**PROTECTED B**

# GenAI Copilot for Curam to Assist Agents

Benefits Delivery Modernization

Service Canada

# Risk Mitigation Plan

**CYBER AND IT SECURITY**

**INNOVATION, INFORMATION AND TECHNOLOGY BRANCH**

| | |
|---|---|
| Document Version Status: | FINAL |
| Document Version Number: | 1.2 |
| Document Version Date: | 2024-Apr-15 |

# Document Revision History

| | Description | Author | Date |
|---|---|---|---|
| 0.1 | Risk Mitigation Plan<br>- initial draft | Dan Bastianello | 2024-Mar-25 |
| 0.2 | Adding LOE for identified risk | Dan Bastianello | 2024-Mar-27 |
| 0.3 | Updating LOE and costing of mitigation | Dan Bastianello | 2024-Mar-27 |
| 0.4 | Initial internal review | Andrea Lemieux | 2024-Mar-28 |
| 0.5 | Adjustments to the risk wording | Erin Rowlinson | 2024-04-02 |
| 0.6 | Initial internal editing review | Beth Roodman | 2024-04-04 |
| 0.7 | Second internal review | Erin Rowlinson | 2024-04-05 |
| 0.8 | Comment review and reply | Dan Bastianello | 2024-04-08 |
| 1.0 | Clean up of comments and updates to signature blocks | Erin Rowlinson | 2024-04-08 |
| 1.1 | Removal of ACME Consolidated risks | Erin Rowlinson | 2024-04-12 |
| 1.2 | Adjusted wording of second sentence in inherited risks section | Erin Rowlinson | 2024-04-15 |

## 1. Introduction, Purpose and Use

This Risk Mitigation Plan (RMP) was prepared for ESDC GenAI Copilot for Curam to Assist Agents (Copilot).

The purpose of this RMP is to document risk mitigation actions which, if implemented, could reduce the risk of Copilot. This RMP was initially developed and reviewed within IT Security before being submitted to the IT solution development team for review and completion.

Once Copilot is authorized, the RMP serves as the action plan to address outstanding risks as noted and allows IT Security to monitor and report on the progress of the risk mitigation to the IT and Business Authorities.

## 2. Risk Mitigation Plan

The following table outlines the RMP. Below is a description of each column:

- **Number:** Sequential number
- **Risk Statement and Risk Level:** Short description of the risk and level of the risk
- **Recommendation and Mitigation Strategy:** Indication of the residual risk after mitigation
- **Lead:** Individual responsible for the action(s)
- **LOE:** Level of Effort (days) required for action(s) to mitigate the risk
- **Cost:** Estimated cost of action(s) to mitigate the risk
- **Commence:** Planned commencement of action(s) to mitigate the risk
- **Completion:** Planned completion of action(s) to mitigate the risk

### 2.1 Inherited Risks

Only risks that require mitigation by the Copilot solution team are included in the Risk Items and Action Items section of this RMP. Risks that are inherited by this solution are listed in the following table.

The inherited risks impacting Copilot are listed below.

**Note:** as of April 8, 2024, there are 67 risks inherited from the Azure Cloud Management Environment (ACME). 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 |

## 2.2 Risk Items and Action Items

| | Risk Statement and Risk Level | Recommendation and Mitigation Strategy | Lead | LOE | Cost | Commence | Completion |
|---|---|---|---|---|---|---|---|
| 1 | **Risk to Confidentiality and Integrity because phased out TLS 1.2 ciphers potentially continue to be enabled - MEDIUM RISK**<br>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. This risk is identified as Medium because the solution will only be used within ESDC and the documents consumed by the solution do not contain any sensitive or classified information.<br><br>This is assessed as a MEDIUM risk, more specifically:<br>• Risk Rating - Confidentiality – MEDIUM<br>• Risk Rating - Integrity – MEDIUM<br>• Risk Rating - Availability - LOW<br><br>**Risk Calculation:** Asset Value (AV) x Threat (T) x Vulnerability (V)<br>Values: AV = 2, T = 3, V = 3<br>Total Risk Score = 18 which is MEDIUM in accordance with HTRA methodology | The use of an API proxy be used with the solution is recommended, which would allow for enabling or disabling of supported ciphers. The following phased out ciphers must be disabled in accordance with ITSP.40.062 Table 3 TLS 1.2 cipher suites:<br>• TLS_RSA_WITH_AES_256_GCM_SHA384<br>• TLS_RSA_WITH_AES_128_GCM_SHA256<br>• TLS_RSA_WITH_AES_256_CBC_SHA256<br>• TLS_RSA_WITH_AES_256_CBC_SHA<br>• TLS_RSA_WITH_AES_128_CBC_SHA256<br>• TLS_RSA_WITH_AES_128_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA<br>• TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA<br>• TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA<br>• TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA<br>• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA<br>• TLS_DHE_RSA_WITH_AES_256_CBC_SHA<br>• TLS_DHE_RSA_WITH_AES_128_CBC_SHA<br><br>The residual risk rating after the mitigation strategy is implemented has been evaluated as:<br>• Risk Rating - Confidentiality - LOW<br>• Risk Rating - Integrity - LOW<br>• Risk Rating - Availability - LOW | Benoit Phaneuf | IT-SecDev x 1 day | $1500 | May 2024 | May 2024 |

Martin Croker — Date
Director General, ESDC Solution Integration and Assurance
Benefits Delivery Modernization, Service Canada

Jacob Raffoul — Date
Director General, Cyber and IT Security
IITB, ESDC