attachment to malware sandbox and review the results
Always
Branch
Perform search operations to determine threat impact
Always
Create Task
Search for mails from the same sender and matching subject line
Always
Join
Join the search investigation
Complete
Create Task
Notify user and update them on the conclusions of the investigation
Always
End
End
Create Task
Does the event require company wide notification ?
Yes
No
Create Task
Send email to other groups that need to be in the know (HR , Legal , Sponsors)
Always
Create Task
Prevent further recurrence of the threat
Always
Create Task
Delete phishing mails using Automation
Always
Create Task
Close Incident and Schedule Incident Awareness Training
Always

Figure 5: ServiceNow Workflow - Phishing Incident Management

The workflow for a phishing incident response is shown in Figure 5. The workflow is triggered by acknowledgement of user incident submission, and the user is asked if they interacted with the email. Next, Zapier is utilised to parse and extract structured data from the suspected phishing email. The extracted data, such as email body, URLs, IPs, are analysed for malware scans and threat indicators using VirusTotal. If there are no threat indicators, then the user is notified of the conclusion of the investigation. If threat indicators are found, then the contents are attached to a malware sandbox, and search operations are conducted to determine the impact. Following this, more emails from the suspected sender are probed and isolated.

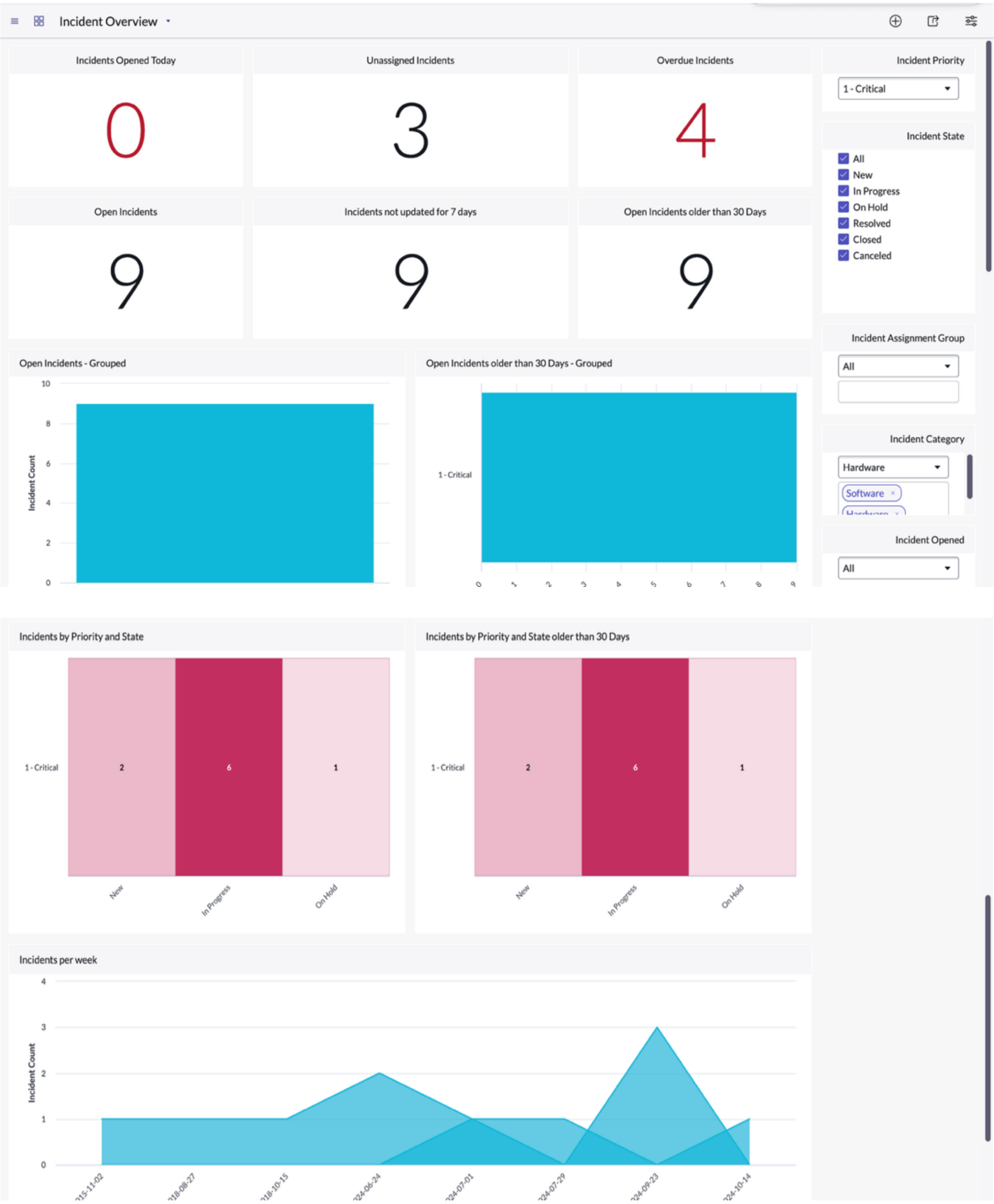
Subsequently, a company-wide notification is released if required, and further recurrence of the threat is prevented. All the phishing emails from the sender are automatically deleted, and the incident is logged. The workflow concludes by closing the request and informing employees of access to security awareness training.

The proposed phishing incident management regime also includes Tier 1 and Tier 2 support. Incidents are automatically routed to Tier 1 for handling low to medium severity incidents, where the security compromise is likely to be very low. Tier 2 is assigned for high to urgent cases, where the compromise is likely to be very high, such as confirmed credential theft or affected systems. Swift detection, analysis, containment, eradication, recovery and post-incident activity is ensured by this comprehensive phishing incident management workflow.

3.3 User Interfaces of the Faceplate

This section exhibits the user interface (UI) layout of the prototype in ServiceNow, which acts as the main point of interaction for employee, security support teams and system administrators. The interfaces presented include, the dashboard, forms for submitting incidents and problems, and knowledge base articles and Frequently Asked Questions (FAQs).

The UIs have been devised to elevate usability and clarity, making sure that the employees and other users are able to navigate and perform their actions with ease. The dashboard provides analytics and summarised insights about phishing incidents and responses. Forms enable employees to submit problems, issues, and articles that provide support for employees with information related to ServiceNow and MFA.



Incident Overview

Incidents Opened Today: 0

Unassigned Incidents: 3

Overdue Incidents: 4

Open Incidents: 9

Incidents not updated for 7 days: 9

Open Incidents older than 30 Days: 9

Incident Priority: 1 - Critical

Incident State:
- ☑ All
- ☑ New
- ☑ In Progress
- ☑ On Hold
- ☑ Resolved
- ☑ Closed
- ☑ Canceled

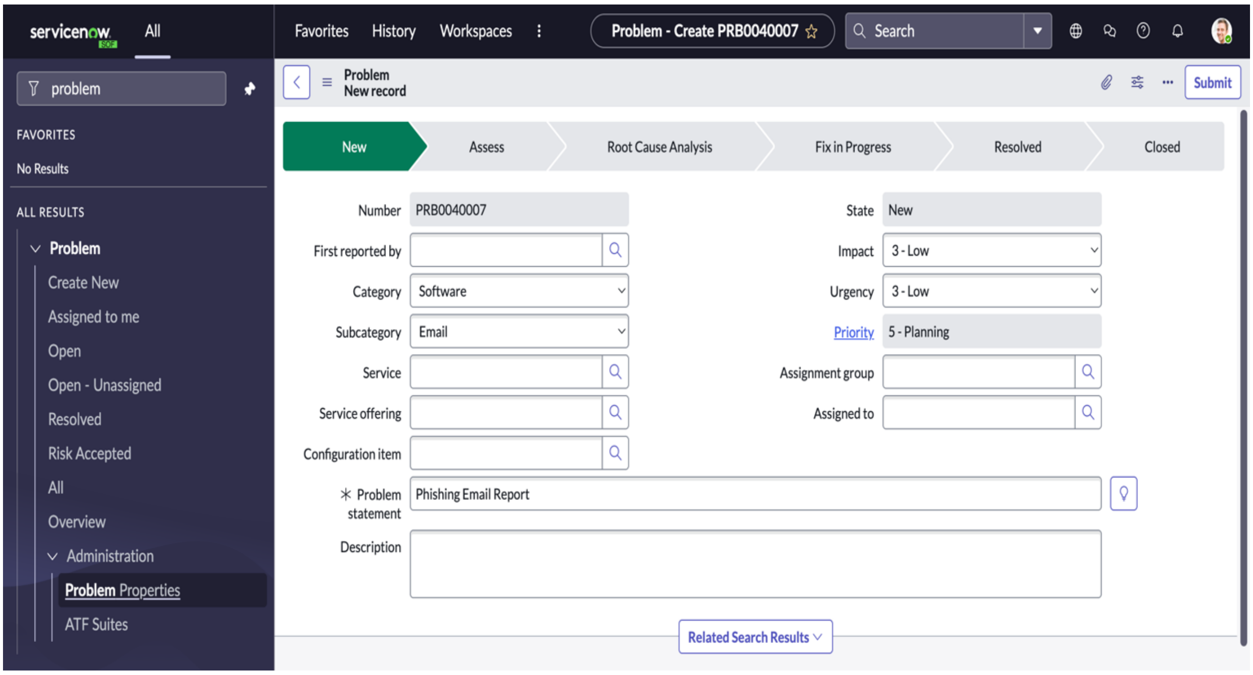
Incident Assignment Group: All

Incident Category: Hardware (Software ×, Hardware ×)

Incident Opened: All

Figure 6: ServiceNow User Interface for Incident Dashboard

Figure 6 demonstrates a prototype of the dashboard user interface providing real-time insights and analytics for incidents in the organisation. The dashboard provides the system administrator with an overview of open and closed incidents, priority-based visualisations, recorded incidents per week, and allows users to filter incidents based on priority and category. The user can click on a widget and explore more information about the analytics. For example: clicking on the “Overdue Incidents” widget navigates the system administrator to a page where all the overdue incidents are listed with all the details. The overall design of the dashboard increases productivity and efficiency of handling incidents for the system administrator and incident management team.

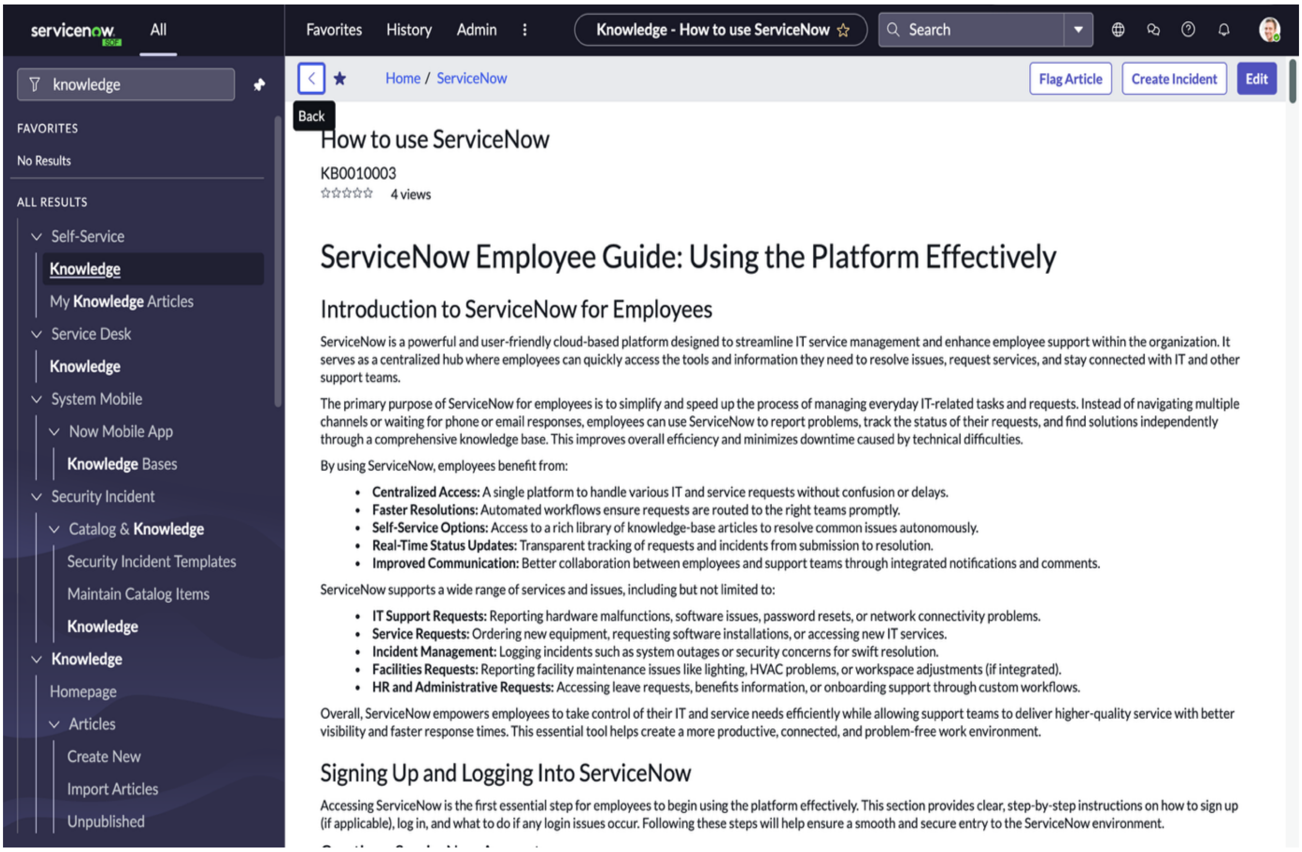


Number	PRB0040007	State	New
First reported by		Impact	3 - Low
Category	Software	Urgency	3 - Low
Subcategory	Email	Priority	5 - Planning
Service		Assignment group	
Service offering		Assigned to	
Configuration item			
* Problem statement	Phishing Email Report		
Description			

Figure 7: ServiceNow User Interface for Forms

Figure 7 shows the form UI for reporting incidents or issues within the ServiceNow Platform. It is accessed by clicking on “Problems -> Create New” tab in the sidebar. The form has the following field inputs which are important for the reporter to fill:

1. Category: Select category of the problem from “Hardware”, “Software”, “Network, and “Database” options.
2. Subcategory: Select a subcategory from options such as “Email” and “operating System”.
3. Impact and Urgency: Highlight the impact and urgency of the issue using “1-High”, “2-Medium”, and “3-Low”.
4. Problem Statement: Provide a short description of the issue. For example: “Reporting phishing incident”.
5. Description: Provide a detailed description of the problem and include attachments



How to use ServiceNow

KB0010003

☆☆☆☆☆ 4 views

ServiceNow Employee Guide: Using the Platform Effectively

Introduction to ServiceNow for Employees

ServiceNow is a powerful and user-friendly cloud-based platform designed to streamline IT service management and enhance employee support within the organization. It serves as a centralized hub where employees can quickly access the tools and information they need to resolve issues, request services, and stay connected with IT and other support teams.

The primary purpose of ServiceNow for employees is to simplify and speed up the process of managing everyday IT-related tasks and requests. Instead of navigating multiple channels or waiting for phone or email responses, employees can use ServiceNow to report problems, track the status of their requests, and find solutions independently through a comprehensive knowledge base. This improves overall efficiency and minimizes downtime caused by technical difficulties.

By using ServiceNow, employees benefit from:

- **Centralized Access:** A single platform to handle various IT and service requests without confusion or delays.
- **Faster Resolutions:** Automated workflows ensure requests are routed to the right teams promptly.
- **Self-Service Options:** Access to a rich library of knowledge-base articles to resolve common issues autonomously.
- **Real-Time Status Updates:** Transparent tracking of requests and incidents from submission to resolution.
- **Improved Communication:** Better collaboration between employees and support teams through integrated notifications and comments.

ServiceNow supports a wide range of services and issues, including but not limited to:

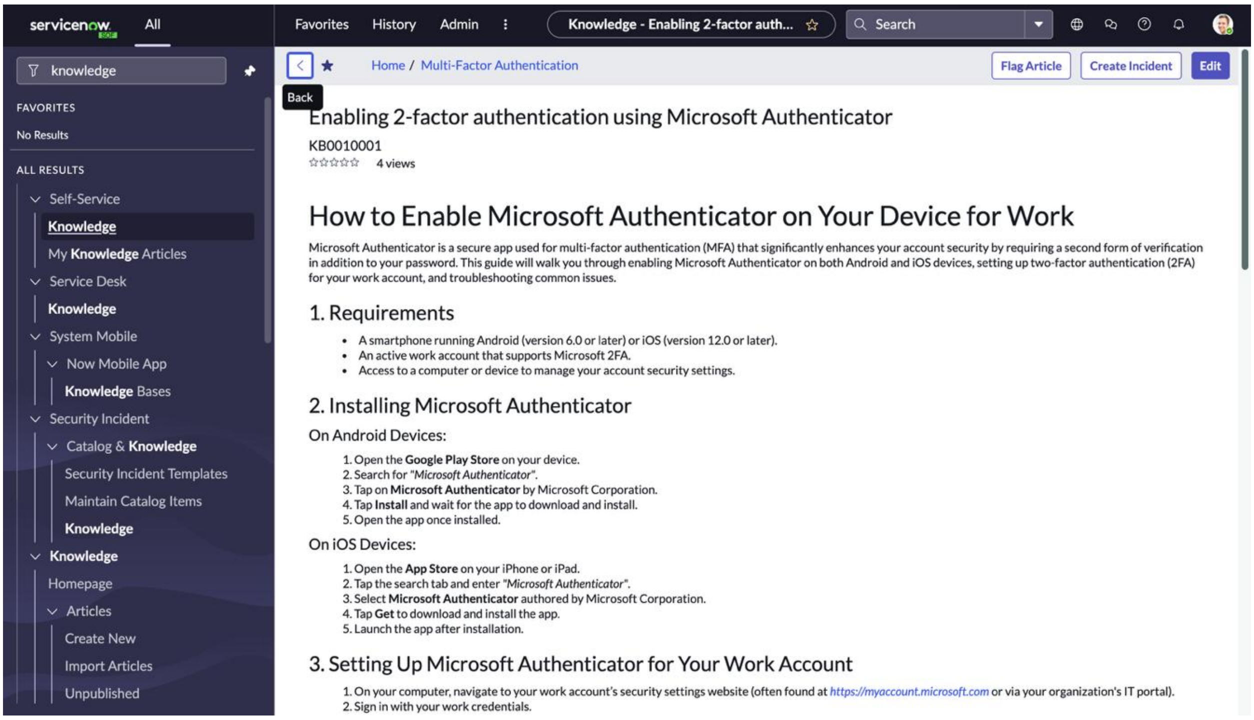
- **IT Support Requests:** Reporting hardware malfunctions, software issues, password resets, or network connectivity problems.
- **Service Requests:** Ordering new equipment, requesting software installations, or accessing new IT services.
- **Incident Management:** Logging incidents such as system outages or security concerns for swift resolution.
- **Facilities Requests:** Reporting facility maintenance issues like lighting, HVAC problems, or workspace adjustments (if integrated).
- **HR and Administrative Requests:** Accessing leave requests, benefits information, or onboarding support through custom workflows.

Overall, ServiceNow empowers employees to take control of their IT and service needs efficiently while allowing support teams to deliver higher-quality service with better visibility and faster response times. This essential tool helps create a more productive, connected, and problem-free work environment.

Signing Up and Logging Into ServiceNow

Accessing ServiceNow is the first essential step for employees to begin using the platform effectively. This section provides clear, step-by-step instructions on how to sign up (if applicable), log in, and what to do if any login issues occur. Following these steps will help ensure a smooth and secure entry to the ServiceNow environment.

Figure 8: ServiceNow User Interface for Self-Support Knowledge Documents



Enabling 2-factor authentication using Microsoft Authenticator

KB0010001

4 views

How to Enable Microsoft Authenticator on Your Device for Work

Microsoft Authenticator is a secure app used for multi-factor authentication (MFA) that significantly enhances your account security by requiring a second form of verification in addition to your password. This guide will walk you through enabling Microsoft Authenticator on both Android and iOS devices, setting up two-factor authentication (2FA) for your work account, and troubleshooting common issues.

1. Requirements

- A smartphone running Android (version 6.0 or later) or iOS (version 12.0 or later).
- An active work account that supports Microsoft 2FA.
- Access to a computer or device to manage your account security settings.

2. Installing Microsoft Authenticator

On Android Devices:

1. Open the **Google Play Store** on your device.
2. Search for "*Microsoft Authenticator*".
3. Tap on **Microsoft Authenticator** by Microsoft Corporation.
4. Tap **Install** and wait for the app to download and install.
5. Open the app once installed.

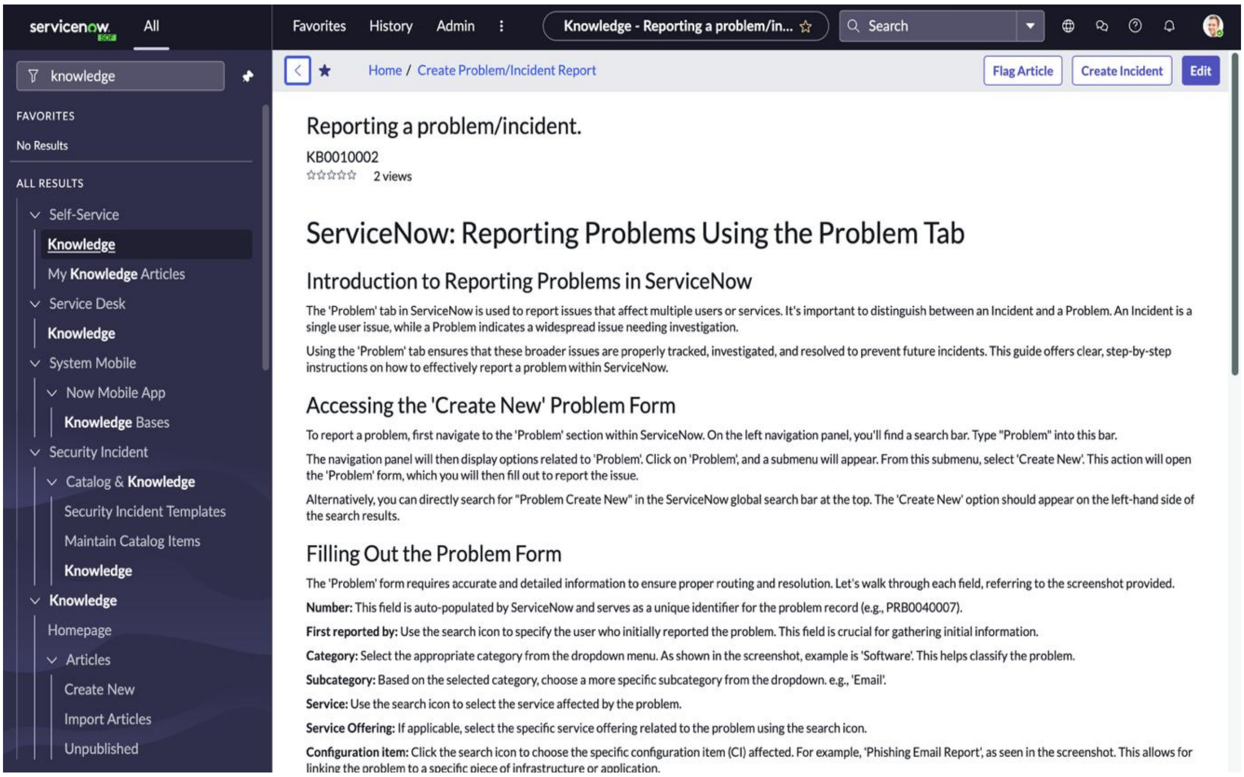
On iOS Devices:

1. Open the **App Store** on your iPhone or iPad.
2. Tap the search tab and enter "*Microsoft Authenticator*".
3. Select **Microsoft Authenticator** authored by Microsoft Corporation.
4. Tap **Get** to download and install the app.
5. Launch the app after installation.

3. Setting Up Microsoft Authenticator for Your Work Account

1. On your computer, navigate to your work account's security settings website (often found at *https://myaccount.microsoft.com* or via your organization's IT portal).
2. Sign in with your work credentials.

Figure 9: ServiceNow User Interface for Self-Support Knowledge Document - Multi-Factor Authentication using Microsoft Authenticator



Reporting a problem/incident.

KB0010002

2 views

ServiceNow: Reporting Problems Using the Problem Tab

Introduction to Reporting Problems in ServiceNow

The 'Problem' tab in ServiceNow is used to report issues that affect multiple users or services. It's important to distinguish between an Incident and a Problem. An Incident is a single user issue, while a Problem indicates a widespread issue needing investigation.

Using the 'Problem' tab ensures that these broader issues are properly tracked, investigated, and resolved to prevent future incidents. This guide offers clear, step-by-step instructions on how to effectively report a problem within ServiceNow.

Accessing the 'Create New' Problem Form

To report a problem, first navigate to the 'Problem' section within ServiceNow. On the left navigation panel, you'll find a search bar. Type "Problem" into this bar.

The navigation panel will then display options related to 'Problem'. Click on 'Problem', and a submenu will appear. From this submenu, select 'Create New'. This action will open the 'Problem' form, which you will then fill out to report the issue.

Alternatively, you can directly search for "Problem Create New" in the ServiceNow global search bar at the top. The 'Create New' option should appear on the left-hand side of the search results.

Filling Out the Problem Form

The 'Problem' form requires accurate and detailed information to ensure proper routing and resolution. Let's walk through each field, referring to the screenshot provided.

Number: This field is auto-populated by ServiceNow and serves as a unique identifier for the problem record (e.g., PRB0040007).

First reported by: Use the search icon to specify the user who initially reported the problem. This field is crucial for gathering initial information.

Category: Select the appropriate category from the dropdown menu. As shown in the screenshot, example is 'Software'. This helps classify the problem.

Subcategory: Based on the selected category, choose a more specific subcategory from the dropdown. e.g., 'Email'.

Service: Use the search icon to select the service affected by the problem.

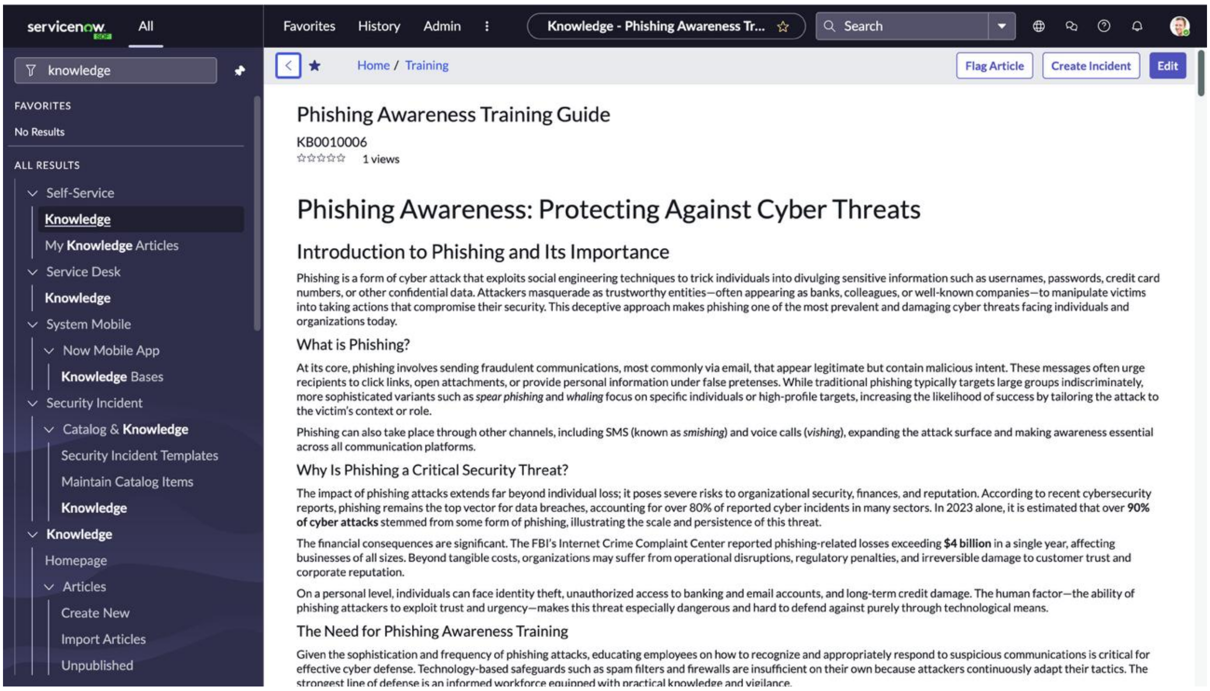
Service Offering: If applicable, select the specific service offering related to the problem using the search icon.

Configuration item: Click the search icon to choose the specific configuration item (CI) affected. For example, 'Phishing Email Report', as seen in the screenshot. This allows for linking the problem to a specific piece of infrastructure or application.

Figure 10: ServiceNow User Interface for Self-Support Knowledge Document - Reporting Incidents using Forms

Figures 8, 9, and 10 demonstrate helpful knowledge documents and other material which would be accessible to the users in the new implementation. These documents, found under the “Knowledge” tab, would guide users to navigate and understand the ServiceNow platform, navigate around dashboards, and enable easier reporting of problems and incidents. As demonstrated by Figure 10, the “Enabling 2-factor authentication using Microsoft Authenticator” document would direct the employees to set up Microsoft Authenticator on their devices, sync with their login credentials, and deal with common MFA issues.

A primary facet of the solution involves improving the phishing awareness among employees to create a strong, robust culture and a security-first mindset at FeatherDrive Flying Cars. A “Phishing Awareness” training manual is to be developed (Figure 11) to facilitate the training program. This would include an introduction to phishing and its security threats, types of phishing attacks and the necessity of phishing awareness training. Moreover, it would be comprised of common threat indicators, detection techniques, and reporting methods for phishing. A security training team would be delegated with the responsibility of conducting quarterly training sessions to cover this content and provide real-world phishing examples to raise awareness amongst the employees.



Phishing Awareness Training Guide

KB0010006

☆☆☆☆☆ 1 views

Phishing Awareness: Protecting Against Cyber Threats

Introduction to Phishing and Its Importance

Phishing is a form of cyber attack that exploits social engineering techniques to trick individuals into divulging sensitive information such as usernames, passwords, credit card numbers, or other confidential data. Attackers masquerade as trustworthy entities—often appearing as banks, colleagues, or well-known companies—to manipulate victims into taking actions that compromise their security. This deceptive approach makes phishing one of the most prevalent and damaging cyber threats facing individuals and organizations today.

What is Phishing?

At its core, phishing involves sending fraudulent communications, most commonly via email, that appear legitimate but contain malicious intent. These messages often urge recipients to click links, open attachments, or provide personal information under false pretenses. While traditional phishing typically targets large groups indiscriminately, more sophisticated variants such as *spear phishing* and *whaling* focus on specific individuals or high-profile targets, increasing the likelihood of success by tailoring the attack to the victim's context or role.

Phishing can also take place through other channels, including SMS (known as *smishing*) and voice calls (*vishing*), expanding the attack surface and making awareness essential across all communication platforms.

Why Is Phishing a Critical Security Threat?

The impact of phishing attacks extends far beyond individual loss; it poses severe risks to organizational security, finances, and reputation. According to recent cybersecurity reports, phishing remains the top vector for data breaches, accounting for over 80% of reported cyber incidents in many sectors. In 2023 alone, it is estimated that over **90% of cyber attacks** stemmed from some form of phishing, illustrating the scale and persistence of this threat.

The financial consequences are significant. The FBI's Internet Crime Complaint Center reported phishing-related losses exceeding **$4 billion** in a single year, affecting businesses of all sizes. Beyond tangible costs, organizations may suffer from operational disruptions, regulatory penalties, and irreversible damage to customer trust and corporate reputation.

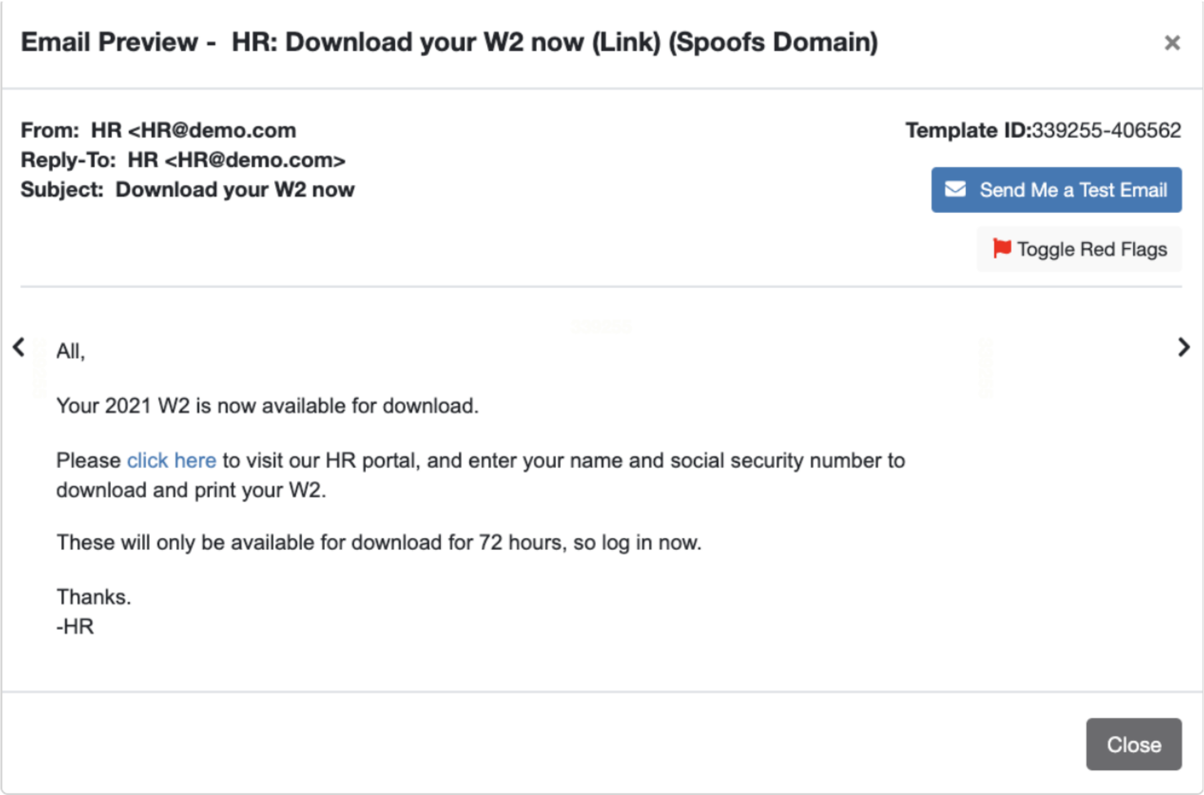
On a personal level, individuals can face identity theft, unauthorized access to banking and email accounts, and long-term credit damage. The human factor—the ability of phishing attackers to exploit trust and urgency—makes this threat especially dangerous and hard to defend against purely through technological means.

The Need for Phishing Awareness Training

Given the sophistication and frequency of phishing attacks, educating employees on how to recognize and appropriately respond to suspicious communications is critical for effective cyber defense. Technology-based safeguards such as spam filters and firewalls are insufficient on their own because attackers continuously adapt their tactics. The strongest line of defense is an informed workforce equipped with practical knowledge and vigilance.

Figure 11: ServiceNow User Interface for Phishing Awareness Training Guide

ServiceNow offers integration with KnowBe4 to conduct phishing simulation tests (ServiceNow, 2024). The solution leverages this integration to conduct a Phishing Security Test (PST) in KnowBe4, which would assist in evaluating the level of awareness amongst the employees and how susceptible they are to phishing attacks (KnowBe4, 2025c). This operates by sending phishing emails to the employees, prompting them to click embedded links and URLs (KnowBe4, 2025c), as shown in Figure 12. If the employees click the link, it navigates them to a landing page to inform the that they have failed the phishing simulation test (KnowBe4, 2025c). The PST test results are integrated within the ServiceNow dashboard to allow the security teams and senior management to identify areas of weakness and allocate required training to address these weaknesses (ServiceNow, 2024).



Email Preview - HR: Download your W2 now (Link) (Spoofs Domain)
×
Send Me a Test Email
Toggle Red Flags
Close

From: HR <HR@demo.com
Reply-To: HR <HR@demo.com>
Subject: Download your W2 now

Template ID:339255-406562

All,

Your 2021 W2 is now available for download.

Please click here to visit our HR portal, and enter your name and social security number to download and print your W2.

These will only be available for download for 72 hours, so log in now.

Thanks.
-HR

Figure 12: Example of a Simulated Phishing Email Test

From *Phishing Security Test (PST) Overview* by KnowBe4, 2025b,(*https://support.knowbe4.com/hc/en-us/articles/236271227-Phishing-Security-Test-PST-Overview)*

3.4 System Interfaces with Existing IT Environments

The proposed solution with ServiceNow is designed to act as a core component in the seamless integration of other IT systems in FeatherDrive Flying Car Company and be deployed as a centralised IT service management platform. One of the primary benefits of ServiceNow is its ability to communicate and coordinate with a variety of other systems from different vendors, and the solution leverages this feature by integrating ServiceNow with the company's IT systems, CRM, ERP, and IoT platforms (ServiceNow, 2025g). This interface would enable FeatherDrive Flying Cars management to obtain a higher operational efficiency, improve data management, and achieve better decision-making from within a single platform.

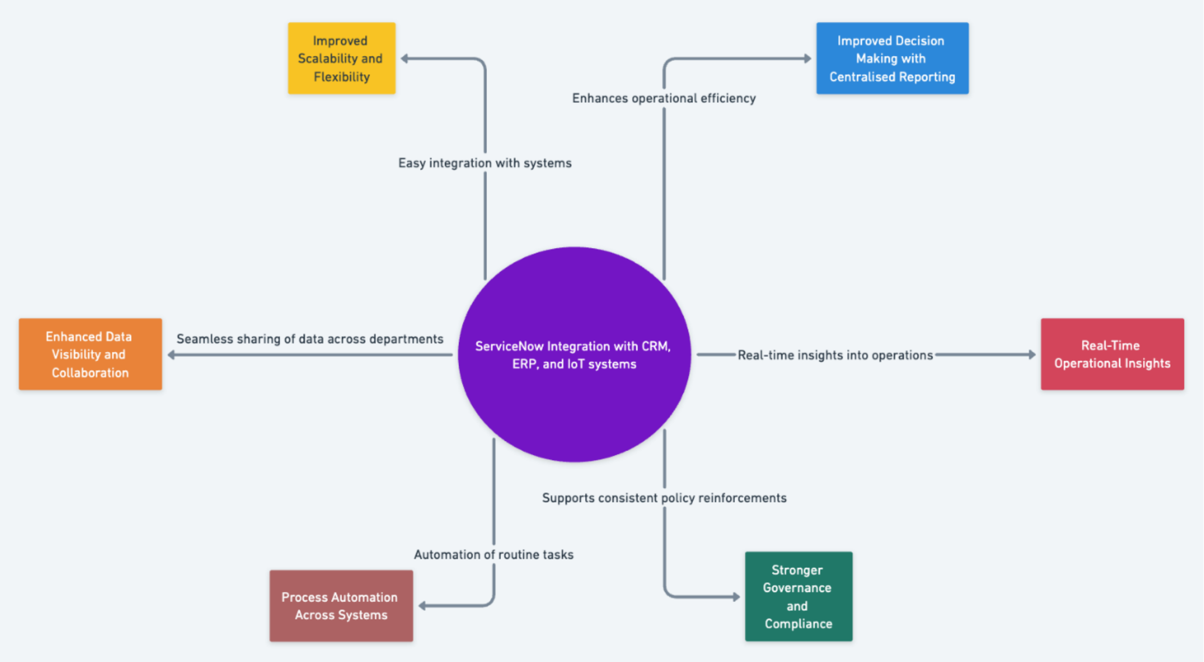

Improved Scalability and Flexibility
Improved Decision Making with Centralised Reporting
Enhances operational efficiency
Easy integration with systems
Enhanced Data Visibility and Collaboration
Seamless sharing of data across departments
ServiceNow Integration with CRM, ERP, and IoT systems
Real-time insights into operations
Real-Time Operational Insights
Supports consistent policy reinforcements
Automation of routine tasks
Process Automation Across Systems
Stronger Governance and Compliance

Figure 13: Leveraging Systems Integration in ServiceNow

Figure 13 illustrates the benefits of leveraging ServiceNow integration with the company's existing systems. This unified hub simplifies the sharing and coordination of customer, inventory and financial data across departments through the links created with CRM and ERP systems. This improves cross-functional team collaboration (IT, HR, Finance, Operations) and encourages smoother workflows for enhanced output and productivity (ServiceNow, 2025). This integration also allows automation of routine tasks across systems such as approvals and regular updates using triggered workflows at regular intervals, reducing time to perform tasks and manual entries (Ezenduka, 2024).

The integration interface would provide connection and real-time status updates from IoT platforms and valuable analytics into device performance, condition and availability (ServiceNow, 2025f). These insights would allow IT teams to be proactive and allocate resources efficiently to increase optimisation and effective operational performance

(Ezenduka, 2024). Additionally, with the implementation of the integration, ServiceNow analyses data from various systems and collects them into one centralised dashboard interface, allowing management to easily access insights and reports from different departments with regular updates to make more timely and informed decisions (Ezenduka, 2024).

Further benefits of this integration interface include higher scalability and flexibility, as ServiceNow offers flexible architecture to easily integrate with new systems (Ezenduka, 2024). The interface would remain adaptable to more systems, operations, and departments as the company continues to evolve. FeatherDrive Flying Cars would also be able to enforce stronger and consistent governance and compliance with the implementation of the systems integration interface in ServiceNow and gather all data into one hub. Monitoring of all data processes and interactions would be simpler to ensure the processes comply with the regulatory requirements and internal standards, reducing the chances of data policy breach.

3.5 Data Management

Secured, regulated and transparent management of data is a primary objective of our proposed solution, and our prototype with ServiceNow brings a secure and policy-driven approach to ensure this (ServiceNow, 2025b). Data integrity, confidentiality, and availability is central to the organisational goals of FeatherDrive Flying Cars. Our approach, with RBAC, data encryption, policy, compliance and risk management, and quality of data, as described in Figure 14, ensures the new framework meets the organisation’s standards.

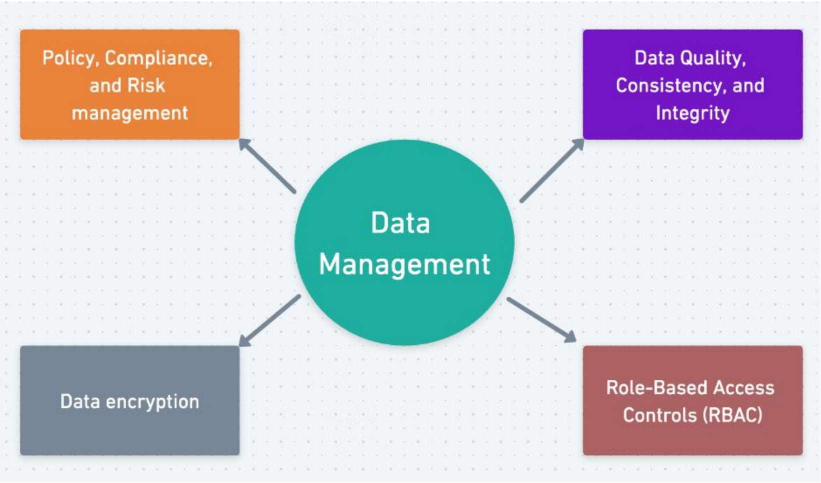

Policy, Compliance, and Risk management
Data Quality, Consistency, and Integrity
Data Management
Data encryption
Role-Based Access Controls (RBAC)

Figure 14: Data Management Approach and Policies with ServiceNow

Role-Based Access Controls (RBAC) is an essential function in the data protection strategy. ServiceNow allows implementation of RBAC by providing access to data and systems strictly based on the defined roles of the employees in the organisation (Lundqvist, 2025). The user roles are clearly articulated and are only granted access to the data and systems that are necessary for their tasks (Lundqvist, 2025). Applying these controls would prevent unauthorised access to data and reduce the risk of threats from within the company. The role management is automated with the usage of workflows within ServiceNow, which is integrated with the HR system and triggered whenever there are changes in the employee structure. RBAC is regularly monitored and audited to validate appropriate access and identify any issues, with quarterly assessments and review of user roles to be conducted to ensure that the employees are assigned with correct access and any changes in roles are adjusted. The entire process is described in Figure 15.

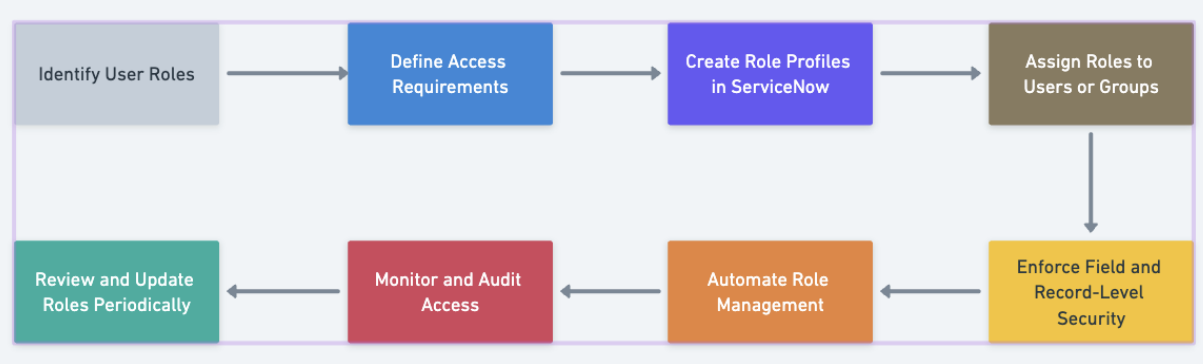

Identify User Roles
Define Access Requirements
Create Role Profiles in ServiceNow
Assign Roles to Users or Groups
Enforce Field and Record-Level Security
Automate Role Management
Monitor and Audit Access
Review and Update Roles Periodically

Figure 15: Role-Based Access Controls (RBAC) Implementation using ServiceNow

The prototype also provides data encryption to secure sensitive data in rest or in communication process, ensuring confidentiality during the process. The ServiceNow platform uses the benefits of HTTPS protocols and robust encryption standards such as AES-256 to ensure that the data is protected (ServiceNow, 2025). Data quality, accuracy, and integrity is also ensured through maintaining standardised formats for data entry and storage. The consistency of data is ensured by the integration and coordination of existing systems in the company such as CRM, ERP, and IoT systems into one interface.

A key segment of the data management process also involves policy and compliance management. ServiceNow provides this management service by automating best practice lifecycles and combining compliance processes to ensure the framework meets the required standards (ServiceNow, 2025c). The prototype would build policy and governance frameworks into the system, enabling continuous risk monitoring through alerts and risk scores (ServiceNow, 2025e).

All these features merge to shape a comprehensive approach to data management in the proposed solution using ServiceNow, empowering FeatherDrive Flying Car Company with a strong foundation to operate business functions effectively and efficiently.

Section 4. Project Team, Tasks and Schedule

4.1 Team Organisation

The team consists of four members, each of whom are assigned with different roles based on technical competencies and communication responsibilities.

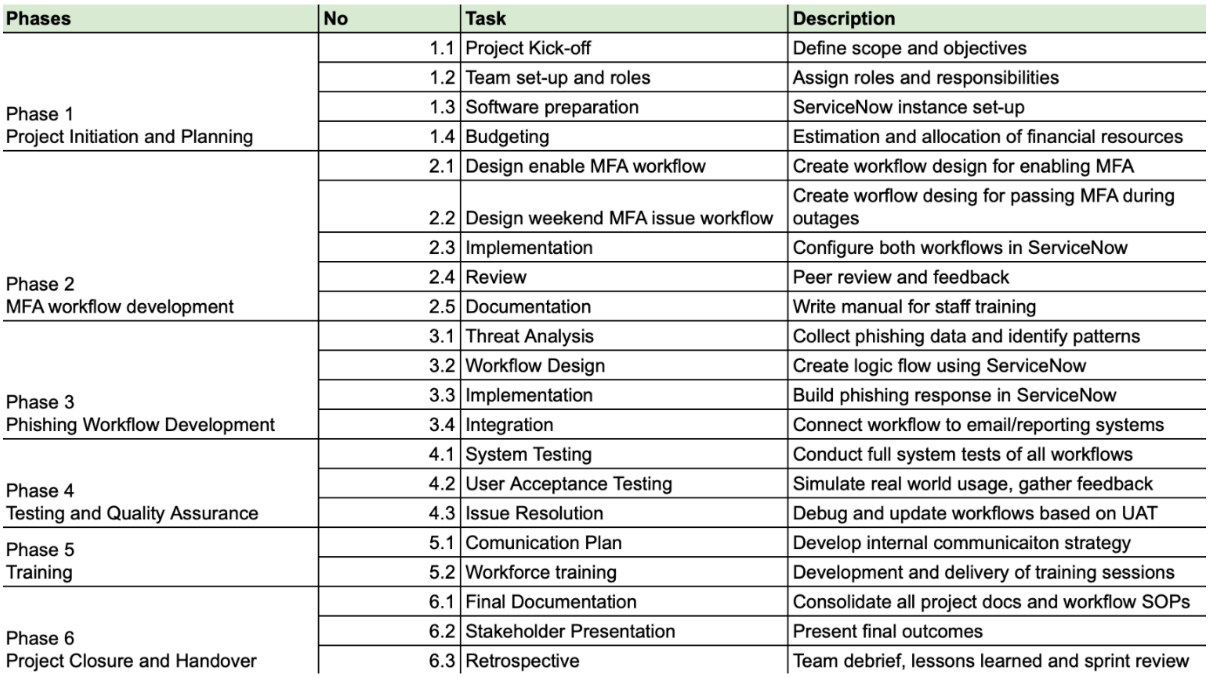
Led by Henry Ng, our team leader and project manager, who is responsible for overall project delivery, stakeholder communication, team coordination, and timeline adherence.

Minhaj Ahmed, our security architect**,** designs the security framework and technical architecture of the MFA and phishing workflows in ServiceNow.

Ansaf Althaf, our security engineer, implements and configures the workflows in the ServiceNow environment based on the designs provided by the security architect. He then conducts testing, debugging, and documentation of technical components.

And finally, Sherina Lu, our security analyst, conducts phishing and MFA incident data analysis to identify threat patterns and contributes to logic development within the phishing response workflow.

4.2 Work Breakdown Structure



Phases	No	Task	Description
Phase 1 Project Initiation and Planning	1.1	Project Kick-off	Define scope and objectives
	1.2	Team set-up and roles	Assign roles and responsibilities
	1.3	Software preparation	ServiceNow instance set-up
	1.4	Budgeting	Estimation and allocation of financial resources
Phase 2 MFA workflow development	2.1	Design enable MFA workflow	Create workflow design for enabling MFA
	2.2	Design weekend MFA issue workflow	Create worflow desing for passing MFA during outages
	2.3	Implementation	Configure both workflows in ServiceNow
	2.4	Review	Peer review and feedback
	2.5	Documentation	Write manual for staff training
Phase 3 Phishing Workflow Development	3.1	Threat Analysis	Collect phishing data and identify patterns
	3.2	Workflow Design	Create logic flow using ServiceNow
	3.3	Implementation	Build phishing response in ServiceNow
	3.4	Integration	Connect workflow to email/reporting systems
Phase 4 Testing and Quality Assurance	4.1	System Testing	Conduct full system tests of all workflows
	4.2	User Acceptance Testing	Simulate real world usage, gather feedback
	4.3	Issue Resolution	Debug and update workflows based on UAT
Phase 5 Training	5.1	Comunication Plan	Develop internal communicaiton strategy
	5.2	Workforce training	Development and delivery of training sessions
Phase 6 Project Closure and Handover	6.1	Final Documentation	Consolidate all project docs and workflow SOPs
	6.2	Stakeholder Presentation	Present final outcomes
	6.3	Retrospective	Team debrief, lessons learned and sprint review

Table 3: Work Break Down Structure

The project is divided into five structured phases: Initiation & Planning, MFA Workflow Development, Phishing Workflow Development, Testing & QA, and Project Closure. Each phase is broken down into specific activities and subtasks assigned to individual team members based on their roles and technical expertise.

In the Initiation phase, Henry Ng establishes the scope, assigns roles, and prepares the ServiceNow environment. The MFA Workflow Development phase includes designing and implementing two workflows: one for enabling MFA and another for handling access issues during weekends. Minhaj Ahmed leads the design work, while Ansaf Althaf handles implementation and documentation.

The Phishing Workflow Development phase involves identifying phishing patterns (Sherina Lu), designing response logic (Minhaj Ahmed), and configuring workflows (Ansaf Althaf). Integration and testing follow, with Sherina performing scenario-based validation.

Testing and QA spans both sets of phishing and MFA workflows, including system testing, user acceptance testing, and issue resolution. The final phase includes documentation, stakeholder presentation, and a team retrospective.

4.3 Key Deliverables, Milestones and Timelines

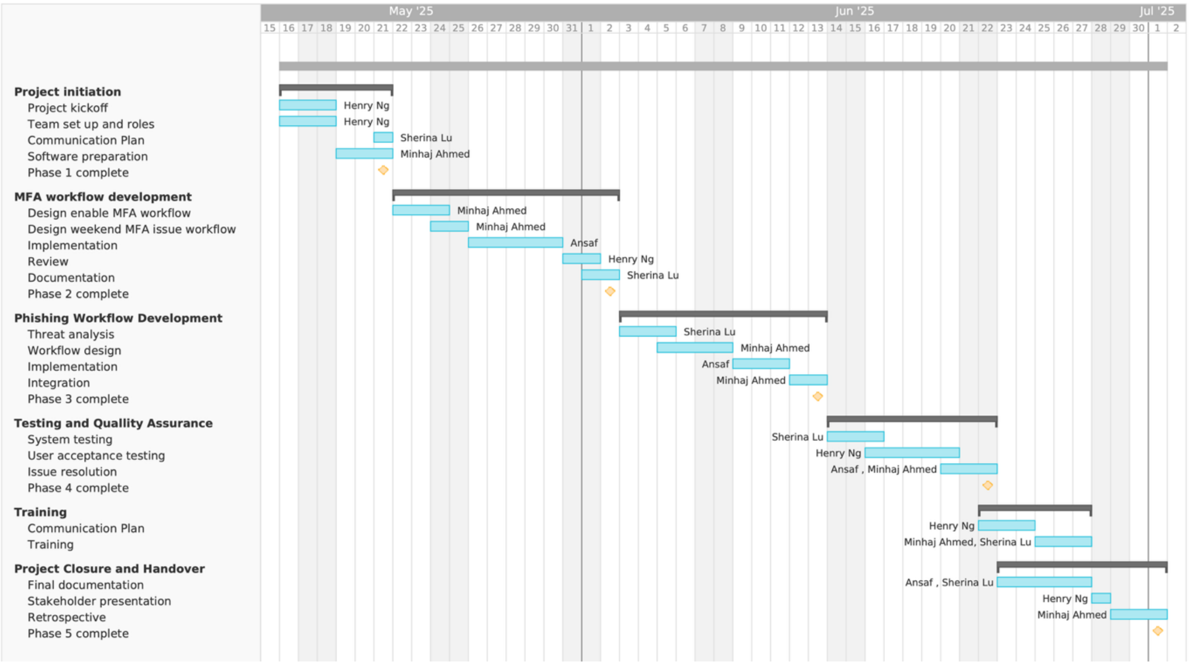


Figure 16: Gnatt Table Representing the Timeline of Project Tasks

The project is structured across five phases with clearly defined deliverables and milestones. Each phase ends in a milestone marked as a yellow point in the chart. Key deliverables are, finalised MFA workflow designs (Phase 2), completed phishing detection and response workflow (Phase 3), and tested/validated ServiceNow automation processes (Phase 4). Final project documentation and stakeholder presentation (Phase 5) marks the project closure. The project timeline spans 12 weeks from project initiation to handover, with some tasks overlapping to maximise efficiency.

4.4 Dependencies/Critical Path Analysis

The timeline of the project and the integrity of its workflow are influenced by a variety of interconnected, dependent tasks. Although the advancements in MFA and phishing workflows are intended to occur at the same time, testing and quality assurance processes cannot commence until both are fully implemented. This creates a significant reliance on testing which depends on the successful completion of both workflow implementations. Minhaj Ahmed and Ansaf Althaf would need to collaborate to address issues during the testing stage, which relies on the outcomes of system and user acceptance testing. The final phase, Project Closure and Handover, cannot begin until all quality assurance tasks, including troubleshooting, have been completed. Consequently, quality assurance acts as a critical gating factor for the completion of the project.

The critical path of the project is as follows:

1. Implementation of both MFA and Phishing workflows
2. Testing and Quality Assurance
3. Stakeholder presentation

Any delays in these activities will directly affect the timeline for final delivery, as they are interconnected. Tasks that are not on the critical path, such as documentation or internal evaluations, have some leeway in scheduling, if they do not hinder the commencement of subsequent phases. These established dependencies and the arrangement of the critical path facilitate controlled progress and ensure timely completion.

4.5 Project Methodology

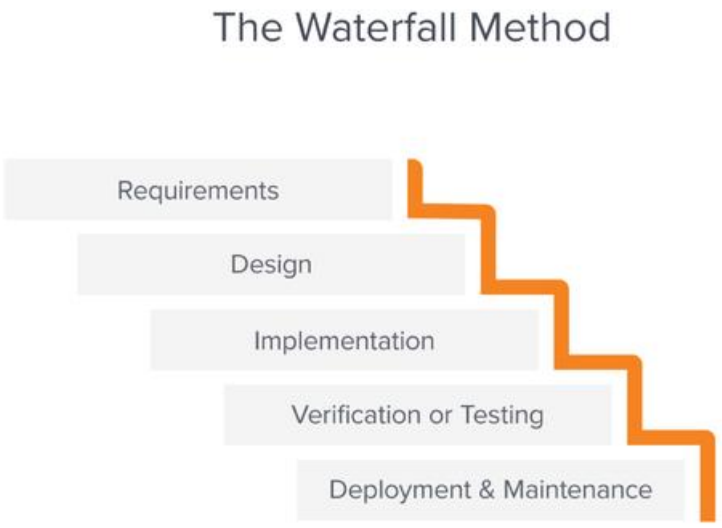


Figure 17: Conceptual Representation of Waterfall Method

From *Waterfall Methodology: A Complete Guide* by Adobe, 2022, (https://business.adobe.com/uk/blog/basics/waterfall)

The project utilises a Waterfall methodology, which is ideal for its organised, phase-oriented execution (Adobe, 2022). Since the project requirements were clearly defined from the beginning and are unlikely to evolve, a linear and sequential approach was selected to maintain oversight, minimise uncertainty, and streamline task management. Each phase is contingent upon the successful completion of the previous one, with no overlap in deliverables or feedback loops between the phases.

The waterfall model suits the team's working style, wherein task responsibilities were allocated early, communication with stakeholders was planned only at milestone updates, and testing was scheduled for the conclusion of the development cycle. For example, both the MFA and phishing workflows were crafted and executed prior to the start of the Testing and Quality Assurance phase. Similarly, Project Closure tasks, including documentation, presentations to stakeholders, and retrospectives, only start once the testing phase has been fully completed.

This strategy facilitates a clear understanding of task dependencies, ensures strict adherence to timelines, and prevents downstream activities from starting too early. It also makes milestone tracking easier and simplifies the project management process.

Section 5. Budget Plan

Cybersecurity incidents are inevitable, and the financial costs can be extensive. According to the Netwrix Research Lab (2024), 45% of companies faced unexpected expenses to address security gaps. In addition to that, 16% reported a decrease in company valuation, and 13% had to deal with lawsuits, a significant increase from just 3% for each of those outcomes in 2023. As a result, 62% of companies now purchase cyber insurance coverage within 12 months, compared to 59% in 2023, as a means to tackle these unexpected expenses.

5.1 Planning and Testing Cost

Possessing a solid incident response plan is an astute decision for FeatherDrive Flying Car Company as a means to reduce costs associated with potential data breaches. IBM Security (2023) suggested that the average cost and frequency of phishing attacks was the second most costly security breach for organisations with an average of USD$4.76M per incident, while stolen or compromised credentials were also commonly used at an average cost of USD$4.62M per incident. By implementing incident response (IR) planning and testing, organisations could save up to USD$1.49M for a data breach, compared to those companies without such planning or testing. Furthermore, companies who invest in cybersecurity would also generally invest in IR plan & testing and employee training (IBM, 2023).

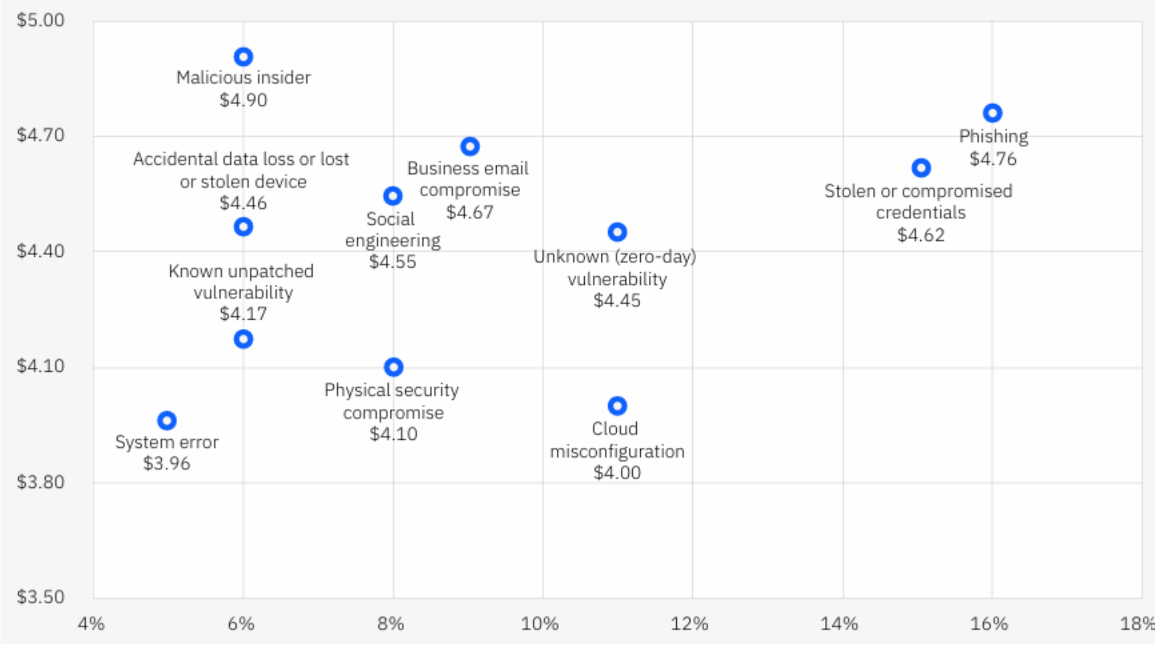


Figure 18: The Average Cost and the Frequency of Breaches (in USD millions)

From *Cost of a Data Breach Report 2023* by IBM, 2023, (https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf)

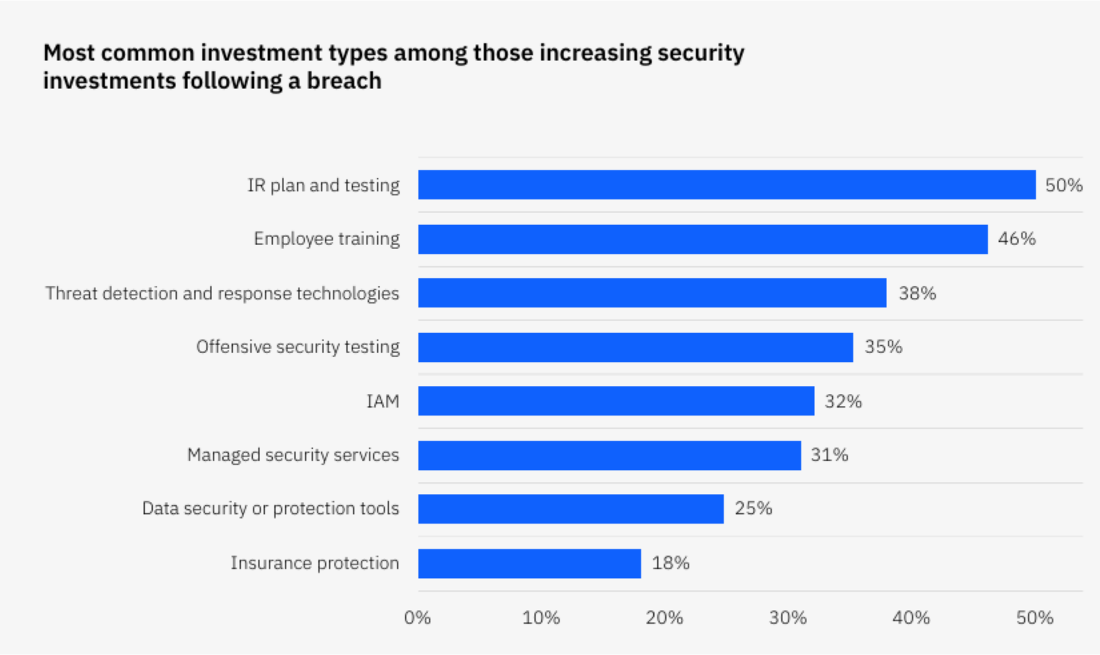


Figure 19: The Types of Security Investments Following a Data Breach

From *Cost of a Data Breach Report 2023* by IBM, 2023, (https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf.)

The cost table below outlines the overall budget for 2025 and 2026 related to the planning and evaluation phase. Before implementing ServiceNow and other software, this phase includes planning and testing configurations and workflows. ServiceNow (2021) emphasises the importance of initial planning and ongoing testing whenever changes occur to ensure that developed applications meet requirements, ultimately saving time and money.

Burton (2024) introduced a 5-step process for planning and testing, along with associated costs. The first step, planning, focuses on understanding goals and objectives. The second step, scenario design, involves conducting research and drafting the scenario. Next is preparation, which includes organising a tabletop exercise and coordinating with stakeholders. The fourth step, tabletop delivery, is when key management and vendors validate workflows and document the outcomes. Finally, the process concludes with analysis, where results are evaluated to identify improvement areas. Additionally, companies implementing ServiceNow would incur consultation fees based on the complexity of their business and customisation needs, starting at USD$100,000 (Balasubramanian, 2025).

	2025	**2026**
Planning and Testing Cost		
Planning and Testing		
Incident Response Planning	$5,000	$0
Scenario Design	$17,500	$0
Tabletop Exercise Preparation	$8,500	$0
Tabletop Exercise Delivery	$15,000	$15,000
Ongoing Assessment & Update	$8,500	$8,500
Consultation Fee	$100,000	$0
Insurance Coverage		
Cyber Liability Insurance	$15,000	$15,000
	$169,500	**$38,500**

Table 4: Forecast Planning and Testing Cost for Y2025 & 2026

5.2 Optimal Staff Cost

Once incident response planning is finalised, the next step is to assemble an incident response team. This team will receive credible alerts from the system (Microsoft, 2025b). Team members are responsible for verifying whether an event qualifies as an incident and requires further isolating and elimination of the threat. If the incident is serious or takes considerable time to resolve, companies may need to restore backup data, negotiate a ransom, or inform customers about compromised data (Microsoft, 2025c). Consequently, individuals from existing key management, in addition to cybersecurity experts, typically participate in the incident response process, including the CEO, CIO, Operations Manager, and HR Manager. These roles help guide the response efforts to minimise damage and restore normal operations (Microsoft, 2025d).

A new training and support team will be established within FeatherDrive Flying Car Company to address enquiries and issues, consisting of 15 Support Specialists to provide 24/7 service across the Asia Pacific and Europe. According to Tsai (2025), referencing data from the U.S. Bureau of Labor Statistics for 2024, the average salary for Tier 1 IT Support Specialists is USD$60,000, while Tier 2 IT Support Specialists earn an average of USD$71,500. As outlined by Adcyber (2023), Tier 1 specialists manage non-critical incidents and perform triage, escalating issues as necessary, while Tier 2 specialists conduct thorough investigations and resolutions for these incidents, further escalating to the incident response team if required. Additionally, all staff members are projected to receive a 5% salary increase in 2026.

Regular training sessions are included in the staff budget. Ganesan (2025) indicates that security awareness training costs approximately USD$20 per employee per year, totalling around USD$200,000 per year. One widely used platform for this purpose, KnowBe4, offers programs within this price range (KnowBe4, 2025) and is currently being integrated with ServiceNow in this project.

	2025	**2026**
Staff Cost		
24/7 Training and Support Team		

Tier 1 IT Support Specialists x 10	$600,000	$630,000
Tier 2 IT Support Specialists x 5	$357,500	$375,375
Awareness Training Materials (KnowBe4)	$200,000	$200,000
	$1,157,500	**$1,205,375**

Table 5: Forecast Staff Cost for Y2025 & 2026

5.3 Software Cost

Identified software requirements associated with the project are ServiceNow, Azure Active Directory, Zapier, and VirusTotal Enterprise. Further research on potential costs notes that setting up access for 10,000 employees is complimentary, while the SIR response model is priced at USD$75 per user per month (Apty, 2025). It is estimated that the company will need licenses for 100 users given its size. Balasubramanian (2025) posited that using ServiceNow would involve migration costs, integration costs (using Integration Hub) and annual maintenance fees for ongoing support.

Additionally, the company will implement Azure Entra ID P1, which offers essential identity features such as RBAC and MFA, enhancing secure management of user access to applications and company resources. When a user tries to log in, Entra ID P1 will request MFA, allowing them to approve the sign-in via Microsoft Authenticator, generate a time-based code, or utilise passwordless authentication (Microsoft, 2025c). The monthly fee for this service is USD$6 per user (Microsoft, 2025c). Furthermore, the Zapier email parser will automatically extract data from incoming emails to ServiceNow. As reported by Saasworthy (2021), the company package is priced at USD$599 per month and can manage up to 100,000 tasks monthly. The email content will also be scanned with VirusTotal. Protalinski (2018) indicated that the Enterprise service costs USD$10,000 per year, which is projected to rise to USD$15,000 in 2025 and 2026.

Finally, the budget for Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) is included in this project, as they are valuable supplements to ServiceNow, to enhance overall incident response capabilities by detecting, monitoring, analysing, and recovering from events through ServiceNow's automated workflows (Darwin’s Data, 2023).

	2025	**2026**
Software Cost		
ServiceNow		
Requesters License (10,000 users)	$0	$0
Security Incident Response Model (100 users)	$90,000	$90,000
Integration Hub License	$1,200	$1,200
Annual Maintenance Fee	$0	$200
Precision Bridge		
Migration Fee	$4,950	$0
Microsoft		
Authenticator (MFA)	$0	$0
Azure Extra ID P1 (10,000 users)	$720,000	$720,000
Zapier		
Email Parser	$7,188	$7,188

VirtusTotal		
Premium (Enterprise)	$15,000	$15,000
Splunk, IBM Qradar (SIEM)	$25,000	$25,000
CrowdStrike, Carbon Black (EDR)	$25,000	$25,000
	$888,338	**$883,588**

Table 6: Forecast Software Cost for Y2025 & 2026

5.4 Hardware cost

To establish a robust backup system that ensures data protection, even with all primary servers and systems online, Moore (2025) recommends securely backing up critical files and important files using a local backup server. This approach provides an additional safeguard against potential data encryption by malicious software especially the company is establishing multiple systems. Furthermore, there will be additional hardware costs associated with acquiring equipment and office supplies which are required for setting up the new support team.

	2025	**2026**
Hardware Cost		
Laptops/Desktops		
HP Business Laptops (i7, 16GB RAM, SSD) x 20	$30,000	$0
Monitors & accessories		
24–27" Monitor, Docking Station, Mouses x 20	$12,000	$0

Printers/scanners		
HP Colour LaserJet x 3	$3,000	$0
Switches, routers, APs		
Cisco Catalyst 9400 (switches) x 2	$2,400	$0
Cisco ASR 1000 Series (router) x 2	$4,000	$0
Catalyst 9100 Series (APs) x 4	$3,200	$0
Local backup		
Synology 16 Bay RackStation RS4021xs x 2	$12,000	$0
Maintenance & Upgrade Fee		$2,000
	$66,600	**$2,000**

Table 7: Forecast Hardware Cost for Y2025 & 2026

The total budget is projected at approximately USD$2.3 million per year after accounting for all subsections. For a detailed breakdown of the total project costs, please refer to the cost table in the Appendix. While this represents a significant investment for the company, it is important to consider that, according to IBM (2023), the average cost of a phishing attack exceeds USD$4 million. This budget aligns with IBM's findings that effective incident response can save up to USD$1.49 million if a data breach occurs, reinforcing the value of this investment. Ganesan (2025) also agreed that the annual cost for an enterprise-level organisation would cost up to USD$2.4 million.

Section 6. Risk Management Plan

6.1 Project Risk and Risk Controls

As highlighted in the previous section, enterprises are increasingly purchasing cyber insurance due to the rapid evolution of technology, the inevitability of cyber incidents, and the potential for significant financial losses. Identifying and mitigating project risks through effective risk controls is essential for project success. According to PwC's Global Risk Survey (Gibson, 2023), companies that practice strategic risk management are five times more likely to deliver stakeholder confidence and achieve better business outcomes. Effective risk controls not only protect reputation and minimise losses but also enhance growth and decision-making. The following outlines five key risks that may emerge during the project.

Budget overruns

To mitigate the risk of budget overruns caused by unforeseen expenses, it is advisable to allocate a contingency fund. As noted by Monday (2022), large-scale projects frequently exceed their budgets by 30–45%, often due to unanticipated expenses. Allocating a contingency reserve of 5–10% of the total budget helps ensure that the project remains within financial parameters, even when unforeseen issues arise (Monday, 2022).

Staffing challenges

Recruiting and retaining skilled cybersecurity professionals can be difficult due to high market demand. The report from ISC2 (2024) Cybersecurity Workforce Study stated that there is a global shortage of over 3.4 million cybersecurity professionals. To address this, the report further suggested that companies have to offer competitive salaries and provide ongoing training and development opportunities. Additionally, engaging third-party recruitment agencies may become necessary, which could require extra budget allocation.

Tool integration or compatibility

Integrating ServiceNow with existing enterprise systems could require substantial time and financial resources. According to Gartner (2024), ITSM tool integrations frequently exceed projected timelines and budgets when pre-implementation validation and stakeholder coordination are insufficient. Conducting thorough pre-implementation testing is therefore critical to ensuring system compatibility, reducing the risk of integration issues, and avoiding unexpected disruptions or added costs.

False positives in phishing detection

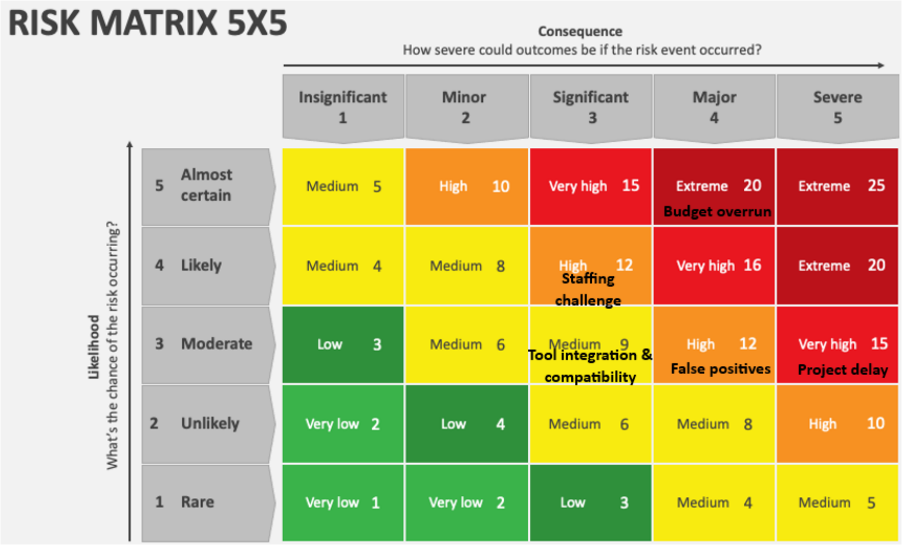
Legitimate emails may sometimes be mistakenly flagged as phishing attempts, leading to false positives. These misclassifications can disrupt business operations, delay critical communications, and reduce overall productivity. According to Proofpoint (2023), organisations face considerable productivity losses when employees and IT teams must frequently review and release incorrectly flagged messages. To address this risk, it is essential to provide ongoing cybersecurity awareness training and establish clear protocols for managing and reviewing flagged emails.

Project delays

Project delays represent a significant risk due to the involvement of multiple stakeholders and the complexity of coordinating activities such as testing, approvals, and deployment. Scrobota (2024) highlights that unclear objectives and misalignment among stakeholders are key contributors to project setbacks and failures. To mitigate these risks, it is essential to develop a well-defined, realistic, and accountable project timeline that ensures timely execution and the successful achievement of project goals (Scrobota, 2024).

By proactively addressing these risks with targeted controls, the company could significantly increase the likelihood of project success, stakeholder trust, and long-term business resilience.

6.2 Risk Matrix/Register



RISK MATRIX 5X5

Consequence
How severe could outcomes be if the risk event occurred?

Likelihood
What's the chance of the risk occurring?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost certain	Medium 5	High 10	Very high 15	Extreme 20 Budget overrun	Extreme 25
4 Likely	Medium 4	Medium 8	High 12 Staffing challenge	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9 Tool integration & compatibility	High 12 False positives	Very high 15 Project delay
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Figure 20: 5 x 5 Risk Matrix Associated with Project Risks

Risk	Likelihood	Consequence	Risk Level
Budget Overrun	5	4	**20**
Staffing Challenges	4	3	**12**
Tool Integration or Compatibility	3	3	**9**
False Positives in Phishing Detection	3	4	**12**
Project Delays	5	3	**15**

Table 8: Project Risk Level Based on the 5 x 5 Risk Matrix

Given that approximately 30–45% of projects experience budget overruns (Monday, 2022), this risk poses a significant threat to both the project and the entire company. Persistent overspending can drain financial resources, potentially compromising not only the project’s success but also the company’s overall financial health (Project Management Institute, 2021). In the long term, this may disrupt other business operations, damage the organisation’s reputation, and reduce stakeholder trust and confidence (Project Management Institute, 2021). Furthermore, financial strain could lead to scope reduction or quality compromises, which may negatively affect project outcomes and strategic objectives (Project Management Institute, 2021). These cascading effects make budget overrun an *Extreme* risk to manage in project execution.

Staffing challenges are rated *High* risk in this project. The global shortage of over 3.4 million cybersecurity professionals, as reported by the ISC2 (2024) Cybersecurity Workforce Study, makes it highly probable that the company will struggle to recruit and retain skilled talent. This can lead to project delays, increased costs, and a reliance on external resources, posing a moderate but impactful risk to this project.

Tool integration or compatibility is considered a *Medium* risk. While ServiceNow is being used to streamline and centralise integration efforts, it does not fully eliminate the possibility of issues, especially when interfacing with third-party systems. Minor integration issues may still arise, potentially causing delays or requiring additional configuration effort. According to Gartner (2024), even with strong integration platforms, companies should anticipate some level of complexity when managing tool ecosystems.

False positives in phishing detection are rated as a *High* risk. While technical controls are in place, users may mistakenly report legitimate emails as phishing, leading to unnecessary investigations and delayed communication. Repeated false reports can also cause alert fatigue for security teams, diverting attention from real threats. According to Verizon's (2023) Data Breach Investigations Report, human error remains a key factor in phishing-related incidents, highlighting the operational risk of user-driven false positives in this project.

Project delays represent a *Very High* risk because managing multiple stakeholders and coordinating activities such as testing, approvals, and deployment can be complex and challenging. Scrobota (2024) emphasises that unclear objectives and misalignment among stakeholders are major factors contributing to project setbacks and failures, making project delays one of the more significant risk factors for this project.

6.3 Risk Analysis and Mitigation

A robust risk analysis process is essential to successful project execution, particularly for initiatives that involve multiple stakeholders, technical complexity, and strict time or budget constraints. This process must involve identifying, evaluating, quantifying and measuring the risks on project outcomes. These steps enable the team and key stakeholders to prioritise risk responses, apply appropriate mitigation strategies, and make decisions at critical points throughout the project lifecycle.

Budget overrun has been identified as the most significant threat to this project. Industry data indicates that 30–45% of projects experience budget overruns (Monday, 2022), highlighting the critical need for effective contingency planning. To mitigate budget overruns, a realistic budget should be developed with contingency buffers in the initial phase of the project. Courtney et al. (2019) emphasises that up-front contingency planning improves transparency and helps manage forecasting uncertainty. Ongoing financial monitoring is also crucial to ensure informed decision-making and project control (Courtney et al., 2019). Thus, it is suggested to monitor actual spend and budget monthly, with a 5% variance threshold triggering a go/no-go review by executive management.

Staffing challenges are rated as a *High* risk due to the global shortage of cybersecurity professionals. To mitigate staffing risks, the project should implement proactive hiring, invest in cross-training and upskilling starting from Phase 1. Vickers (2025) emphasised these strategies are effective responses to the global cybersecurity talent shortage.

Tool integration and compatibility issues are considered a *Medium* risk. Challenges may arise when integrating ServiceNow with third-party platforms, potentially causing minor delays. Early testing, proof-of-concepts, and strong collaboration with vendors will help manage this risk and avoid disruptions to the schedule (Cole, 2024).

False positives in phishing detection are classified as a *High* operational risk. Misclassification of legitimate emails can disrupt communication and overburden security teams, contributing to alert fatigue. To reduce false positives, Living Security Team (2023) suggested companies should provide ongoing focused security awareness training that reinforces key phishing indicators and correct reporting procedures can further empower users to identify true threats without flagging false messages. Therefore, quarterly refreshment trainings would help to minimise this risk.

Project delay is categorised as a *Very High* risk. Coordinating activities such as testing, approvals, and deployment across departments and stakeholders introduces significant complexity. Scrobota (2024) highlights that misalignment and unclear objectives are among the top drivers of project delays. These delays could potentially disrupt delivery schedules and increase costs. To mitigate this risk, the project must establish a clear and realistic timeline with clearly defined milestones and responsibilities (Scrobota, 2024). Regular meetings with stakeholders, progress tracking, and escalation procedures should be implemented from Phase 1 to ensure issues are identified and addressed early (Prabakaran & Ramana, 2025). Effective timeline management is essential to identify potential problems before they occur and enforce recovery plans, ensuring that delays are caught and addressed early (Prabakaran & Ramana, 2025).

6.4 Project Risk Management Plan

The Project Risk Management Plan addresses the five key risks identified in this section to ensure successful project execution. Budget overruns and project delays are prioritised due to their potential risks. They will be mitigated through proactive financial controls, milestone planning, and escalation protocols. Medium-priority risks such as staffing challenges and false positives in phishing detection are managed through targeted recruitment, cross-training, and regular awareness programs. A lower priority is given to the tool integration as it could be addressed via early proof-of-concept testing and thorough system integration procedures. Each risk is assigned an owner with clear mitigation actions and timelines to support accountability and timely resolution.

ID	Risk Title	Description	Priority	Affected Area	Actions / Timelines	Owner
1	Budget Overrun	Project exceeds allocated budget due to unforeseen costs or poor forecasting.	**HIGH**	Accounting & Finance	***1. Create a detailed budget with a 10% contingency buffer by project initiation.*** ***2. Track actual vs. budget monthly. If >5% variance is detected, trigger senior***	Senior Management/ Finance Manager

					management review within 7 business days.	
2	Project Delay	Delay in key phases such as testing or deployment due to misalignment and complex coordination.	**HIGH**	R&D	***1. Set milestone dates during planning (Phase 1).*** ***2. Hold fortnightly progress meetings with executive management and stakeholders.*** ***3. Use project dashboard for real-time tracking.*** ***4. Escalate unresolved blockers within 48 hours.***	Project Manager/ Operations Manager
3	Staffing Challenges	Inability to secure or retain qualified cybersecurity professionals.	**MEDIUM**	Human Resources	***1. Launch recruitment campaign by end of first month.*** ***2. Fill critical roles within 60 days. Seek for external recruitment agencies if needed.*** ***3. Start cross-training 100% of technical staff and executive management by end of Phase 1.*** ***4. Review staffing plan quarterly.***	HR Manager/ Training & Development Specialist

4	False Positives in Phishing Detection	Legitimate emails are misclassified as phishing, causing alert fatigue and communication issues.	**MEDIUM**	Human Resources / IT	1. ***Conduct phishing simulation tests quarterly.*** 2. ***Distribute articles and provide mandatory 1-hour phishing awareness refresher training for staff every three months.*** 3. ***Implement feedback forms to review and enhance training sessions. Provide updates to staff on any new changes.*** 4. ***Track and reduce false positives by 15% per quarter.***	Training & Development Specialist
5	Tool Integration or Compatibility	ServiceNow may have compatibility issues when integrated with third-party platforms, leading to minor delays.	**LOW**	R&D / IT	1. ***Complete proof-of-concept for each integration by end of Phase 3.*** 2. ***Schedule 2 rounds of system integration testing.*** 3. ***Log and resolve 90% of integration bugs before Phase 5 begins.***	Quality Assurance & Testing Analyst

Table 9: Project Risk Management Plan to Tackle 5 Key Risks

6.5 Incident Response Plan

An incident response plan is at the forefront of the prototype and risk management strategy. Executives at FeatherDrive Flying Cars have complained about the recent occurrences of phishing emails which have targeted and victimised the employees of the company. It is imperative that robust methodology be deployed to tackle and respond to these incidents which have experienced an upwards trajectory in recent times. ServiceNow provides an end-to-end automated management system for incident response through the deployment of workflows, which have been demonstrated as a workflow prototype in Figure 6 (see Section 3.2) for the management of phishing incidents. Incident response plan involves key phases and timeline, which have been described in Figure 20 for the prototype.

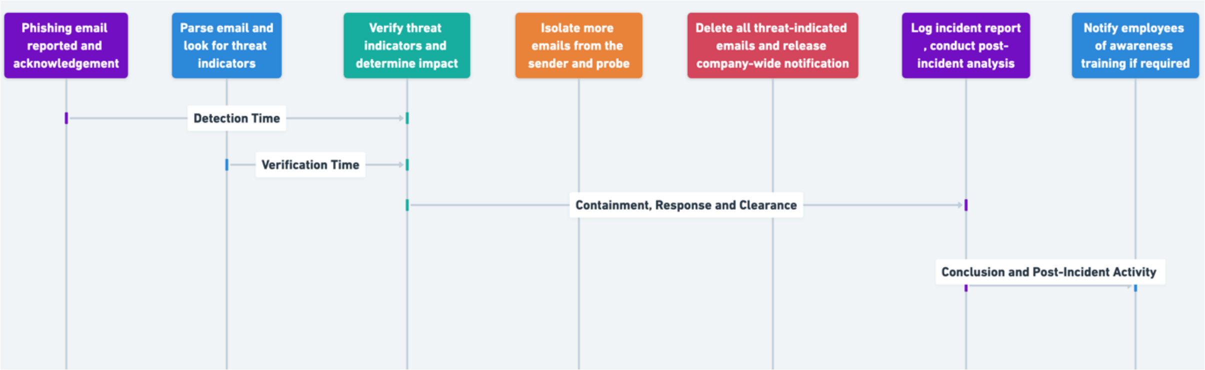

Phishing email reported and acknowledgement
Parse email and look for threat indicators
Verify threat indicators and determine impact
Isolate more emails from the sender and probe
Delete all threat-indicated emails and release company-wide notification
Log incident report , conduct post-incident analysis
Notify employees of awareness training if required
Detection Time
Verification Time
Containment, Response and Clearance
Conclusion and Post-Incident Activity

Figure 21: Timeline for Phishing Incident Management Workflow

The initial phases include the detection and verification processes, where the employee incident report is received, the suspected email contents are parsed and checked for threat indicators. This process is initiated by the ServiceNow workflow, which is automatically triggered when the employee reports a suspected phishing email. The incidents are routed to Tier 1 or Tier 2 based on the severity of the incident. Next steps involve searching for more emails related to the sender, isolate the emails if found, and probe them for further investigation. After a thorough investigation and analysis, the threat-related emails are deleted from the organisation and a company-wide notification is released to inform the employees and executive management of the incident. These steps are part of the containment, response and clearance phase of the incident management, as indicated in Figure 21.

The final phase involves concluding the incident and conducting post-incident activity. After the confirmation that the threat has been completely wiped out, the incident activities are logged, including all the details related to emails, sender, IP address, and threat contents, to keep a record for future reference. Post-incident activities are carried out, such as performing a thorough analysis of the incident and root cause, and a notification of employee training is pushed through if required. This completes a comprehensive and automated end-to-end process through the usage of ServiceNow workflow to manage phishing incidents and enhance the security operations at FeatherDrive Flying Cars.

Section 7. Continual Improvement

7.1 Strategies for Cyber Protection/Defence/Incident

A structured and automated phishing detection and response system is implemented using the ServiceNow platform. This is built to protect users from email-based threats through a proactive and sustainable workflow. When an employee receives a suspicious email, they access the custom-built “Report Phishing” form on the ServiceNow portal. Submitting this form triggers a workflow that automatically processes the reported content. The email file is parsed through Zapier, which extracts metadata and attachments. This data is then passed to VirusTotal, a threat intelligence aggregator, that scans the content for known malware signatures, phishing links, and behavioural indicators. If the scan identifies malicious content, ServiceNow takes automatic action by flagging and deleting similar emails across the organisation. Simultaneously, a ticket is escalated to the security support team for documentation and training.

This process not only responds to phishing incidents but actively reduces the risk of lateral spread by deleting similar messages and recording the attack pattern. The support team plays a critical role in cyber defense by maintaining a repository of these phishing events. This documentation feeds directly into employee training materials and awareness simulations.

To protect user identities, MFA is enforced and monitored by a separate ServiceNow workflow. In cases where users cannot access MFA, especially during weekends, an emergency access request can be submitted, which is then validated and fulfilled securely based on predefined roles.

7.2 Ongoing Monitoring and Maintenance

Maintaining the integrity of phishing response workflows and MFA systems demands a clear operational structure post-deployment. FeatherDrive’s approach centers on automation, human oversight, and ongoing evaluation embedded into routine operations.

The support team is responsible for 24/7 monitoring and support of the workflows within ServiceNow. Every phishing report submitted through the system generates an incident ticket, which is reviewed and resolved based on the threat level detected. Support team analysts regularly audit VirusTotal scan results, Zapier parsing logs, and deletion actions to ensure that automated responses are accurate and consistent.

All incident reports are archived in ServiceNow and classified by type, severity, and department. This allows for targeted training and enables trend analysis by the support team.

These insights inform quarterly updates to the ServiceNow phishing response workflow and the staff training plan.

Dashboards within ServiceNow track metrics such as the number of phishing emails reported, average response time, number of successful detections, and MFA exception requests.

Scheduled maintenance activities include weekly checks for broken integrations (e.g., Zapier/ VirusTotal), monthly testing of form submissions and ticketing logic as well as quarterly reviews of the automated deletion script to avoid false positives.

7.3 Additional Processes, Policies and Compliance

A formal phishing policy is established to define acceptable and unacceptable email behaviours, outline procedures for identifying and reporting suspicious messages, and reinforcing the use of ServiceNow as the central reporting platform. Regular updates to this policy are scheduled to ensure alignment with evolving phishing threats. Mandatory policy acknowledgements are captured through the ServiceNow compliance module, while awareness is reinforced through quarterly training sessions and simulated phishing campaigns delivered to all staff.

Detection and response processes are embedded within ServiceNow workflows. Once a phishing report is submitted through the user-facing form, the email is parsed using Zapier and analysed via VirusTotal to detect malicious content. If confirmed, similar emails are automatically deleted, and a security incident is logged. Documentation of the event is managed by the support team, and the data is retained for training and simulation design. System configuration and policy adherence are evaluated using the Security Center within ServiceNow, where deviations are flagged and addressed through predefined escalation paths

Ongoing compliance with internal security frameworks and regulatory expectations is maintained through ServiceNow's Policy and Compliance Management capabilities. Audit trails, policy acknowledgements, training completions, and workflow changes are continuously monitored and documented within the platform. To support awareness and reinforce security practices at the operational level, a team would be appointed across departments to assist in communicating security protocols, encouraging correct use of the phishing reporting workflow, and guiding colleagues on appropriate responses to suspicious activity.

Section 8. Training and Communication

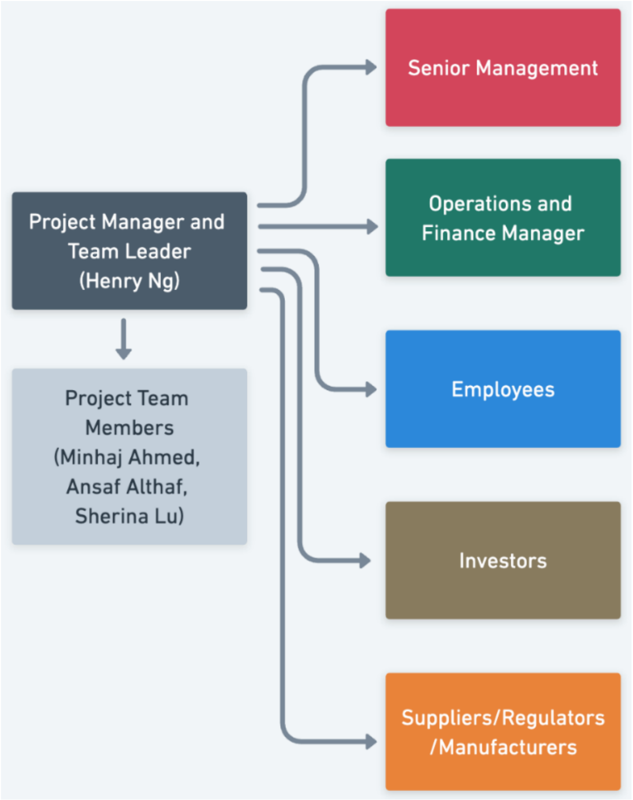

Project Manager and Team Leader (Henry Ng)
Project Team Members (Minhaj Ahmed, Ansaf Althaf, Sherina Lu)
Senior Management
Operations and Finance Manager
Employees
Investors
Suppliers/Regulators /Manufacturers

Figure 22: Stakeholder Engagement Diagram

8.1 Stakeholder Engagement

This cybersecurity project utilises ServiceNow to enhance security across FeatherDriveFlying Cars’ digital ecosystem through the integration of MFA and phishing incident management workflows. For smooth implementation and long-term success of the project, establishment of a strong strategy for stakeholder engagement is essential. This strategy outlines all the internal and external stakeholders who are impacted or contribute to the project.

Internal stakeholders and their roles are:

- Senior Management: They include Executive Board members, Chief Executive Officer (CEO), Chief Information Officer (CIO), and Chief Technology Officer (CTO). Senior leadership is required to endorse the vision of the project and ensure the project aligns with the overall goals and standards of the company. They provide strategic direction and approval of the project and funding.
- Investors: It is imperative that the organisation is managing cybersecurity risks and demonstrating a strong security culture to provide assurance to the investors. Investors need to be regularly updated with the risk mitigation processes and operational resilience.
- Operations Manager: The Operations Manager coordinates the ServiceNow workflows with the operational activities of the organisation, ensuring there is minimal disruptions with the integration of the automated workflows.
- Financial Manager: The integral role of the Financial Manager is to oversee project budgeting and validate the cost-efficiency and economic advantages of the outlined security improvements.

- Employees: As the primary users of the existing systems and the new prototype at FeatherDrive Flying Cars, the employees are central to the success of the project. They would be engaged through phishing awareness training and participating in surveys for the new rollout.

External stakeholders and their roles are outlined below:

- Customers: Customers prioritise the security of their personal information and expect smooth and uninterrupted services. Their experience and feedback would assist in refining the new integrations.
- Suppliers: Suppliers must adhere to the refined security enforcements and MFA protocols while accessing FeatherDrive Flying Cars systems, and tailored guidance would be provided to support them.
- Manufacturers (Hardware and Software): They also include technology vendors and partners who would be engaged, as part of the stakeholder engagement, so that the hardware and software are compatible with the security protocols.
- Regulators: It is the role of the regulatory bodies to ensure that FeatherDrive Flying Cars complies with the company policies and security standards. They are engaged in the project through auditing of compliance as well as aligning the workflows and procedures within the standard frameworks.

8.2 Communication Plan

The Communications Plan aims to provide all stakeholders with clear and accessible information regarding the project’s objectives, tasks, user requirements, data quality, data analytics, and their respective roles.

The accompanying matrix outlines the methods and frequency of information dissemination throughout the project lifecycle.

Audience	Information Required	Frequency of Communication	Method of Communication	Information Provider
Senior Management	Design Document	One-Off	Email and Meeting	Project Manager
	Project Initiation and Planning	One-Off	Email	Project Manager
	Project Progress	Fortnightly	Meetings	Project Manager
	Project Budget	Monthly	Meetings	Finance Manager
	MFA Workflow Development	Monthly	Email	Project Manager
	Phishing Workflow Development	Monthly	Email	Project Manager

	Testing and Quality Assurance	End of Implementation Phase	Email	Project Manager
	Project Closure and Handover	One-Off	Presentation	Project Manager
Other Internal Stakeholders	Design Document	One-Off	Email	Project Manager
	Project Initiation and Planning	At Start of Planning Phase	Briefing Meeting	Project Manager
	Project Progress	Fortnightly	Briefing Meeting	Project Manager
	MFA Workflow Development	Weekly	Email Updates	Security Architect
	Phishing Workflow Development	Weekly	Email Updates	Security Architect

	Testing and Quality Assurance	After Completion of Development	Email	Security Analyst
	Project Closure and Handover	One-Off	Email	Project Manager
External Stakeholders	Design Document	On-Request or When Necessary	Email	Project Manager
	Project Initiation and Planning	One-Off	Public Briefing	Project Manager and Security Architect
	MFA Workflow Development	One Update During Implementation and After Implementation	Email Updates	Project Manager and Security Architect
	Phishing Workflow Development	One Update During Implementation	Email Updates	Project Manager

		and After Implementation		and Security Architect
	Testing and Quality Assurance	When Reporting or Upon Request	Documentation	Project Manager and Security Analyst
	Project Closure and Handover	One-Off	Email	Project Manager

Table 10: Stakeholder Communication Matrix

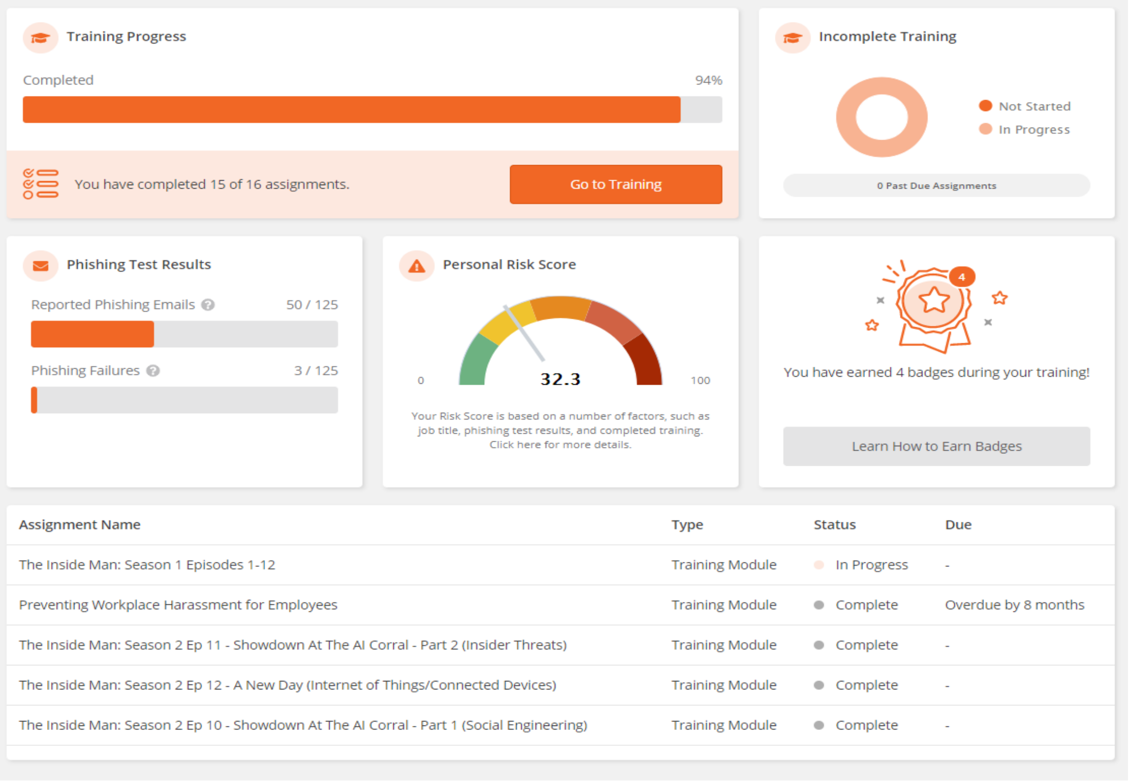
It is important to note that the matrix above outlines the formal channels of information dissemination within the project, a considerable amount of informal and ad-hoc communication is expected to occur throughout its duration particularly between the Project Manager and members of Senior Management.

8.3 Client Workforce Training

Every quarter, staff members will receive simulated phishing emails from KnowBe4 at random times to determine whether they are able to identify illegitimate emails. Should they click on the link provided in these fake emails, a notification is sent to the support team as well as senior management alerting them of the staff member's failure to correctly identify a phishing email. These staff members will then have to undergo further phishing email awareness training. The results in KnowBe4 can be integrated into ServiceNow to increase convenience for staff members to ascertain information such as, how many training sessions they need to complete and how many phishing detection failures they have obtained (see

Figure 23). KnowBe4 also generates an organisation's overall risk scores aggregated from every staff member's risk score (see Figure 24).

To supplement this training, the Training and Development Specialist will also upload articles once every three months. These articles will provide tips to staff members on how to better protect themselves online against email phishing attacks and other cybersecurity attacks. The support team will also conduct training sessions after the articles have been released to ensure that staff members have a comprehensive understanding on phishing and other cybersecurity attacks.



You have completed 15 of 16 assignments.

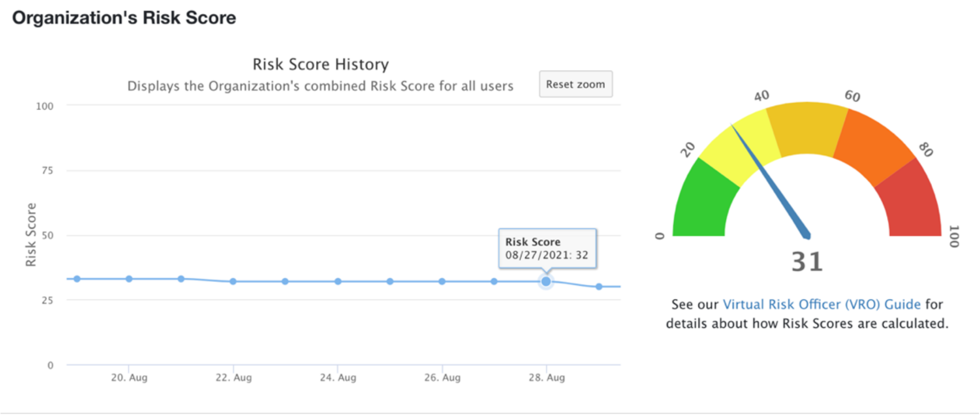
Your Risk Score is based on a number of factors, such as job title, phishing test results, and completed training. Click here for more details.

You have earned 4 badges during your training!

Assignment Name	Type	Status	Due
The Inside Man: Season 1 Episodes 1-12	Training Module	● In Progress	-
Preventing Workplace Harassment for Employees	Training Module	● Complete	Overdue by 8 months
The Inside Man: Season 2 Ep 11 - Showdown At The AI Corral - Part 2 (Insider Threats)	Training Module	● Complete	-
The Inside Man: Season 2 Ep 12 - A New Day (Internet of Things/Connected Devices)	Training Module	● Complete	-
The Inside Man: Season 2 Ep 10 - Showdown At The AI Corral - Part 1 (Social Engineering)	Training Module	● Complete	-

Figure 23: Illustration of Team Dashboard Overview on KnowBe4

From *Team Dashboard Overview for Admins* by KnowBe4, 2025d, (https://support.knowbe4.com/hc/en-us/articles/5632850730643-Team-Dashboard-Overview-for-Admins)



See our Virtual Risk Officer (VRO) Guide for details about how Risk Scores are calculated.

Figure 24: Example Illustration of an Organisation’s Risk Score on KnowBe4

From *Dashboard Overview* by KnowBe4, 2025, (https://support.knowbe4.com/hc/en-us/articles/204218028-Dashboard-Overview)

Reference List

Adcyber. (2023, June 21). *What is Tier 1, 2, 3 incident response? A cybersecurity guide*. Cyber Insight. https://cyberinsight.co/what-is-tier-1-2-3-incident-response/

Adobe. (2022, March 18). Waterfall Methodology: A Complete Guide. *Adobe.* https://business.adobe.com/uk/blog/basics/waterfall

Apty. (2025, February 14). ServiceNow implementation cost: Everything you need to know. *Apty*. https://apty.ai/blog/servicenow-implementation-cost/

Balasubramanian, S. (2025, April 4). *ServiceNow pricing 2025: The complete breakdown*. Desk365. https://www.desk365.io/blog/servicenow-pricing/

Basit, A., Safar, M., Liu, X., Javed, A. R., Jalil, S., & Kifayat, K. (2020). *A comprehensive survey of AI-enabled phishing attacks detection techniques.* Telecommunication Systems, 76(1). https://doi.org/10.1007/s11235-020-00733-2

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). *Study on Phishing Attacks*. International Journal of Computer Applications, 182(33), 27–29. http://dx.doi.org/10.5120/ijca2018918286

Bowman, A. (2024, May 13). *What is Artificial Intelligence?* NASA. https://www.nasa.gov/what-is-artificial-intelligence/

Burton, R. (2024, December 19). *The real cost of a tabletop exercise: What goes into creating a successful one?* PreparedEx. https://preparedex.com/the-real-cost-of-a-tabletop-exercise-what-goes-into-creating-a-successful-one/

Chen, M. (2024, November 25). *What is Machine Learning?* Oracle. https://www.oracle.com/au/artificial-intelligence/machine-learning/what-is-machine-learning/#:~:text=Machine%20learning%20(ML)%20is%20the,t%20mean%20the%20same%20thing.

Cole, Z. (2024, January 17). *Best practices for implementing ServiceNow integrations faster*. Perspectium. https://www.perspectium.com/blog/implementing-servicenow-integrations-faster/

Collier, C. (2022, June 14). *Dynamic and Static Malware Analysis.* CyberMaxx. *https://www.cybermaxx.com/resources/dynamic-and-static-malware-analysis/#:~:text=%2C%20user%20input).-,What%20is%20Dynamic%20Malware%20Analysis?,other%20public%20sandboxes%20out%20there*.

Courtney, H., Koller, T., & Lovallo, D. (2019). *Bias busters: Up-front contingency planning*. McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/Bias%20busters%20Up%20front%20contingency%20planning/Bias-busters-Up-front-contingency-planning.pdf

Cyber Management Alliance (2023, June 19). What is Compliance in Cybersecurity and How to Achieve it? *Cm-alliance. https://www.cm-alliance.com/cybersecurity-blog/what-is-compliance-in-cybersecurity-and-how-to-achieve-it*

Darwin's Data. (2023, October 22). *How much does an incident response team cost?* Darwin’s data. https://darwinsdata.com/how-much-does-an-incident-response-team-cost/

Eppright, C. (2021, March 25). *What is Natural Language Processing (NLP)?* Oracle. https://www.oracle.com/au/artificial-intelligence/what-is-natural-language-processing/

Ezenduka, U. (2024, August 26). Everything You Need to Know About ServiceNow Data Integration - Exalate. *Exalate*. https://exalate.com/blog/servicenow-data-integration/

Ganesan, R. (2025, May 12). *What is the average cost of cyber security services? A complete price guide*. Binary IT. https://binaryit.com.au/average-cost-of-cyber-security-services/

Gartner. (2024, December 19). *ITSM best practices for effective IT change management*. https://www.gartner.com/en/documents/6032135

Gibson, K. (2023, October 24). *What is risk management & why is it important?* Harvard Business School Online. https://online.hbs.edu/blog/post/risk-management

Gundeti, R. (2024, June 28). *Understanding Multi-Factor Authentication (MFA) and One-Time Password (OTP) Algorithms*. System weakness. https://systemweakness.com/understanding-multi-factor-authentication-mfa-and-one-time-password-otp-algorithms-955354f95808

Halyday, S. (2022, March 11). Tips on implementing a new ICT system. *Qao.* https://www.qao.qld.gov.au/blog/tips-implementing-new-ict-system

Hashemi-Pour, C. (2023, December 15). *What is the CIA Triad (confidentiality, integrity and availability?)* Tech target. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

IBM. (2023). *Cost of a data breach report 2023*. Ponemon Institute. https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf

ISC2. (2024, October 31). *2024 ISC2 cybersecurity workforce study*. ISC2. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

KnowBe4. (2025, March 12). *Dashboard Overview*. KnowBe4. https://support.knowbe4.com/hc/en-us/articles/204218028-Dashboard-Overview

KnowBe4. (2025b, March 12). *Phishing Security Test (PST) Overview*. KnowBe4. https://support.knowbe4.com/hc/en-us/articles/236271227-Phishing-Security-Test-PST-Overview

KnowBe4. (2025c, January). *Security Awareness Training pricing*. KnowBe4. https://www.knowbe4.com/products/security-awareness-training/pricing

KnowBe4. (2025d, April 25). *Team Dashboard Overview for Admins*. KnowBe4. https://support.knowbe4.com/hc/en-us/articles/5632850730643-Team-Dashboard-Overview-for-Admins

Living Security Team. (2023, September 4). Phishing management: Key metrics to measure to protect against phishing. *Living Security*. https://www.livingsecurity.com/blog/phishing-management-key-metrics-to-measure-to-protect-against-phishing

Lundqvist, G. (2025). *Unlocking the Power of Role-Based Access Control (RBAC) in ServiceNow*. Linkedin. https://www.linkedin.com/pulse/unlocking-power-role-based-access-control-rbac-g%C3%B6ran-aajzf

McCarthy, M. (2025, January 2). *The Definitive Guide to Role-Based Access Control (RBAC).* StrongDM. https://www.strongdm.com/rbac

McDaniel, Z. (2022, September 26). Email Parser: What is it and how can it help your business? *Leadsbridge*. https://leadsbridge.com/blog/email-parser/

Microsoft. (2025). *About Microsoft Authenticator - Microsoft Support*. Microsoft. https://support.microsoft.com/en-us/account-billing/about-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc

Microsoft. (2025b, May). *Microsoft Entra plans and pricing*. https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

Microsoft (2025c). *Virus Total - (Preview)*. Microsoft. https://learn.microsoft.com/en-us/connectors/virustotal/

Microsoft. (2025d). *What is incident response? Plan and steps*. Microsoft. https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response

Monday (2022, July 18). Creating a project contingency budget. *Monday*. ttps://monday.com/blog/project-management/project-contingency/

Moore, M. (2025, April 1). *World Backup Day 2025: All the news, updates and advice from our experts*. TechRadar. https://www.techradar.com/pro/live/world-backup-day-2025-all-the-news-updates-and-advice-from-our-experts

Mukherjee, A. (2023, October 4). *Is MFA As Secure As It Used To Be?* Threat Intelligence. https://www.threatintelligence.com/blog/mfa#:~:text=One%20of%20the%20biggest%20problems,becoming%20increasingly%20fraught%20with%20risks.

National Cybersecurity Centre of Excellence & National Institute of Standards and Technology (2020). (December 1, 2020). *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.* NCCOE & NIST. *https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html#:~:text=The%20CIA%20triad%20represents%20the,to%20and%20use%20of%20information*

National Institute of Standards and Technology (2025). *Security Assurance*. Community Security Resource Center. *https://csrc.nist.gov/glossary/term/security_assurance#:~:text=%2F%20Acronyms%20%2F%20Synonyms%3A-,Assurance,under%20Assurance%20from%20CNSSI%204009*

Netwrix Research Lab. (2024). *2024 hybrid security trends report*. Netwrix. https://www.netwrix.com/download/collaterals/Netwrix%20Hybrid%20Security%20Trends%20Report%202024.pdf

Phillips, S. (2025, January 19). Multi-Scanning Antivirus: Boost Your Threat Hunting With Multiple Layers. *Reversing Labs*. https://www.reversinglabs.com/blog/multi-scanning-antivirus-methodology#:~:text=Multi%2Dscanning%20is%20a%20powerful,more%20comprehensive%20shield%20against%20malware.

Prabakaran, P. A., & Ramana, V. (2025). *Risk management and delay mitigation in construction projects: A comprehensive literature review*. International Journal of Advance Research and Innovative Ideas in Education, 11(2), 788–794. https://ijariie.com/AdminUploadPdf/Risk_Management_and_Delay_Mitigation_in_Construction_Projects__A_Comprehensive_Literature_Review_ijariie26004.pdf

Project Management Institute. (2021). *Beyond agility*. Project Management Institute. https://www.pmi.org/learning/thought-leadership/pulse/pulse-of-the-profession-2021

Proofpoint. (2023, February 28). *Proofpoint's 2023 state of the phish report: Threat actors double down on emerging and tried-and-tested tactics to outwit employees*. Proofpoint. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2023-state-phish-report-threat-actors-double-down-emerging-and-0

Protalinski, E. (2018, September 27). *Alphabet's Chronicle launches VirusTotal Enterprise with Private Graph and 100-times faster malware search*. VentureBeat. https://venturebeat.com/security/alphabets-chronicle-launches-virustotal-enterprise-with-private-graph-and-100-times-faster-malware-search/

Robinson, S. (2024, October 2). *What is cloud infrastructure?* TechTarget. https://www.techtarget.com/searchcloudcomputing/definition/cloud-infrastructure

Rubeck, T. (2019, June 27). *Best Practices for Role Based Access Control (RBAC).* Idenhaus. https://idenhaus.com/best-practices-role-based-access-control-rbac/#:~:text=June%2027%2C%202019,what%20users%20have%20access%20to.

Rubeck, T. (2023, June 6). *The Difference Between Identity Access Management (IAM) And Identity Governance (IGA).* Idenhaus. https://idenhaus.com/difference-between-identity-access-management-and-identity-governance-administration/

Saasworthy. (2021, October 22). *Zapier pricing: Cost and pricing plans*. https://www.saasworthy.com/product/zapier/pricing

Scrobota, M. (2024, July 15). *KPIs and metrics for successful projects*. PMI Budapest. https://pmi.hu/en/blog/kpis-and-metrics-for-successful-projects--22443

ServiceNow. (2021). *How do I conduct effective and efficient testing?. ServiceNow.* https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/quick-answer/testing-basics.pdf

ServiceNow. (2024). *KnowBe4 Integration for SecOps - ServiceNow Store*. (2024). ServiceNow. https://store.servicenow.com/store/app/c5c92b621b246a50a85b16db234bcb34

ServiceNow. (2025). *Data Encryption Technologies for Data Protection on the Now Platform*. ServiceNow. https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/white-paper/wp-data-encryption-with-servicenow.pdf

ServiceNow. (2025b). *Exploring Data Management.* ServiceNow. https://www.servicenow.com/docs/bundle/yokohama-platform-administration/page/administer/managing-data/concept/exploring-data-management.html

ServiceNow. (2025c). *Implementing Integrations with ServiceNow Frequently Asked Questions Definition*. ServiceNow https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/enablement/integration-implementation-faq.pdf

ServiceNow. (2025d). *Integration Hub - ServiceNow AI Platform - ServiceNow*. ServiceNow. https://www.servicenow.com/au/products/integration-hub.html

ServiceNow. (2025e). *Policy and Compliance Management.* ServiceNow. https://www.servicenow.com/au/products/policy-compliance-management.html#benefits

ServiceNow. (2025f). *Risk Management.* ServiceNow. https://www.servicenow.com/docs/bundle/yokohama-governance-risk-compliance/page/product/grc-risk/concept/grc-risk-overview.html

ServiceNow. (2025g). *ServiceNow – The smarter way to workflow*. ServiceNow. https://www.servicenow.com/

Singh, K. (2025, March 5). *What is Push Notification Authentication and How it Works? Loginradius.* https://www.loginradius.com/blog/identity/push-notification-authentication

Terekhov, V. (2024, February 8). Multi-Factor Authentication: Enhanced Security Guide. *Attractgroup*. https://attractgroup.com/blog/the-importance-of-multi-factor-authentication/

Tsai, J. (2024, April 10). *IT technician salary expectations*. Spiceworks. https://www.spiceworks.com/it-careers/it-technician-salary-expectations/

Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

Vickers, S. (2025, March 6). *The cyber talent challenge: Bridging the gap in cybersecurity workforce development*. Leidos. https://www.leidos.com/insights/cyber-talent-challenge-bridging-gap-cybersecurity-workforce-development

Virus Total (2024). VirusTotal Intelligence Introduction. *VirusTotal. https://docs.virustotal.com/docs/virustotal-intelligence-introduction*

Wright, G. (September 15, 2024). What is Access Control? *Tech target.* https://www.techtarget.com/searchsecurity/definition/access-control

Yasar, K. (2024, November 26). What is a cloud-native application? TechTarget. https://www.techtarget.com/searchcloudcomputing/definition/cloud-native-application

Zapier. (2025). *Email Parser by Zapier*. Zapier. https://parser.zapier.com

Appendix

Total Project Cost of Y2025 & 2026

	2025	2026
Planning and Testing Cost		
Planning and Testing		
Incident Response Planning	$5,000	$0
Scenario Design	$17,500	$0
Tabletop Exercise Preparation	$8,500	$0
Tabletop Exercise Delivery	$15,000	$15,000
Ongoing Assessment & Update	$8,500	$8,500
Consultation Fee	$100,000	$0
Insurance coverage		
Cyber Liability Insurance	$15,000	$15,000
	$169,500	**$38,500**
Staff cost		
24/7 Training and Support Team		
Tier 1 IT Support Specialists x 10	$600,000	$630,000
Tier 2 IT Support Specialists x 10	$357,500	$375,375
Awareness Training Materials (KnowBe4)	$200,000	$200,000
	$1,157,500	**$1,205,375**
Software cost		

ServiceNow			
Requesters license (10,000 users)		$0	$0
Security Incident Response Model (100 users)		$90,000	$90,000
Integration Hub License		$1,200	$1,200
Annual Maintenance Fee		$0	$200
Precision Bridge			
Migration Fee		$4,950	$0
Microsoft			
Authenticator (MFA)		$0	$0
Azure Extra ID P1 (10,000 users)		$720,000	$720,000
Zapier			
Email Parser		$7,188	$7,188
VirtusTotal			
Premium (Enterprise)		$15,000	$15,000
Splunk, IBM Qradar (SIEM)		$25,000	$25,000
CrowdStrike, Carbon Black (EDR)		$25,000	$25,000
		$888,338	**$883,588**
Hardware Cost			
Laptops/Desktops			

HP Business Laptops (i7, 16GB RAM, SSD) x 20	$30,000	$0
Monitors & Accessories		
24–27" Monitor, Docking Station, Mouses x 20	$12,000	$0
Printers/scanners		
HP Colour LaserJet x 3	$3,000	$0
Switches, routers, APs		
Cisco Catalyst 9400 (switches) x 2	$2,400	$0
Cisco ASR 1000 Series (router) x 2	$4,000	$0
Catalyst 9100 Series (APs) x 4	$3,200	$0
Local backup		
Synology 16 Bay RackStation RS4021xs x 2	$12,000	$0
Maintenance & Upgrade Fee		$2,000
	$66,600	**$2,000**
Total cost	**$2,281,938**	**$2,129,463**