**PROTECTED B**

# GenAI Copilot for Curam to Assist Agents

Benefits Delivery Modernization

Service Canada

# High Level Assessment

CYBER AND IT SECURITY

INNOVATION, INFORMATION AND TECHNOLOGY BRANCH

| | |
|---|---|
| Document Version Status: | FINAL |
| Document Version Number: | 1.1 |
| Document Version Date: | 2024-04-12 |

## Document Revision History

| Version | Description | Name | Date |
|---|---|---|---|
| 0.1 | Initial Draft – Basic formatting and title/labels entries | Dan Bastianello | 2024-03-25 |
| 0.2 | Initial internal review | Andrea Lemieux/ Erin Rowlinson | 2024-04-02 |
| 0.3 | Initial internal editing review | Beth Roodman | 2024-04-04 |
| 0.4 | Second internal review | Erin Rowlinson | 2024-04-05 |
| 0.5 | Additional clean up and review | Erin Rowlinson | 2024-04-08 |
| 1.0 | Final review after discussion with management | Dan Bastianello | 2024-04-10 |
| 1.1 | Removal of ACME consolidated risks | Erin Rowlinson | 2024-04-12 |

## Summary

ESDC IT Security was asked to review and provide comments and recommendations on the use of the GenAI Copilot for Curam to Assist Agents (Copilot) solution.

Copilot is an AI virtual assistant that provides information from sources such as knowledge articles from Release 1 of the Curam environment knowledge base. Copilot will be deployed to a limited number of agents (10). Copilot is classified as Unclassified, Low Integrity, and Low Availability (ULL).

- Case workers are required to review multiple sources of information, such as knowledge articles, user guides, policies, etc., from knowledge management systems when processing cases. This can be time consuming as the information is scattered across multiple platforms.
- Copilot is supported by a knowledge base containing knowledge articles, FAQs, Curam user guides, policies, and procedures that can be queried by case workers seeking information related to policies, benefits eligibility, and Curam guidelines and processes.

Please note that this High Level Assessment (HLA) is being used to support an Authority to Operate (ATO) in place of a full Security Assessment and Authorization (SA&A).

The solution will be required for August 2024 and is requesting early signoff to enable an initial pilot for 10 users, which will be scaled up to 100 users, and will be performed in a production environment prior to full integration in OAS.

## Risks/Concerns

- Risk to Confidentiality and Integrity because phased out TLS 1.2 ciphers potentially continue to be enabled
    - Risk: **MEDIUM**
    - Safeguard: To mitigate this risk would require the Copilot team to disable all ciphers that are deemed phased out as per ITSP.40.062. The following table of ciphers would need to be disabled:

      TLS_RSA_WITH_AES_256_GCM_SHA384
      TLS_RSA_WITH_AES_128_GCM_SHA256
      TLS_RSA_WITH_AES_256_CBC_SHA256
      TLS_RSA_WITH_AES_256_CBC_SHA
      TLS_RSA_WITH_AES_128_CBC_SHA256
      TLS_RSA_WITH_AES_128_CBC_SHA
      TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA

      The current implementation of Copilot does not allow the configuration of ciphers on the resources within the resource group. A possible solution would be to use an API proxy which allows ciphers to be enabled or disabled.

## Conclusion

ESDC IT Security has highlighted security concerns related to Copilot. If the client decides to go ahead with this initiative, IT Security strongly recommends implementing all safeguards identified in this document.

**Note:** This high level assessment of Copliot is comfortable with the limited and full use of the solution. Should the implementation, data classification, or data sources change significantly, an additional assessment up to and including a full SA&A might be required.

## Background

ESDC IT Security was asked to perform an HLA of Copilot. This type of assessment does not involve security testing. It is primarily a review of the security controls.

## Security Assessment In Scope

The scope of this HLA was limited to Copilot and focused on evidence provided for Copilot only.

The following items were assessed and are considered in scope for this HLA:

- Copilot ESDC Azure subscription Resource Group (RG) resources associated with the Large Language Model (LLM)
- Copilot Azure resource configuration and procedures
- ESDC Microsoft 365 SharePoint permissions

**Note:** IT Security compiled and reviewed information from numerous security websites (Microsoft, CVA, US-Cert, etc.) and conducted a general internet search, looking for any publicly disclosed vulnerabilities concerning the in scope items mentioned above. IT Security also reviewed the implementation of the solution in the ESDC network and all relevant security controls.

## Security Assessment Out of Scope

The following items were not assessed and are therefore not considered in scope for this HLA:

- Azure cloud platform
- ChatGPT-4 base model

Copilot is supported by and interacts with existing ESDC IT infrastructure components, systems, and applications. An assessment of this entire ESDC IT infrastructure is outside the scope of this HLA.

Copilot is also supported by and interacts with Shared Services Canada (SSC) IT infrastructure. An assessment of this IT infrastructure is also outside the scope of this HLA.

## Copilot Overview

Copilot is an AI virtual assistant that provides information from sources such as knowledge articles from Release 1 of the Curam environment knowledge base. Copilot will be deployed to a limited number of agents (10). This section provides information on Copilot technical controls and all related processes.

The following table contains ciphers that have been provided by the Copilot team. This list is not currently enabled on the Azure resource group deployment. It was taken from a URL that lists "possible" ciphers. There are only four cipher suites that could be matched to the ITSP.40.062 TLS 1.2 ciphers. The others do not use the standard cipher suite taxonomy found in ITSP.40.062 standard. Some of the listed ciphers may be sufficient or even recommended but this information could not be verified because ciphers cannot be configured in the Azure web console.

| Enabled Cipher | ITSG.40.062 | | |
|---|---|---|---|
| | Recommended | Sufficient | Phased Out |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | Yes | No | No |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | Yes | No | No |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | No | Yes | No |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | No | Yes | No |
| TLS_ECDHE_RSA_WITH_AES_256_SHA384 | No | No | No |
| TLS_ECDHE_RSA_WITH_AES_256_SHA | No | No | No |
| TLS_DHE_RSA_WITH_AES_256_SHA256 | No | No | No |
| TLS_DHE_RSA_WITH_AES_256_SHA | No | No | No |
| TLS_DHE_RSA_WITH_CAMELLIA_256_SHA | No | No | No |
| AES_256_GCM_SHA384 | No | No | No |
| AES_256_SHA256 | No | No | No |
| AES_256_SHA | No | No | No |
| CAMELLIA256_SHA | No | No | No |
| TLS_ECDHE_RSA_WITH_AES_128_SHA256 | No | No | No |
| TLS_ECDHE_RSA_WITH_AES_128_SHA | No | No | No |
| TLS_DHE_RSA_WITH_AES_128_SHA256 | No | No | No |
| TLS_DHE_RSA_WITH_AES_128_SHA | No | No | No |
| TLS_DHE_RSA_WITH_SEED_SHA | No | No | No |
| TLS_DHE_RSA_WITH_CAMELLIA128_SHA | No | No | No |
| AES_128_GCM_SHA256 | No | No | No |
| AES_128_SHA256 | No | No | No |
| AES_128_SHA | No | No | No |
| SEED_SHA | No | No | No |
| CAMELLIA128_SHA | No | No | No |
| TLS_ECDHE_RSA_WITH_DES_CBC3_SHA | No | No | No |
| EDH_RSA_WITH_DES_CBC3_SHA | No | No | No |
| DES_CBC3_SHA | No | No | No |

**Information from Client**

**Product destination**
Azure Cloud

**Target OS**
N/A

**Product lifespan**
LT

**General product functionality**
Copilot is an AI virtual assistant that provides information from sources such as knowledge articles from Release 1 of the Curam environment knowledge base.

Copilot is accessed from a web browser by Azure authenticated users.

**Business drivers and reasons for submitting the proposal**
Copilot provides processing staff with access to knowledge management, processes, and procedures via a chat interface integrated with the OAS on BDM user interface.

**Business functionality requirements**
All information presented by Copilot is accessible to the agent via other mechanisms (e.g. on the knowledge exchange). Copilot provides and enables a productivity aid to allow information to be accessed more easily.

Copilot is implemented within the secure Azure infrastructure using Azure AI services.

## Common Vulnerabilities and Exposures

The Common Vulnerabilities and Exposures (CVE) system provides a reference for publicly-known security vulnerabilities and exposures.

One (1) medium CVE has been identified below. For the complete list of CVEs for this solution, please refer to NIST's National Vulnerability Database.

| Vulnerability ID | Summary | CVSS Severity |
|---|---|---|
| **CVE-2022-30187** | Azure Storage Library Information Disclosure Vulnerability<br>The Azure Storage Encryption library in Java and other languages is vulnerable to a CBC Padding Oracle attack, similar to CVE-2020-8911. The library is not vulnerable to the equivalent of CVE-2020-8912 because it currently only supports AES-CBC as encryption mode.<br>Microsoft: CBC Padding Oracle in Azure Blob Storage Encryption Library · CVE-2022-30187 · GitHub Advisory Database · GitHub | Medium<br>CVSS_3.1 = 4.7 |

**Note:** It was confirmed that the Copilot implementation does not use the affected SDK to encrypt blob storage. Blob storage is managed at the ESDC subscription level and uses Azure native encryption instead. Any vulnerabilities discovered after this exercise are the responsibility of the product manager who must ensure that they are fixed.

## Risks/Concerns

The following table describes the various risk levels.

| Risk Level | Description |
|---|---|
| High | Medium risk to the business and/or the department. |
| Medium | Medium risk to the business and/or the department. |
| Low | Low risk to the business and/or the department. |
| Unknown | Possible risk, but ESDC IT Security is currently unable to confirm the vulnerability. IT Security recommends further analysis by IT Security, legal, or privacy experts, should the business owner not be comfortable with the ambiguity of this risk.<br>**Note:** Additional information about the solution would be needed for a more in-depth analysis. |

As of April 8, 2024, there are 67 risks inherited from the Azure Cloud Management Environment (ACME).

**Note:** Refer to the ACME Risk Mitigation Plan for additional details on all ACME risks.

| Parent Risk ID | Risk Statement | Risk Level | Planned Completion |
|---|---|---|---|
| TBDs | Inherited risks related to the Azure Cloud Management Environment (ACME) | High | Q4 2027 |

In addition, there is one (1) risk identified for Copilot as noted below.

### Risk 1: Risk to Confidentiality and Integrity because phased Out TLS 1.2 ciphers potentially continue to be enabled

| Risk Level | Description |
|---|---|
| **MEDIUM** | There is a possible risk to Confidentiality and Integrity due to potentially enabled phased out TLS 1.2 ciphers as per ITSP.40.062 Table 3: Recommended Cipher Suites for TLS 1.2. The phased out ciphers could allow eavesdropping and manipulation on secured communications. The risk is identified as Medium since the solution will only be used within ESDC and the documents consumed by the solution do not contain sensitive or classified information. |

| Safeguards |
|---|

To mitigate this risk would require the Copilot team to disable all ciphers that are deemed **phased out** as per ITSP.40.062. The following table lists the ciphers that need to be **disabled**:

**TLS_RSA_WITH_AES_256_GCM_SHA384**
**TLS_RSA_WITH_AES_128_GCM_SHA256**
**TLS_RSA_WITH_AES_256_CBC_SHA256**
**TLS_RSA_WITH_AES_256_CBC_SHA**
**TLS_RSA_WITH_AES_128_CBC_SHA256**
**TLS_RSA_WITH_AES_128_CBC_SHA**
**TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA**
**TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA**
**TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA**
**TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA**
**TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA**
**TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA**
**TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA**
**TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
**TLS_DHE_RSA_WITH_AES_128_CBC_SHA**

The current implementation of Copilot does not allow the configuration of ciphers on the resources within the resource group. It is recommended that an API proxy be used with the solution, which allows ciphers to be enabled or disabled.

## Conclusion

While completing the assessment of Copilot, one (1) risk was identified.

- Risk to Confidentiality and Integrity because phased out TLS 1.2 ciphers continue to be enabled

**Note:** This is an HLA of the potential risks of this solution based on the information available to the assessor as of March 19, 2024.

Should the scope of use change significantly or should the implementation, data classification, or data source change, the IT and Business Authorities are strongly urged to seek a revised assessment.

## Signatures

_____ Date _____

**Jacob Raffoul - IT Security Assessment Approver**

Director General, Cyber and IT Security
Innovation, Information and Technology Branch
Employment and Social Development Canada

_____ Date _____

**Martin Croker - Product Owner**

Director General, ESDC Solution Integration and Assurance
Benefits Delivery Modernization
Service Canada