State of California
Department of Technology
Office of Information Security

Generative Artificial Intelligence Risk Assessment for General Office Productivity

Statewide Information Management Manual (SIMM) 150

September 2025

REVISION HISTORY

Revision	Date of Release	Owner	Summary of Changes
Initial Release	September 2025	California Office of Information Security - Payam Hojjat	Initial Release of the Generative Artificial Intelligence Risk Assessment for standalone Standardized Office Productivity Tools.

Table of Contents

I. Introduction

Generative Artificial Intelligence (GenAI) has the potential to improve the delivery of government services and operations. GenAI enables enhancements to the development, adoption, and implementation of new technologies to streamline and optimize business operations and state services to Californians. With that, it is critical for entities to be cognizant of GenAI risks and mitigations to ensure that GenAI does not lead to a situation where life, health, property, or public services are negatively impacted. GenAI systems are to be used to augment and improve workflows, not to replace or impair the services provided by state entities.

As described in the State of California Report: Benefits and Risks of GenAI report, GenAI offers a wide variety of potential applications with varying impacts. Any application of GenAI tools within the California state government will adhere to appropriate protocols and testing procedures. To proactively address potential threats to state-owned information assets, privacy, and the welfare of California's citizens, the Statewide Information Management Manual (SIMM) 5305-F, GenAI Risk Assessment introduces a risk assessment methodology that will aid state entities in evaluating the risks associated with GenAI systems.

NOTE: These forms must be signed by the CIO and ISO.

This SIMM is to ensure alignment with:

- Executive Order (EO) N-12-23
- NIST Artificial Intelligence Risk Management Framework

Please note that a completed SIMM 5310-C Privacy Threshold Assessment and Privacy Impact Assessment must be accessible upon request.

II. Office Productivity Risk Assessment

General office productivity refers to the effective use of GenAI technologies to streamline and enhance routine business functions and knowledge work across various domains, such as content creation, communication, research, data analysis, administrative support, training, etc., within an organizational environment. This includes leveraging GenAI to assist with tasks like document drafting, grammar correction, summarization, scheduling, content generation, data organization, translation, network analysis, and more, all with the goal of increasing efficiency, improving quality, and reducing manual effort while maintaining safeguards for security, privacy, compliance, and ethical standards.

Instructions

- This form is only completed for general office productivity use cases. All non-applicable form sections have been grayed out or rendered non-editable. Only complete required areas and ensure the use case qualifies under the general office productivity categories.
- If your use case does not fall under general office productivity categories then complete the *SIMM 5305-F Generative Artificial Intelligence Risk Assessment* form.
- This risk assessment is required for ***all*** GenAI procurements, acquisitions, renewals and internally developed systems.
- This risk assessment applies to **free** or no-cost GenAI products and services that interact with state data, defined as any samples, demonstrations, beta-versions, protypes, trial software, products or services. Examples include users entering state data into conversational GenAI platforms or installing GenAI plugins and extensions. However, this assessment does not apply in cases where state data is not being used, such as browsing the web with search engine GenAI results or using conversational GenAI systems where no state data is entered.
- This risk assessment is required for ***existing*** GenAI tools that do not already have a GenAI Risk assessment completed and were acquired prior to the release of this document. These assessments must be retained and accessible by the entity as it may be requested during an information security program audit or assessment.
- After completion, submit a Case via the New Technology Consultation and Assessment request, in the CDT IT Service Portal for all risk levels. When the request has been processed, a CDT Customer Engagement Services (CES) representative will reach out to provide a secure location to upload the required documents.
- *CDT reserves the right to audit and consult on **"Low"** GenAI Risk Levels with potential higher risk concerns.*

Once completed, this form is confidential and may be exempt from disclosure pursuant to Government Code sections 7929.210 and 8592.45.

General Office Productivity does NOT include:

- Use cases that require the use of confidential or PII data
- Use cases rated as Moderate or High risk based on the GenAI Risk Table Assessment Scale section
- Use cases involving automated decisions systems
- Use cases that materially impact the health, safety, or welfare of people

Data Types

General Office Productivity data types must be classified as **Public Information**. If the GenAI application or product accesses, processes, or outputs Confidential or PII information then complete the 5305-F GenAI Risk Assessment Form.

- **Public Information** - Information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act, Government Code Sections 7929.210, or other applicable state or federal laws.

GenAI Risk Table Assessment Scale

This form is only to be used for General Office Productivity that is rated Low risk. A Low rating means:

- FIPS 199 must be rated Low for Confidentiality, Availability, Integrity
- Data Types are Non-Confidential/Non-PII Related
- Use cases are narrow in scope

FIPS 199 Impact	Data Type	Use Case Examples
LOW (Green) Depending on the nature & sensitivity of the affected systems or information, losses related to confidentiality, integrity, & availability may still result in ***limited*** adverse impacts	**Non-Decision Related, Non-Confidential/Non-PII Related** • The data inputs, activities, & outputs are non-PII, non-confidential, & neither involve nor lead to decision-making throughout the end-to-end business process **Decision Related, Non-Confidential/Non-PII Related, Validated** • The data inputs, activities, and outputs are non-PII, non-confidential, and support decision-making, with the original data source of the GenAI output verified by a qualified subject matter expert (SME).	• Network & Security Tools (e.g., packet inspection, system monitoring, intrusion prevention/detection, spam filtering tools, malware detection tools like anti-virus, anti-malware, and endpoint detection & response). • Content & Communication Tools (e.g., grammar correction tools, summarization tools, reference generating tools like laws, case law, policies, translation tools, text to speech, & content creation tools for image, video, ads, and marketing).

If any part of your GenAI application or product falls within the Moderate or High rating, complete the 5305-F GenAI Risk Assessment

FIPS 199 Impact	Data Type	Use Case Examples
HIGH (Red) *Depending on the nature & sensitivity of the affected systems or information, losses related to confidentiality, integrity, & availability may still result in **severe or catastrophic** adverse impacts*	***Confidential/Personally Identifiable Information*** • *The data inputs, activities, and outputs involve processing Personally Identifiable Information (PII) or confidential data.* ***Safety Related*** • *The data inputs, activities, and outputs support decision-making processes that impact public safety.*	• *Inputs and processing of confidential data, including data that identifies or describes an individual, authentication, biometric identification, financial, medical, procurement, investigative, national security, network architecture schematics, ports, protocols, and others.* • *Inputs and processing of data that inform safety decisions, such as water treatment ratios, load-bearing specifications for bridges, and similar critical information.*
MODERATE (Yellow) *Depending on the nature & sensitivity of the affected systems or information, losses related to confidentiality, integrity, & availability may still result in **serious** adverse impacts*	***Decision Related, Non-Confidential/Non-PII Related, Resident (Public) Related*** • *The data inputs, activities, and outputs are non-PII and non-confidential but lead to decision making in public (resident) programs and services.* ***Decision Related, Non-Confidential/Non-PII Related, Not Validated*** • *The data inputs, activities, and outputs are non-PII, non-confidential, and support decision-making, but the GenAI model/output lacks verification by a qualified subject matter expert against the original data source used by the GenAI.* ***Mission Related, Resident (Public) Facing Web Apps*** • *The data inputs, activities, and outputs involve mission-critical, state-critical, critical infrastructure, or public-facing systems.*	• *Code Analysis & Development Tools (e.g., static and dynamic code analysis, code generation tools, code assistant tools, platforms used to create GenAI solutions).* • *Chatbots (e.g., internal chatbots for resource finding and process advice, resident-facing chatbots for public interaction and information retrieval).* • *Public & Direct Contact Services (e.g., customer service, public relations, jurisprudence, output providing recommendations such as legal, tax, regulatory information).* • *Critical Infrastructure & Safety (e.g., handling mission-critical apps/systems, service eligibility assessments for housing or income assistance, drafting organizational documents, generating data for public use like soil composition or seismic considerations).*

Risk Assessment Questionnaire

GenAI application and/or product details:
(a) **What is the vendor's name that offers the GenAI?**
(b) **What is the application and/or product name?** *(Note: Only One Product Per Form)*
(c) **What is the model and version of the product?**
(d) **What is the license tier of the GenAI product, if applicable (free, enterprise, platinum, etc.)?**
(e) **How is the GenAI solution delivered: IaaS, PaaS, SaaS, or will it be deployed on-premises?** ***(Indicate if this is a thin client, thick client, web extension, plugin, etc.)***

General Office Productivity

Instructions

The General Office Productivity section is organized by categories, use cases, and safeguards. Use cases provide representative examples. Departments must checkmark the category that most accurately reflects their activities and document all applicable use cases and safeguards. Checkmark all the Office Productivity Categories that apply.

The following safeguards apply to **all** office productivity categories.

- When real-time internet content retrieval is enabled, it must be restricted to *.ca.gov domains (grounding)
- A qualified SME must carefully review applicability and accuracy of references and content (Human Review)
- Traceability of content or information as generated by Gen-AI (Identification of GenAI generated content)
- Limit the tools to user groups who do not use Confidential/PII. If user groups use the same GenAI applications or products that will utilize Confidential or PII data, complete the *SIMM 5305-F GenAI Risk Assessment* form.

☐ Office Productivity Use Case Category: Summarization

Sub Use Case	**Suggested Minimum Safeguards**
• Summarizing public articles or white papers • Creating executive summaries of internal non-sensitive reports • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Ensure all GenAI input and output data is validated by a qualified SME. • Ensure user's open-source material and validate the information exists and is accurately represented. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Content Creation

Sub Use Case	Suggested Minimum Safeguards
• Creating images (non-sensitive, illustrative) • Generating thumbnails • Automating cut scenes in videos • Creating animated transitions • Generating social media post templates • Designing non-sensitive infographics • Writing product descriptions • Drafting blog outlines or titles • Social media captions • Suggesting color palettes • Generating icons or simple vector art • Auto-formatting presentation slides • Auto-resizing images for web platforms • Scheduling posts • Recommending hashtags • Generating variations of post text • Creating short video captions for reels • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Review license levels to identify if there are product versions that enable administrative configuration by state staff to restrict data collection. • Establish clear organizational policies for acceptable content creation, ensuring compliance with advertising standards and consumer protection laws. • Require a review process to validate that content aligns with ethical and legal standards before publication. • Disclose when content has been AI-generated to maintain trust. • Staff creating content with GenAI should be vigilant in check for and minimizing bias that may impact diversity, equity, inclusion, and access (DEIA). • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Email Assistance

Sub Use Case	Suggested Minimum Safeguards
• Drafting internal email templates • Suggesting professional phrasing • Auto-filling repetitive responses Other*: (List any additionally **closely aligned** office productivity use cases):*	• Configure tools to ensure the disabling of automatic reading of emails • Update Acceptable Use Policy to include statements that prohibit the copy and pasting of confidential sensitive, or personally identifiable data or information email threads into prompts for analysis. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Grammar Correction

Sub Use Case	Suggested Minimum Safeguards
• Grammar/spelling correction • Rewording and style suggestions • Suggesting tone or format improvements • Alternative phrasing for clarity • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Update Acceptable Use Policy to address data handling of sensitive and confidential information with grammar correcting tools, including prohibited statements for using confidential sensitive, or personally identifiable data or information. • Ensure there is minimal to no data collection and data sharing with vendors to minimize data exposure. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Translation & Transcription

Sub Use Case	Suggested Minimum Safeguards
• Meeting summarization (non-sensitive, internal use) • Transcribing publicly shared videos or podcasts • Translating website content or multilingual instructions • Generating image alternative text (alt text) • Converting text to simplified language • Captioning non-sensitive videos • Reading text aloud via text-to-speech • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Obtain consent before recording meetings. • Limit how long audio, video, and transcription data are stored and ensure proper deletion protocols. • Human reviews translation and transcription for accuracy. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Research & Reference Analysis

Sub Use Case	Suggested Minimum Safeguards
• Locating article leads or academic sources • Extracting key topics from public documents • Locating publicly available laws or policies • Linking to case law summaries • Providing official procedural templates • Tagging documents with topics • Suggesting categories or labels for files • Organizing documents based on metadata • Auto-linking related documents Other: (List any additionally closely aligned office productivity use cases):	• Validate generated references against official or authoritative sources before use. • Require qualified SMEs to confirm applicability and accuracy of references in the given context. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Writing Canvases (word, text)

Sub Use Case	Suggested Minimum Safeguards
• Idea brainstorming • Drafting outlines • Auto-generating content blocks • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Clearly label AI-generated ideas as drafts • Use prompt guardrails to limit controversial outputs • Require manual review before publishing • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Formula Computational (spreadsheets)

Sub Use Case	Suggested Minimum Safeguards
• Auto-generating Excel formulas • Explaining formula logic • Formatting tables and data • Identifying missing values • Suggesting column names • Reformatting date fields or text • Removing duplicate entries • Detecting inconsistent field entries • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Result validation by users • Formula previews before insertion • Maintain version history of original datasets • Disable GenAI access to confidential sensitive, or personally identifiable data or information during transformation • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Administrative Support

Sub Use Case	Suggested Minimum Safeguards
• Scheduling meetings based on calendar availability • Creating to-do lists or agendas • Summarizing meeting minutes (non-sensitive) • Auto-filling repetitive forms (non-confidential) • Notetaking • Collating • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Confirms with human before sending invites • Human review before sharing notes or summarization • Timestamped context or links to full transcript • Label as AI-generated content • Restrict access to only the calendar or data explicitly authorized for use. • Prevent AI from referencing confidential sensitive, or personally identifiable files • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Surveys & Feedback

Sub Use Case	Suggested Minimum Safeguards
• Summarizing customer survey responses (non-sensitive, non-confidential, non-personally identifiable) • Categorizing open-ended responses • Suggesting improvements to survey language • Generating survey templates • Generating action item recommendations • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Human-in-the-loop review for sensitive question generation or sentiment classification. • Exclude sensitive attributes from influencing AI decisions (e.g. race, gender). • Natural language validation filters for neutrality. • Manual spot-checking of AI outputs against responses. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Conversational GenAI (e.g., Chatbots)

Sub Use Case	Suggested Minimum Safeguards
• Grammar/spelling correction • Rewording and style suggestions • Suggesting tone or format improvements • Alternative phrasing for clarity • Auto-generating content blocks • Ideation • Prompting for information about topics • Basic troubleshooting guidance • Policy Explanation • Technical Q&A • Document Processing & Conversion • Summarization • Suggesting related resources or documents • Extracting FAQs from policy documents • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Deploy Conversational AI tools in isolated, secure environments without external internet connectivity to prevent data leaks. • Train users to always go into the sources and locate the page number, paragraph, table, etc., where the information was found to ensure it exists and is in the right context. • Include metadata, notification, and banners indicating potential inaccuracies with outputs reminding users to manually review outputs. • Allow users to flag inaccuracies and provide feedback for system improvement. • Use a curated set of validated responses (prompt sanitization) to mitigate inappropriate prompts and responses • Ensure datasets are inclusive, representative, and free of systemic bias. • Other: *(List any additional safeguards that are applicable to the use case)*:

☐ Office Productivity Use Case Category: Training & Onboarding

Sub Use Case	Suggested Minimum Safeguards
• Generating training quizzes • Summarizing onboarding material • Drafting internal FAQs • Creating simple training simulations (non-regulated topics) • Other*: (List any additionally **closely aligned** office productivity use cases):*	• Qualified SME review required • Retain links to full source documents • Clearly state “for training only” use • Label as AI-generated content • Other: *(List any additional safeguards that are applicable to the use case)*:

Signatures and Acknowledgement (Required Completion)

Required Signatures for Risk Assessment Part 1

You are required to ensure that the Acceptable Use Policy is updated to address GenAI. A completed SIMM 5310-C Privacy Threshold Assessment and Privacy Impact Assessment must be accessible upon request. If additional GenAI features are enabled in the future beyond those outlined in this document, a new SIMM 5305-F must be submitted for review.

By signing this document, the signatory is confirming that the state entity certifies the intended GenAI use case, its risk level, and understands that all procurements are mandated to comply to all CDT-published security and privacy policies (SAM Sections 5100 and 5300 - 5399). The signatory further confirms that its intended GenAI use case falls within the description of general office productivity provided in this form. The signatory agrees to implement the required safeguards and understands the suggested minimum safeguards for the sub-use cases listed above.

Labor Relations Engagement

California state hiring authorities are responsible for ensuring that the implementation of changes affecting state employees’ terms and conditions of employment complies with relevant policies and codes. For specific guidance on applicable labor relations policies and procedures, please coordinate with your labor relations office or CalHR Labor Relations.

☐ *As the CIO (or equivalent), I acknowledge that our Department's Labor Relations officer (or equivalent) has received and reviewed a copy of this 5305-F Risk Assessment form.*

_____ ISO Name (print)	_____ CIO Name (print)
_____ _____ ISO Signature (or equivalent) Date	_____ _____ CIO Signature (or equivalent) Date

III. Definitions

Relevant definitions for this guidance are available in SAM 4819.2 and 5300.4

Generative Artificial Intelligence means an artificial intelligence system that can generate derived synthetic content, including text, images, video, and audio that emulates the structure and characteristics of the system's training data.

Human Verification is the process in which one or more people review and validate the output generated by an automated system, such as a GenAI tool, to ensure its accuracy, correctness, and alignment with factual information before it is used or implemented. This step acts as a safeguard against errors or misleading content produced by the automated system.

Resident Facing Service refers to any service or application that interacts directly with residents or the public. This typically involves systems or tools that provide information, make decisions, or deliver services to residents.

Automated Decision-Making System means a computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decision making and materially impacts natural persons. "Automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data (Government Code 11546.45.5).

IV. References

1. Generative Artificial Intelligence
   https://www.genai.ca.gov/

2. Artificial Intelligence Risk Management Framework (AIRMF1.0)
   https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

3. Federal Information Processing Standards, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)
   https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

4. California Government Operations Agency website
   GovOps | Government Operations (ca.gov)

5. Statewide Administrative Manual (SAM) policies:
   https://www.dgs.ca.gov/en/Resources/SAM/TOC/

V. Questions

Please reference SIMM 71B for questions regarding procurement. For all other inquiries and implementation of this standard, please contact the California Department of Technology, Office of Information Security at Security@state.ca.gov.