UNCLASSIFIED

ESDC's Virtual Assistant EVA Foundation

Technical Design and Concept of Operations

Version 0.2

Artificial Intelligence Center of Enablement

Innovation, Information, and Technology Branch (IITB)

March 2025

1 Revision History

Version #	Description	Date	Author
0.1	Initial version	Jan 25, 2025	Kristel Parsons
0.2	Updated entire document to use the official business requirement template provided by EPMO.	Feb 10, 2025	Kristel Parsons
0.3	Completed requirements for Domain Assistant	Feb 25, 2025	Kristel Parsons
0.4	Added information for testing and validation, prioritization, and included more details for accessibility.	March 7, 2025	Kristel Parsons

Table of Contents

2 About this Document

2.1 Document Purpose

The purpose of this document is to communicate a clear and comprehensive understanding of the technical specifications needed for the design, deployment and integration of ESDC's Virtual Assistant (EVA) Foundation. It also outlines the Concept of Operations (ConOps) for hosting the EVA solution: **EVA Chat** and **EVA Domain Assistant** in Azure Cloud within the ESDC's secure infrastructure.

This document serves as a reference point for all parties involved, ensuring alignment and understanding across the organization. Any changes to the scope or requirement details will be reflected in the document's revision history.

2.2 Intended Audience

Table 1: Intended Audience

Stakeholder	Role
EVA Solution Architecture Team	Responsible for the solution architecture systems/subsystems roles, their associated relationships and connectivity to other actors and components in the solution.
EVA Solution project leaders	Overseeing project timelines and deliverables.
EVA Solution Developers	Implementing the required code for the solution as per the functional requirements.
AICoE Management team	Executives, DGs, and Directors providing high-level management and strategic direction.
Subject Matter Expert (SME)	Specialists in domain architectures including Business Architecture, Application Architecture, Enterprise Architecture, IM Architecture, and IT Security.
Cloud Administrators	Responsible for installing, maintaining and upgrading any software or hardware required to efficiently the EVA solution.
Other partners and stakeholders	As identified throughout the project lifecycle.

2.3 References

The following documents were used as references when creating this document.

Table 2: References

Document Name	Link		Version

Business Case	EVA Foundation Business Case	Marco Presta	V1
Business Requirements Document	AICoE-PROJ-EVAFoundation-BusinessRequirementsDocument-v2.docx	Kathleen Ayre and Stephanie Leach	V2
EVA Foundational Requirements Management Matrix	EVA Foundational Requirements Management Matrix.xlsx	Kathleen Ayre and Stephanie Leach	V1
Cloud Connective Questionnaire – EVA Chat	Cloud Connectivity Questionnaire (SA-ID1216) EVA Chat (work-in-progress).docx	Abdur Rafey Matin	V0.1
Cloud Connective Questionnaire – Supplementary Material - EVA Chat	Cloud Questionnaire - Supplemental material (SA-ID1216) EVA Chat V1.0.docx	Abdur Rafey Matin	V1
EVA IT Security Role Based Access Control	EVA - IT Security Role Based Access Control (RBAC) -V1.0.docx	Abdur Rafey Matin	V1
EVA Chat Security Assessment	EVA Chat Security Assessment Questionnaire (Protected B)	Abdur Rafey Matin	
EVA Cloud Solution Audit Strategy	AICoE EVA Cloud Solution Audit Strategy v1.docx	Abdur Rafey Matin	V1
EVA Cloud Contingency and Technical Recovery Plan	AICoE EVA Cloud Contingency and Technical Recovery Plan_V1.docx	Abdur Rafey Matin	V1
EVA Cloud Incident Management process	AICoE EVA Cloud Incident Management process V1.docx	Abdur Rafey Matin	V1
EVA Domain Assistant - RBAC	AICoE EVA DA IT Security Role Based Access Control (RBAC) V1.docx	Abdur Rafey Matin	V1

3 Executive Summary

This project is led by the AI Centre of Enablement (AI COE) within ESDC's Innovation and Information Technology Branch (IITB), in collaboration with Shared Services Canada (SSC). The ESDC's Virtual Assistant (EVA) Foundation is a generative AI (GenAI) platform aimed at enhancing the productivity and efficiency of employees within Employment and Social Development Canada (ESDC), Labour, and Service Canada.

The architecture for EVA prioritizes accessibility, privacy and security in alignment with the department's mandates and the broader Government of Canada (GC) standards. Approved by the Enterprise Architecture Review Board (EARB) on January 29, 2025, ESDC's Virtual Assistant (EVA) includes two **core** applications:

- **EVA Chat**
  - Uses the capabilities of a large language model (LLM) to generate ungrounded responses.
  - Designed as a generative AI work-aid tool for tasks such as document editing, coding, summarizing, and other routine tasks.
- **EVA Domain Assistant**
  - Uses Retrieval Augmented Generation (RAG) AI framework to generate grounded responses.
  - Uses ESDC's internal datasets for more specific, domain-relevant answers.

Hosted in a Protected B Azure environment, the EVA platform complies with ESDC, Canadian Centre for Cyber Security (CCCS), and Government of Canada (GC) standards for privacy, security and accessibility. EVA addresses critical security and compliance issues identified with public tools like OpenAI's ChatGPT, offering a safe, reliable GenAI experience for GoC employees.

Expected Outcomes

EVA is expected to deliver significant benefits for the department. It supports our goals to improve efficiency, enhance services, and promote responsible AI use. The following outcomes apply to employees, clients, and the department.

3.1.1 For employees

- **Enhanced Productivity**

  EVA streamlines tasks such as document handling, coding, summarizing, and research. This allows employees to focus on creative and strategic work, boosting overall productivity.

- **Improved Decision Making**

  While EVA Chat and EVA Domain Assistant offer strong AI support, users must review the output for accuracy. Combining AI insights with personal expertise ensures better, more trustworthy decisions.

- **Increased Understanding of GenAI**

  Regular interaction with EVA will build employees' familiarity with GenAI, enabling them to use AI tools responsibly in their work.

- **Accessibility & Inclusivity**

  Meeting Government of Canada accessibility standards and offering support in both French and English, EVA is usable by all employees, including those with disabilities.

3.1.2 Client Outcomes

- **Faster and More Accurate Service Delivery**

  EVA helps staff quickly retrieve accurate information, reducing wait times and enhancing service quality.

- **Around-The-Clock Availability**

  With 24/7 access, EVA ensures that client queries and tasks receive prompt attention, even outside regular hours.

- **Improved Client Interactions**

  As employees manage complex tasks more efficiently, client interactions become smoother and more personalized, increasing overall satisfaction.

3.1.3 For IITB

- **Responsible Integration of GenAI**

  Implementing EVA is a key step in our digital transformation. Its ethical and secure AI standards boost our reputation and leadership in responsible AI use.

- **Cost-efficient Operations**

  EVA's cost recovery model—billing users based on usage—helps manage expenses while providing advanced AI tools.

- **Scalability and Future-Readiness**

  EVA's flexible design allows us to expand our AI capabilities as needs evolve, keeping us current with technological advances.

- **Strengthened Data Security and Compliance**

  Hosted in a Protected B environment and compliant with CCCS protocols, EVA ensures that sensitive data remains secure.

- **Enhanced Organizational Efficiency**

  By simplifying tasks and improving access to key data, EVA increases overall efficiency, helping us meet our operational goals and better serve Canadians.

A detailed business requirements document can be accessed here → AICoE-PROJ-EVAFoundation-BusinessRequirementsDocument-v2.docx

4 Risks, Assumptions and Constraints

This section identifies potential risks, ranging from security and privacy concerns to adoption challenges and it outlines strategies to mitigate their impact. This section also highlights any assumptions and constraints, such as dependencies on external systems or architectural decisions that could impact the project's scope, timelines, or deliverables.

4.1 Risks

#	Description	Impact	Probability	Mitigation strategy	Applies to
1	The stability of the platform is dependent on the infrastructure and services provided by the vendor.	High	Low	Ensure the platform leverages high-availability configurations and implement resilient architecture.	EVA Chat
2	The quality of responses and features is dependent on the model's capabilities, such as handling images, attachments, and document size.	High	Medium	Utilize multi-region deployments to distribute load and reduce dependency on single data centers. Implement robust failover mechanisms.	EVA Chat and EVA DA
3	Cloud service disruptions (e.g., Azure outages) could lead to temporary platform unavailability.	High	Low	Deploy the platform using high-availability configurations and implement disaster recovery plans.	EVA Chat and EVA DA
4	Disruptions to Microsoft services could result in outages affecting the platforms.	High	Low	Establish a comprehensive Service Level Agreement (SLA) with Microsoft to ensure support during service interruptions.	EVA Chat and EVA DA

5	Model "hallucination" or inaccuracies could result in poor quality outputs if not verified by the end user.	Medium	Medium	Provide clear disclaimers instructing users to verify the outputs against appropriate sources before making decisions.	EVA Chat and EVA DA
6	Data leakage (loss of sensitive info)	High	Medium	Implement a document-scanning mechanism to detect and remove sensitive information before it is stored in the vector database. Ensure scanning occurs during document uploads.	EVA Chat and EVA DA
7	Scalability/capacity issues if user load spikes.	Medium	Medium	Conduct comprehensive performance testing under high-load conditions. Leverage lessons learned from previous deployments. Continue collaboration with CanChat (SSC).	EVA Chat and EVA DA
8	Loss of user data (chat history)	Medium	Low	Implement scheduled snapshots and overnight backups. Collaborate with the database group within IITB to ensure robust data storage and recovery management.	EVA Chat
9	User adoption is slower than usual	Low	Medium	Establish clear communication channels to address user concerns (Teams Channel, Feedback forms, prompting guides, etc.).	EVA Chat and EVA DA
7	Rapidly changing AI regulations or new risks identified	Medium	High	Design a flexible architecture that can adapt to evolving regulatory requirements. Maintain close collaboration with	EVA Chat and EVA DA

				CCCS to proactively address compliance needs.	

4.2 Assumptions, constraints and architectural decisions

#	Description	Applies to
1	EVA Domain Assistant is designed to help programs manage their information in alignment with their specific practices and operational needs. It does not eliminate the requirement for programs to independently track and maintain their documentation.	EVA DA
2	Data governance will be applied to EVA Foundation in the same manner as it is applied across ESDC. Users will be provided with guidance on how to manage their documents and act as data stewards. Please refer to the Business Requirements Document.	EVA Chat and EVA DA

5 Solution overview

5.1 In Scope

This document focuses on the deployment and integration components necessary to support the EVA solution in Azure Cloud. It includes:

1. **EVA Chat architecture**
   a. Using OpenAI models hosted internally or through approved secure channels.
   b. EVA is deployed on Azure Cloud infrastructure using Hub and spoke model.
   c. All traffic will be going through Secure Cloud Enablement Defence (SCED) managed by SSC.
   d. ESDC Cloud infrastructure is exclusively connected to a Virtual Network (VNet).

2. **EVA Domain Assistant**
   a. Based on Microsoft's Info-Assistant PubSec project and the Retrieval Augmented Generation (RAG) framework using Large Language Models (LLMs).
   b. Role-Based Access Control (RBAC) to meet business requirements, uphold privacy, and adhere to the Principle of Least Privilege (PoLP).
   c. EVA Domain Assistant leverages government-owned data repositories to enhance accuracy and context specificity, including:
      i. Retrieval of relevant documents from secure data storage.

ii. Integration with the LLM to generate context-rich responses based on user's input and refined prompts.

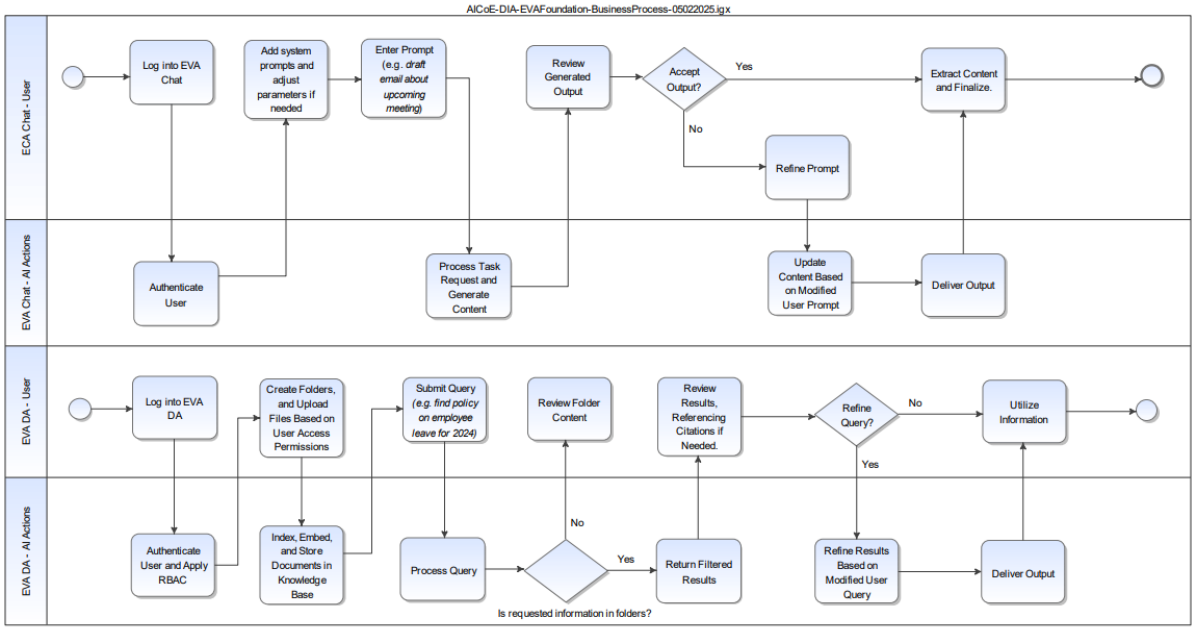
3. **Infrastructure and cloud connectivity**
4. **Audit and compliance**
5. **User interface**
6. **Accessibility**
7. **Incident management and contingency**
8. **Maintenance and testing**

Note: this is an *evergreen* document that will continue to evolve to convey the technical solution design needed to support and maintain EVA.

5.2 Out of Scope

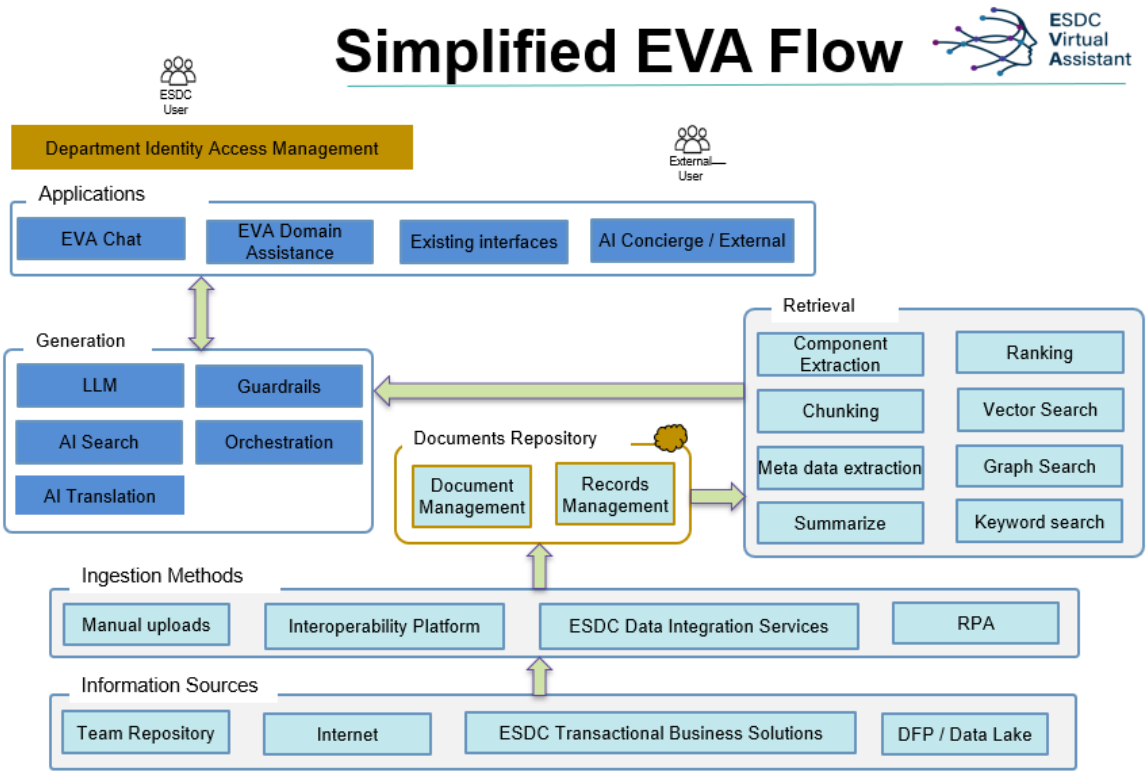
1. End-user training materials. EVA Course is part of a collaboration with College@ESDC and AICoE.
2. Policies for data governance
3. Project deliverables outside of EVA core capabilities (Innovation Fund and Investment Fund projects)
4. Future model upgrades
5. Future enhancements to the user interface

5.3 Business Context Diagrams



AICoE-DIA-EVAF-BusinessProcess-05022025.pdf

5.4 System Context Diagram



6 Solution Requirements

Solution requirements describe the capabilities and qualities of a solution that meets the stakeholder and business requirements. Solution requirements can be divided into two sub-categories:

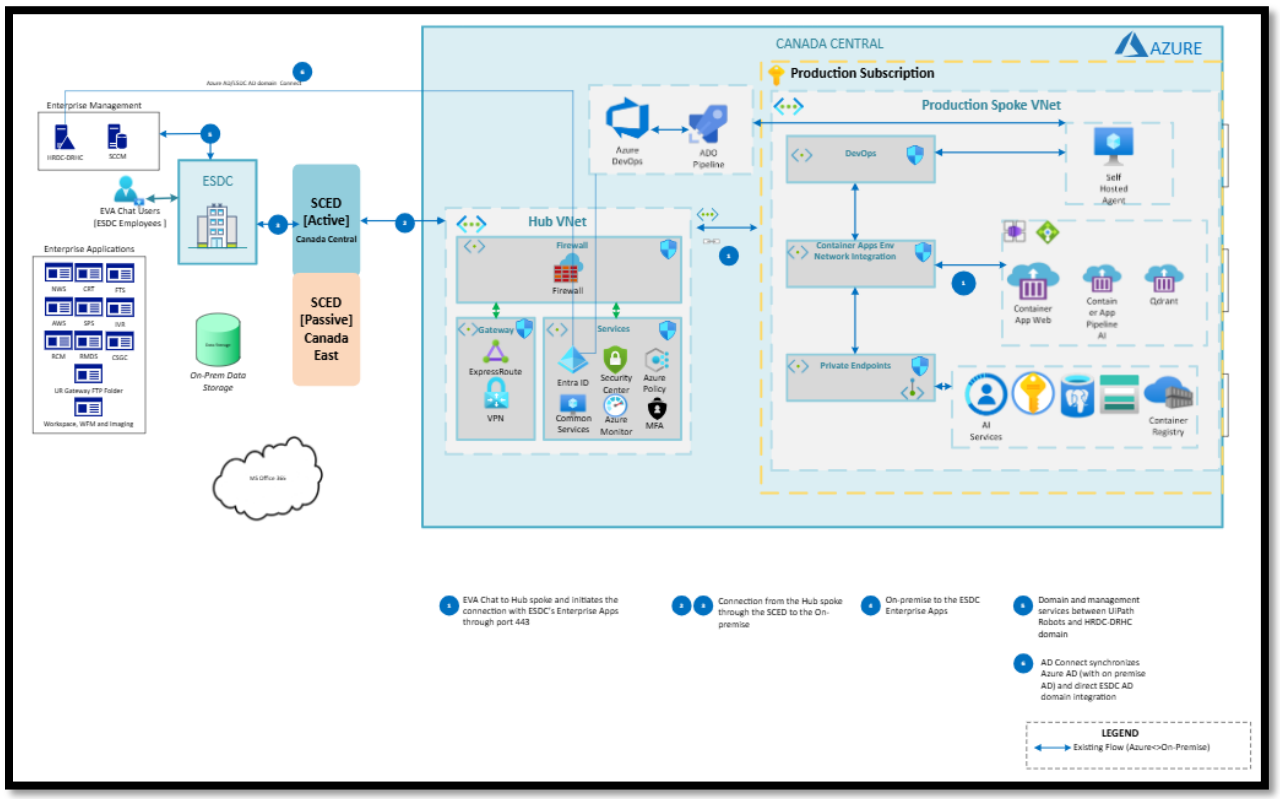
- Functional requirements: describe the capabilities that a solution must have in terms of the behaviour and information that the solution will manage.
- Non-functional requirements: do not relate directly to the behaviour or functionality of the solution, but rather describe conditions under which a solution must remain effective or qualities that a solution must have.

The textual descriptions of solution requirements for **EVA Foundation** are listed in the Requirements Management Matrix available here.

7 Solution requirements – EVA Chat

7.1 Infrastructure Architecture

ID	Requirement	Description	BRD - ID
INF01	Access	The solution will be accessible from any location where GCNet is available. • ESDC Employees (users) will have the ability to access EVA through the web interface. • Users working remotely must be connected to the Virtual Private Network (VPN) to access the platform.	FR01
INF02	Hosting	The EVA Chat platform will be hosted in ESDC's cloud infrastructure and will be exclusively connected to a Virtual Network (VNet) for secure access.	
INF03	User authentication	User authentication and permissions will be handled by Azure Active Directory (AAD) for centralized access control.	
INF04	Traffic management	All inbound and outbound traffic must be routed through the Secure Cloud Enablement Defence (SCED), managed by SSC (Shared Services Canada), to ensure compliance with security policies.	
INF05	SCED Connection and failover configuration	The SCED Connection has a Failover Configuration between the Canada Central and Canada East Data Centres. This is done to enhance the failover capabilities.	



See the detailed diagram here.

7.2 Cloud connectivity

The following section highlights the key requirements that support the security of the cloud connectivity requirements for EVA Chat.

ID	Requirement	Description
CC01	Private cloud connectivity	The solution will establish private and dedicated connections with Cloud Service Providers (CSPs) to ensure secure access and service availability. • EVA Chat will be peered with ESDC's Azure Hub to enable seamless communication. • A dedicated private Azure subscription will be used exclusively for AI services, ensuring resource isolation and security compliance.
CC02	Cloud to Ground connectivity	No direct cloud-to-ground connectivity will exist between Azure Platform as a Service (PaaS) and SSC on-premises systems.

		This restriction ensures **network segmentation** and prevents unauthorized data exposure.
CC03	Internal use and IP address restriction	EVA Chat will be for internal use only and will not be assigned a public IP address.
CC04	Security and traffic management	EVA Chat will utilize Shared Services Canada (SSC) Secure Cloud Enablement and Defence (SCED) Trusted Interconnection Points (TIP) for secure and compliant traffic routing. This ensures all data traffic flows through government-approved secure channels and adheres to GoC Security standards.
CC08	Data center hosting	EVA resources will be hosted in the Azure Canada Central Data Center to ensure compliance with regional data residency requirements. To prevent a single point of failure within the data center, the application will allocate resources across multiple Azure Availability Zones within the Azure Canada Central Data Center.
CC09	Azure Availability Zone Architecture	1. The Azure Availability Zones used by EVA Chat will be physically and logically separated within the data center. • Each zone will have its own independent power source, network infrastructure, and cooling system to enhance system resilience. • The zones will be connected via an extremely low-latency network, ensuring seamless failover and high availability.

7.3 Interoperability

ID	Requirement	Description
IOP01	Integration with other systems or applications	The EVA Chat solution does not integrate with any internal applications. It only interacts with the Cloud Service provider and Large Language Models (LLMs).
IOP02	Configurable Model Selection	EVA Chat will provide configurable options to select and utilize different models based on product needs and in order to maintain service performance for users.

See ST&E Testing Team Demo

7.4 Accessibility

ID	Requirement	Description	BRD - ID
ACC01	Compliance	EVA Chat will follow accessibility guidelines based on GoC requirements: Standard on Web Accessibility- Canada.ca	NF06
ACC02	Bilingualism	EVA Chat will comply with bilingualism guidelines based on GoC requirements.	FR09 BR03
ACC03	Accessibility	EVA Chat will support the following features to ensure usability: • Keyboard navigation • Compatibility with screen readers • Text alternatives • High-contrast modes and font resizing for improved readability. • Speech to text and text to speech functionalities. • Clear error messages	NF-6
ACC04	Browser compatibility	EVA Chat will be compatible with Microsoft Edge, Google Chrome and Firefox.	
ACC05	Device compatibility		
ACC06	Accessibility Testing	Periodic accessibility testing will be conducted to ensure ongoing compliance. See Testing and Validation Strategy.	

7.5 User interface

ID	Requirement	Description	BRD - ID
UI01	User settings	EVA Chat will provide users with the ability to: • Upload documents for processing. • Engage in conversations with the large language model (LLM) currently in use. • Utilize speech-to-text and text-to-speech functionalities for accessibility and ease of use.	FR06 NF-6

UI02	User workspace	Users will have access to a dedicated 'Workspace' feature that allows them to: • Retrieve and interact with models. • Access previously saved prompts. • Manage and utilize stored documents. • Leverage additional workspace functionalities as needed.	
UI03	User permissions	EVA Chat will allow users to configure and manage their experience through the following permissions: • Change language settings. • Modify or add system prompts. • Adjust basic interface options. • Enable or disable memory functionality (default setting: off). • Configure audio settings, including speech-to-text and text-to-speech. • Import, export, archive, and delete chat histories. • Manage user profiles, including customization options.	FR04 FR06 FR07 FR08 FR09
UI03	Archived chats	EVA Chat will provide users with the ability to access and retrieve archived chat history for reference and continuity.	FR11

7.6 IT Security

ID	Requirement	Description	BRD - ID
ITS01	Role-Based Access Control (RBAC)	The EVA Chat solution will implement Role-Based Access Control (RBAC) to restrict access to only authorized users based on predefined roles and permissions.	FR05
ITS02	User roles and access levels	Users will be assigned one of the following roles to control access to platform features:	

		• **Admin**: full administrative privileges, including user management and configuration. • **User**: standard user access to chat functionalities. • **Reader**: read-only access to historical chat data and system logs.	
ITS03	Authentication management	EVA Chat will integrate with Microsoft Entra ID (formerly known as Active Directory) for Single Sign-On (SSO).	
ITS04	Security deployment	The solution will be deployed internally as a secured web-based platform, accessible only to authorized employees within Employment and Social Development Canada (ESDC).	
ITS05	Cloud and hosting flexibility	EVA Chat will be vendor-agnostic and capable of operating in multiple cloud environments or on-premise hosting.	
ITS06	Data encryption	• All in-transit data will be encrypted using Transport Layer Security (TLS) version 1.3 to protect against interception. • Data at rest will be encrypted using Microsoft-managed encryption keys, with configurable options to adjust encryption settings based on security needs.	
ITS07	API exposure restrictions	EVA will not expose any external APIs to unauthorized parties, mitigating the risk of data breaches and ensuring compliance with security best practices.	

EVA - IT Security Role Based Access Control (RBAC) -V1.0.docx

EVA Chat Security Assessment Questionnaire (Protected B)

8 Solution Requirements – EVA Domain Assistant

8.1 Infrastructure architecture

ID	Requirement	Description	BRD - ID
INF01	Access and authentication	ESDC Employees (users) must have the ability to access EVA through the web interface.	FR01
INF02	Hosting	EVA will be hosted in ESDC's cloud infrastructure, exclusively connected to a Virtual Network (VNet) and private endpoints.	

See the detailed diagram here.

8.2 Cloud connectivity

ID	Requirement	Description
CC01-DA	Cloud connection	EVA Domain Assistant's code will be managed using Azure DevOps, including EVA configuration and execution. The code is stored in Azure DevOps ESDC-AICoE Team Repository, within the EVA Portal Project. eva-info-asst - Repos The code is executed from a Docker file through Azure pipelines.
CC02-DA	Containerized Development Environment	1. The deployment process will utilize the *Developing Inside a Container* concept to containerize all required pre-requisite components. 2. The development environment will be created using a development container (dev container) hosted on a virtual machine via GitHub Codespaces.
CC03-DA	Baseline configuration	The Admin Configuration provides control over the application's settings, allowing administrators to configure various aspects of the EVA Chat application. In contrast, Normal Users will only have access to the Baseline Configuration, enabling them to use the application solely for chat purposes.
CC04-DA	Baseline configuration reviews and updates	A quarterly meeting will be held throughout the year to review the current baseline configuration and determine whether any changes are required.

8.3 Interoperability

ID	Requirement	Description	BRD - ID
IOP01	Interoperability	No integration with other internal applications. The Domain Assistant will only interact with OpenAI services and large language models (LLMs).	

See ST&E Testing Team Demo

8.4 Accessibility

ID	Requirement	Description	BRD - ID
ACC01	Accessibility	EVA Domain Assistant will follow accessibility guidelines based on GoC requirements. See Standard on Web Accessibility- Canada.ca	NF06
ACC02	Bilingualism	EVA DA must comply with bilingualism guidelines based on GoC requirements.	FR14

8.5 User interface

ID	Requirement	Description	BRD - ID
UI01	Baseline configuration for regular Domain Assistant users	Users have access to the following customizations within the Domain Assistant: - Select the number of documents to be retrieved from search. - Select User Persona - Select System Persona - Configure the response length and conversation type - Select the folder(s) to narrow the search. - Use tags to restrict the search to only the relevant documents.	

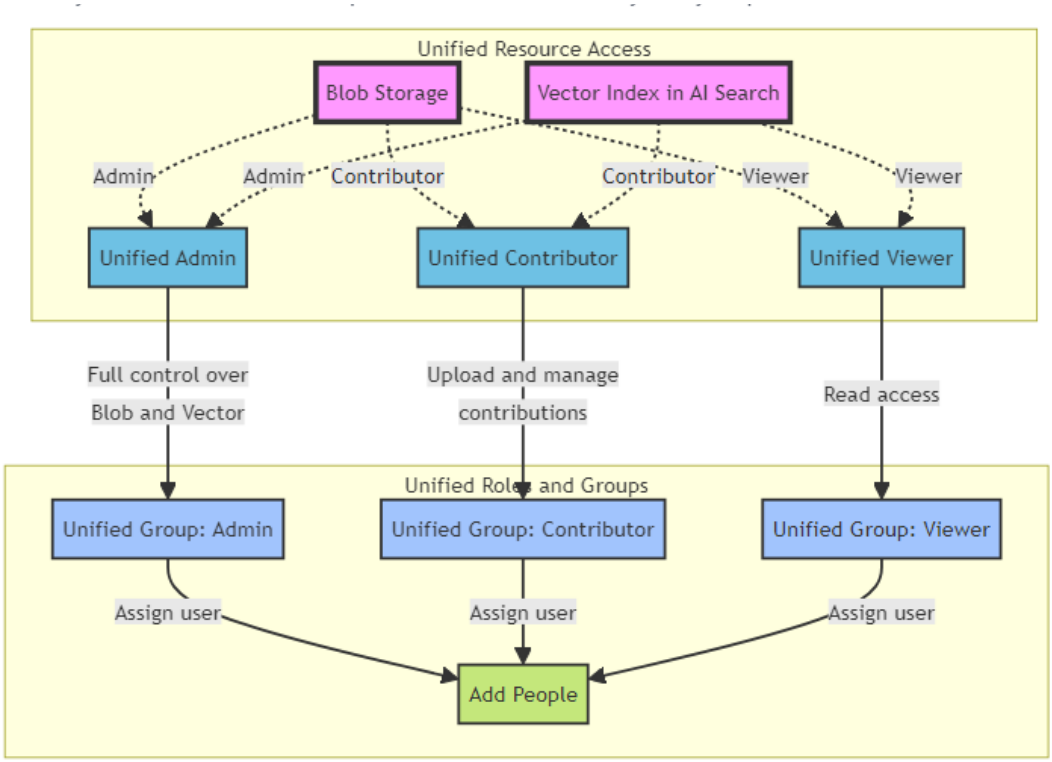
UI02	User settings	EVA Domain Assistant will provide users with the ability to:
		• Upload documents for processing and manage content after upload. See IT Security for details on access control.
		  • Engage in conversations with the large language model (LLM) currently in use.
		  • Utilize speech-to-text and text-to-speech functionalities for accessibility and ease of use.
		  • Translate documents between the two official languages.
			FR14
			FR16
			FR19
			FR20

8.6 IT Security

ID	Requirement	Description
IT01-DA	Access control	Users will be organized into groups which will be associated with different levels of access.
IT02-DA	User roles for DA configuration	There will be three unified custom roles: 1. **Admin**: with the ability to manage both Blob storage and Vector Index. 2. **Contributor**: can upload documents to Blob storage and manage contributions to Vector Index. Contributors have all the permissions from Viewer. 3. **Viewer**: Read/query documents in Blob storage and view Vector Index data.
IT03-DA	File upload and processing	Before any processing begins, the system will determine the appropriate Blob Storage and Vector Index based on the user's group. This ensures that documents are stored and processed in the correct location according to the user's role.
IT04-DA	Role verification	Once storage resources are identified, the application will validate the user's role through Azure AD. Users are assigned one of three primary roles
IT05-DA	Access control for users	Before allowing file uploads, the application checks the user's permissions:

		- **Admin**: Has full access, including the ability to upload, manage, and delete files. - **Contributor**: Can upload and manage files but does not have full administrative rights. - **Viewer**: Has read-only access and cannot upload or modify files. -

AICoE EVA DA IT Security Role Based Access Control (RBAC)_V1.docx



8.7 Data processing

ID	Requirement	Description
DP01	Document processing	When a file is uploaded to a Blob Storage container, the FileUploadedFunc, will be triggered. This is a function responsible for determining the appropriate processing path based on the file type.
DP02	File type detection	Domain Assistant will identify whether the uploaded file is text-based or non-text:

		- Text-based files are further classified as PDF or Other text formats. - Non-text files are categorized as images or media.
DP03	Queue Management	Based on the file type, Domain Assistant routes the file to the appropriate Azure Queue for processing: • PDFs are sent to pdf_submit_queue for form recognition and polling. • Non-PDF text files are processed for layout parsing in non_pdf_submit_queue. • Images are sent to image_enrichment_queue for processing. • Media files are sent to media_enrichment_queue for enrichment.
DP04	Storage and output	The final processed documents will be stored back in Blob Storage. Any additional embeddings or enrichment data are saved in their respective containers for future retrieval.

9 Other requirements for EVA Chat and EVA Domain Assistant

9.1 Audit and compliance

ID	Requirement	Description	BRD - ID
AUD01	Log monitoring	There will be weekly log monitoring, with all logs securely stored in Azure Logs to ensure traceability and compliance with security policies.	
AUD02	Log monitoring and storage	1. Any investigation related to suspicious or unauthorized activities will be conducted in accordance with departmental policies. 2. Information entered in EVA DA will not be included in logs unless explicitly requested due to architectural or compliance requirements.	

		3. Azure logs will only capture whether a request was made and whether it was successfully processed. 4. Audit records will be securely stored in an Azure app container with daily incremental backups to ensure data integrity and recoverability.	
AUD03	Data privacy and retention	EVA DA will support flexible chat history settings to accommodate potential future modifications in data retention policies. See Directive on Data Management and Analytics for the Enterprise Data Foundations Platform. Appendix J: Standard on Systems that Manage Information and Data- Canada.ca	
AUD04	Chat history	Chat history will be retained for a minimum of 7 days and a maximum of 35 days, in accordance with standard best practices. The retention period will be configurable based on ESDC's policy requirements.	FR22
AUD05	User logs	User logs will remain fully anonymized unless otherwise indicated by the Sponsor and/or Product Owner.	
AUD06	User inputs	User inputs will not be utilized to retrain Large Language Models (LLMs), ensuring user privacy and preventing unintended data exposure.	
AUD07	Content filtering	EVA Chat will implement Microsoft content filtering to prevent the use of threatening or criminal language, as well as any misuse of the platform. The filtering mechanism will ensure compliance with organizational and security policies to maintain a safe user environment.	

AICoE EVA DA System Development Life cycle & Security Engineering.docx

9.2 Incident and contingency planning

ID	Requirement	Description	BRD - ID
INC01	Incident identification	There will be mechanisms to detect and log incidents, including but not limited to: • System failures or outages. • Security breaches or unauthorized access attempts. • Performance degradation affecting user experience. • Errors in AI model responses. Real-time alerts and logs will be generated to facilitate timely resolution.	
INC02	Communication	1. There will be automated alerts to system administrators upon incident detection. 2. Notification to affected users when system downtime or degradation occurs. 3. Regular status updates during critical incidents will be communicated via the Teams Channel. 4. Post-incident reports summarizing root cause analysis and corrective actions.	
INC03	Contingency	EVA Chat and EVA DA will have contingency measures in place to minimize disruptions, including: • Automated failover mechanisms to backup servers in case of system failure. • Redundancy measures to maintain service availability. • A recovery plan to restore functionality within a predefined timeframe. • Data integrity measures, such as scheduled backups and disaster recovery protocols.	
INC04	NSD incident routing	• Users will have the ability to submit a ticket using the National Service Desk (NSD) to log	

		any issues with the user interface, defects or questions about EVA's performance issues.	

For more details about the incident management process, please refer to:
AICoE EVA DA Cloud Incident Management process_V1.docx

9.2.1 AICoE Team – Infrastructure Team Contact information

Role	First / Last Name	On-Call Phone:	Cell Phone:	Email:
AICoE Director	Todd Whitley	N/A	N/A	Todd.Whitley@hrsdc-rhdcc.gc.ca
AI/RPA Infrastructure Manager	Eric Cousineau	N/A	N/A	Eric.Cousineau@hrsdc-rhdcc.gc.ca
AICoE Manager	Blake Niasha	N/A	N/A	Blake.Niasha@hrsdc-rhdcc.gc.ca
Senior Technical Advisor	Thaya Shanmugaratnam	N/A	N/A	thaya.shanmugaratnam@hrsdc-rhdcc.gc.ca
Senior Technical Advisor	Abdur Matin	N/A	N/A	Abdur.matin@hrsdc-rhdcc.gc.ca

9.2.2 Service Owners

Role	Primary Contact	Secondary Contact	Responsibilities
Product Owner	Todd Whitley todd.whitley@hrsdc-rhdcc.gc.ca	Niasha Blake niasha.blake@hrsdc-rhdcc.gc.ca	Lead for the overall technical solution Operational coordination and management
Business Owner	Todd Whitley todd.whitley@hrsdc-rhdcc.gc.ca		Lead for the overall business service Operational coordination and management

Senior Technical Lead			Lead for the overall EVA Solution for the Department
Lead, EVA Cloud Infrastructure, Automation Infrastructure Services (AIS), IITB	Thaya Shanmugaratnam thaya.shanmugaratnam@hrsdc-rhdcc.gc.ca		Operational oversight and coordination of the cloud solution resources
Lead, EVA Solution	Shannon O'Rourke shannon.orourke@servicecanada.gc.ca		Lead for EVA Solution, End to End Connectivity
Cloud Centre of Excellence (CCOE)	Dirk Vieira dirk.vieira@hrsdc-rhdcc.gc.ca	Tyler Schiemann tyler.schiemann@hrsdc-rhdcc.gc.ca	Strategic guidance and advice concerning ESDC Cloud enterprise environment.
Lead, Cloud Operations	Dirk Vieira dirk.vieira@hrsdc-rhdcc.gc.ca	Tyler Schiemann tyler.schiemann@hrsdc-rhdcc.gc.ca	Operational oversight and execution of the ESDC Cloud Managers of the "Hub"
Lead, IT Security	Nathalie Delisle Nathalie.delisle@hrsdc-rhdcc.gc.ca		Lead for ESDC IT Security.

9.3 Backup and Recovery

ID	Requirement	Description	BRD - ID
BRec01	Backup restoration capability	EVA Chat and EVA DA will have the capability to restore servers and databases from backups in the event of a failure. The Automation Infrastructure Services (AIS) team will follow standard operating procedures (SOPs) to restore systems from failures.	

		Note: Backup recovery will be subject to the available capacities and limitations of the Azure cloud infrastructure. If the Azure Canada Central Data Center experiences a failure, service restoration will depend on Microsoft's ability to recover the data center.	
BRec02	Recovery steps	The AIS team will oversee Robotic Process Automation (RPA) Cloud Infrastructure, ensuring alignment with recovery procedures. Please refer to this document for steps: AICoE EVA Cloud Contingency and Technical Recovery Plan_V1.docx	
BRec03	Recovery capability	EVA resources, such as Container Apps (App Web and App Pipeline AI), Postgres SQL Database and Private Endpoint must be backed up on Azure Cloud daily incremental.	
BRec04	Dual authentication for Azure logs	EVA Chat will store logs in the App Container Logs, including POST, GET, and request status information. Access to these logs will require dual authentication: • The user will authenticate using Microsoft Entra ID to log in to the Azure Portal. Once inside the portal, the user will require special access permissions to view or delete the logs.	
BRec05	Dual authentication for PostgreSQL	EVA Chat will store chat history in the PostgreSQL database and Volume File Share. Access to this data will require dual authentication: 1. The user will authenticate using Microsoft Entra ID to log in to the Azure Portal. 2. Once at the database level, the user will require additional Active Directory (AD) group membership permissions to access PostgreSQL database records.	
BRec06	Outages	In the event that EVA Chat or EVA DA is not responsive, the AICoE team will send a notification via the Teams Channel to users indicating the application is down. The AICoE and AIS team will	

		work together to rebuild the infrastructure and re-deploy the solution to restore it if needed.	

AICoE EVA DA Cloud Contingency and Technical Recovery Plan_V1.docx

10 Investment Fund and Innovation Fund Projects

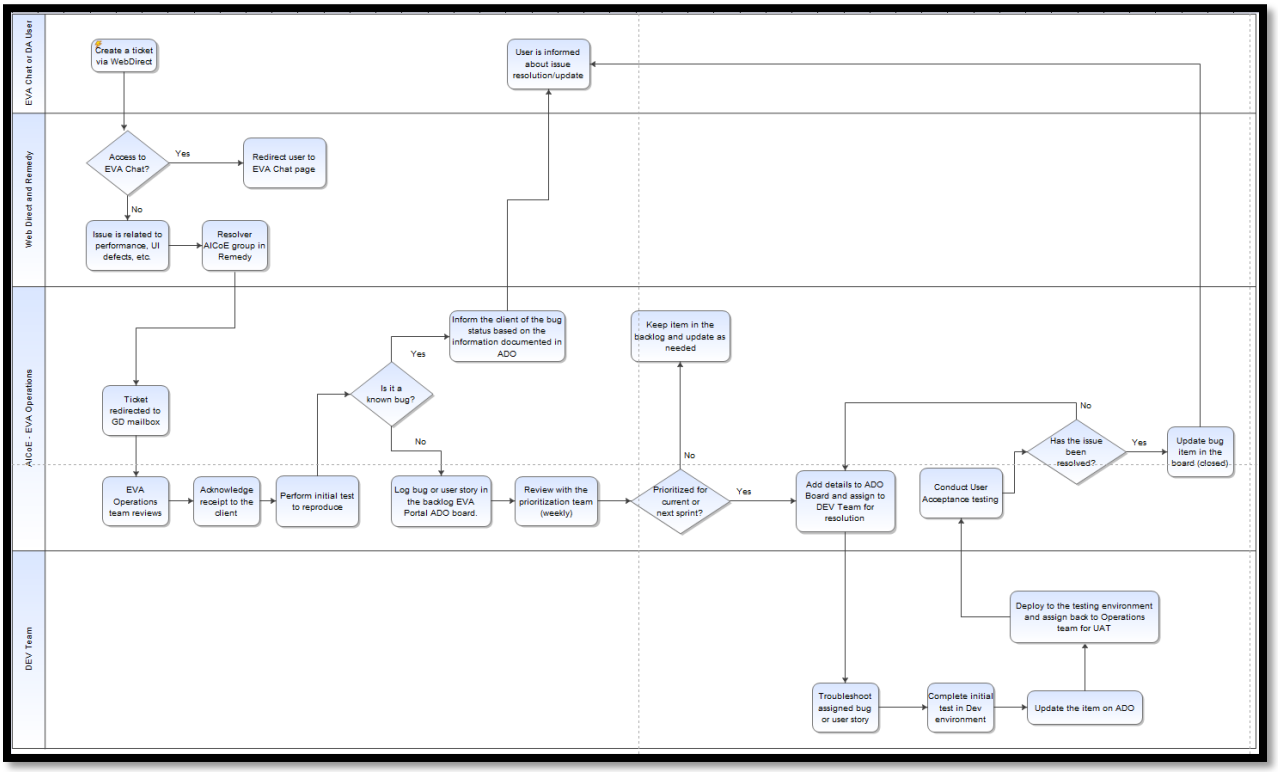
This section outlines the various projects that are currently in progress that will be using EVA Foundation core capabilities with additional customizations to meet clients' needs.

AI-CoE Project List_Aug2024.docx

11 Prioritization of defects and enhancements

1. The AICoE Development team will be responsible for making any changes to the code related to bugs, enhancements or configuration.
2. Future enhancements can come from different sources, from an end-user, due to model upgrades, new features to improve user experience, based on new compliance requirements or new GoC standards and regulations.
3. Enhancements will be reviewed by the management team for prioritization and release planning.

Process flow for logging issues in the ADO board.



12 Testing and Validation Strategy

12.1 Testing and documentation

The AICoE Development team will be responsible for making any changes to the code related to bugs/enhancements, or configuration based on the prioritization process.

1. The EVA Chat application is configured through the group variables. Any changes to these items, will be tested by the development team before deploying the changes to the Production.
2. The developers will create test plans and execute those on the code.
3. Every change will be documented in the GitHub through version control History.
4. For information on continuous monitoring of the applications, please refer to AICoE EVA DA System Development Life cycle & Security Engineering.docx

13 Organizational units

The subsequent table identifies the various service owners, primary / secondary contacts, and which service(s) they are responsible for.

Role	Primary Contact	Secondary Contact	Responsibilities
Product Owner	Todd, Whitley (Todd.whitley@hrsdc-rhdcc.gc.ca)	Niasha Blake niasha.blake@hrsdc-rhdcc.gc.ca	Lead for the overall technical solution. Operational coordination and management
Business Owner			Lead for the overall business service. Operational coordination and management
Lead, AICoE- EVA Solution			Lead for EVA Solution Development
Owner, Azure Cloud Infrastructure (RPA/AI)	Poma Ilambo Poma.ilambo@hrsdc-rhdcc.gc.ca	Eric Cousineau Eric.cousineau@hrsdc-rhdcc.gc.ca	Operational oversight and coordination of the RPA AI Solution in Azure Cloud
Lead, Cloud Operations	Thaya Shanmugaratnam thaya.shanmugaratnam@hrsdc-rhdcc.gc.ca	Andrew Hillyard andrew.hillyard@hrsdc-rhdcc.gc.ca	Operational oversight and execution of the ESDC Cloud Managers of the “Hub”
Lead, IT Security	Daigle, Maria MD maria.daigle@hrsdc-rhdcc.gc.ca		Lead for ESDC IT Security.
EVA Project Coordinator	Mario Lozano mario.lozano@hrsdc-rhdcc.gc.ca		EVA Solution Project Coordinator

RPA- EVA Solution Administrators	Andrew Hillyard andrew.hillyard@hrsdc-rhdcc.gc.ca	Zihan Zhao zihan.zhao@hrsdc-rhdcc.gc.ca	Administrator for EVA Cloud Solution

14 Acronyms

Acronym	Definition
AI	Artificial Intelligence
AICoE	Artificial Intelligence Centre of Enablement
CAB	Change Advisory Board
CCOE	Cloud Centre of Excellence
CCCS	Canadian Centre for Cyber Security
CI/CD	Continuous Integration and Continuous Deployment
ConOps	Concept of Operations
DevOps	Development and Operations
ESDC	Employment and Social Development Canada
EVA	ESDC Virtual Assistant
EVA DA	EVA Domain Assistant
GenAI	Generative Artificial Intelligence
GD Mailbox	General Delivery Mailbox
GoC	Government of Canada
IaaS	Infrastructure as a Service
IT	Information Technology
NSD	National Service Desk
OCMC	Operations and Change Management Committee
PaaS	Platform as a Service
POB	Program Operations Branch
PoLP	Principle of Least Privilege
RAG	Retrieval-Augmented Generation

SCCM	System Center Configuration Manager
SCDE	Secure Cloud Enablement Defence
SQL	Structured Query Language
SROC	Supplementary Record of Claim
SSC	Shared Service Canada
UTC	Coordinated Universal Time
VNET	Virtual Network
VM	Virtual Machine
VPN	Virtual Private Network

15 Appendices

15.1 Glossary

15.1.1 Definitions

Term	Definition

15.2 Requirements Management Matrix

EVA Foundational Requirements Management Matrix.xlsx