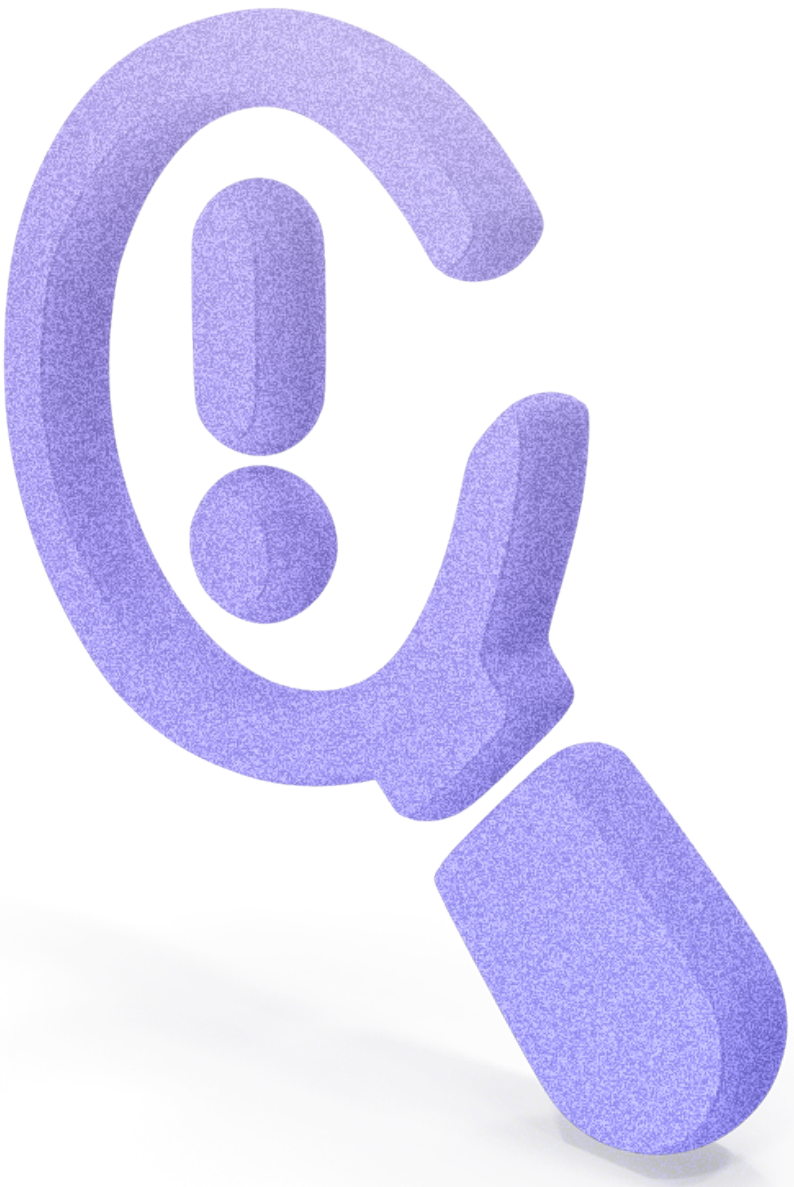
FS-ISAC

Generative AI Vendor Risk Assessment Guide



February 2024

Contents

OVERVIEW

This document describes the purpose and methodology behind the Generative Artificial Intelligence Vendor Evaluation and Risk Assessment workbook ("Vendor GenAI Risk Assessment") as well as instructions on how to use it. This white paper and supporting Vendor GenAI Risk Assessment address a number of risks associated with generative AI (GenAI).

However, generative AI is advancing rapidly. Its applications and the regulatory environment are highly likely to change – indeed, the ramifications of the 30 October 2023 U.S. Executive Order[1] regarding the safety and standards of AI are yet to be seen. Vendors in the space will continue to innovate their use of generative AI, changing financial services organizations' use cases and implementation. Financial services cybersecurity professionals are therefore advised that this white paper is not all-encompassing, and that GenAI-based solutions are constantly evolving.

Executive Summary

The Vendor GenAI Risk Assessment workbook is a tool designed to help organizations assess and select generative AI vendors while managing associated risks. The purpose is to break down the vendor evaluation process and ensure that financial institutions (FIs) make informed decisions when considering generative AI solutions regardless of the FI's type and size.

Methodology

The workbook does not cover all possible use cases, risks, or risk appetites but it does consider a multitude of risks applicable to FIs of various sizes and complexities. This risk assessment model may be considered in two ways:

- A **starting point** for organizations that employ a comprehensive due diligence process or that have lower appetites for risk.
- A **complete process** for organizations that employ a more modest due diligence process or that have a higher appetite for risk.

The methodology used in the generative AI risk assessment process is designed to support Third-Party Risk Management (TPRM) programs in their effort to assist with the discovery and evaluation of GenAI solutions and use cases within their organizations and supplement existing TPRM processes. The assessment is not a universal solution; rather it is designed to be customizable based on the FI's risk appetite.

The workflow of the risk assessment is as follows:

- Complete a high-level risk analysis of the GenAI product or service by categorizing risk across five domains: 1) your organization's use case, 2) business integration, 3) use of confidential data, 4) business resiliency, and 5) potential for exposure. The premise behind the flexible, high-level risk analysis is to avoid a standardized approach to due diligence. Instead, initial risk analysis is designed to guide the user to an appropriate due diligence plan (referred to as Level 1, 2, or 3) based on the FI's risk appetite and use case for generative AI.
- An internal stakeholder questionnaire is provided with a fixed set of questions. The questionnaire is not influenced by the risk analysis and instead may be used to supplement or influence the risk analysis if conducted first. While encouraged, the internal stakeholder questionnaire is not required and may be used at the discretion of the FI as a tool to gather the information needed for the risk analysis.
- The vendor questionnaire is dynamic, created according to the recommended due diligence plan (the outcome of the initial risk analysis). The recommended due diligence plans include FS-ISAC default questions, which are customizable.

- The vendor questionnaire attempts to gather information in the following categories that are relevant to generative AI:
    1. General (discovery)
    2. Data privacy, retention, and deletion
    3. Model training, validation, and maintenance
    4. Information security
    5. Technology integration
    6. Nth party risk/usage
    7. Legal, regulatory, and compliance
- Both questionnaires are customizable, and users can include or exclude questions in Levels 1, 2, or 3. In combination with the risk analysis, the include/exclude functionality provides a very flexible approach to generative AI vendor evaluation and risk assessment.
- When the risk analysis, stakeholder questionnaire (if used), and vendor questionnaire are completed, the results are auto populated into a final report, which may be printed to PDF for archival/record-keeping purposes.

Risk Considerations

In developing the questionnaires, a number of risks were identified. The risks associated with GenAI are not solely information security and privacy risks. As with traditional third-party risk management, a cross-functional questionnaire has been established including the following risk categories:

- Data privacy, retention, and deletion
- Model training, validation, and maintenance
- Information security
- Technology integration
- Nth party risk
- Legal, regulatory, and compliance risk

Industry best practices and frameworks were considered when developing the questionnaires, including NIST's AI Risk Management Framework 1.0, NIST CSF, the FFIEC's IT Examination Handbook, and the FFIEC's 2023 Interagency Guidance on Third-Party Relationships: Risk Management. Language in the FFIEC Interagency Guidance specifically references novel risks and the importance of identifying, assessing, monitoring, and controlling these types of risks.

While the questionnaire includes risk tiering to determine a due diligence plan, the responses to the questions do not yield a risk rating. Due to the varying types of FIs and in consideration of size, complexity, and risk tolerance, FIs are to rely on their internal risk rating processes and methodologies to risk-rate vendors offering generative AI products or services. Future iterations of this risk questionnaire may seek to quantify risks.

WHERE TO BEGIN

The Vendor GenAI Risk Assessment workbook is a Microsoft Excel® workbook that consists of the following four worksheets:

1. Assessment model
2. Stakeholder questionnaire
3. Vendor questionnaire
4. Final report

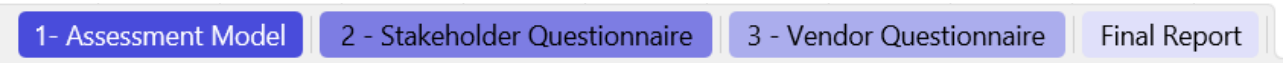


Figure 1: Tabs (worksheets) in the Vendor GenAI Risk Assessment workbook.

Before you begin, we recommend saving a copy of the Vendor GenAI Risk Assessment workbook to preserve the default settings for future use. Always create a working copy when conducting vendor assessments.

ASSESSMENT MODEL

The assessment model in collapsed view is depicted in the screenshot below. It contains the following features:

1. Buttons [1] and [2] that can be used to expand or collapse all sections at once.
2. [+] buttons are used to expand section by section. When expanded they will change to [-] to collapse.
3. Content is organized in a series of five steps, explained in detail below.

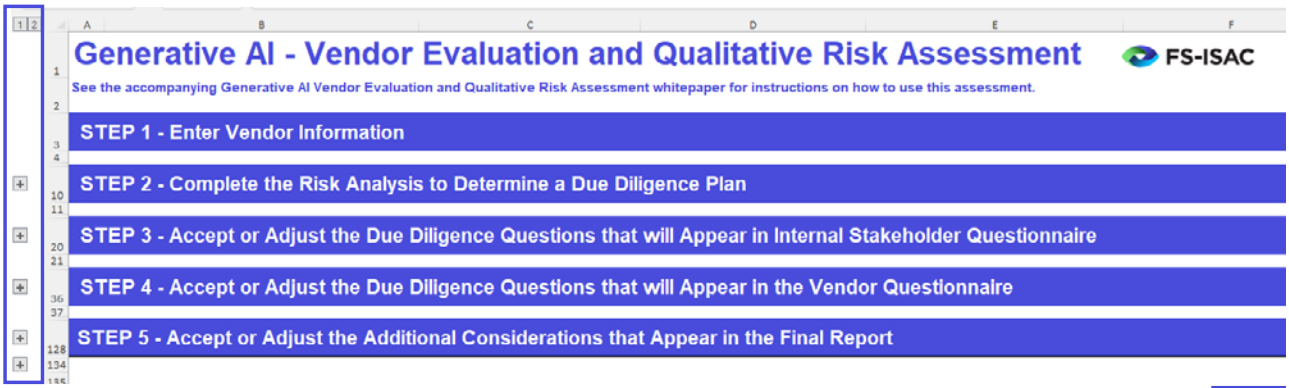


Figure 2: Partial screen capture of the assessment model worksheet, with steps shown in collapsed view.

1 Step 1 | Enter Vendor Information

> Expand the section [+].

> Enter information about the vendor in this section. Save your work.

> Information entered here automatically populates the same information in the stakeholder and vendor questionnaires as well as the final report.

STEP 1 - Enter Vendor Information

Third-Party Name:	Acme, Inc. (example only)
Website:	https://www.acmeinc.com (example)
Product/Service:	Example generative AI service name
Date Completed:	10/20/2023

Save a copy of this workbook to retain the default settings for future use.

Figure 3: Screen capture from the assessment model worksheet showing where to enter vendor information.

2 Step 2 | Complete the Initial Risk Analysis to Determine a Due Diligence Plan

> The risk analysis section determines what due diligence plan is recommended to the user. Lower risk scenarios will have fewer questions and higher risk scenarios will have more in-depth questions. The goal is to provide risk managers with a solid foundation from which to complete or continue the due diligence and risk assessment process.

> **The risk analysis section is listed as step 2. However, depending on your organization's internal processes, you may decide to send the stakeholder questionnaire to the appropriate internal personnel first, in order to capture the information that is helpful to the risk analysis. If this reflects your process, proceed to step 3 below, then complete step 2 using the information you collected.**

> Regardless of your internal process, the risk analysis is designed to be completed before the vendor questionnaire is sent.

> When you are ready to complete step 2, expand the section [+].

> Complete the risk analysis by selecting 1, 2, or 3 in the "Choose Estimated Risk Level" column for each domain. Click on each cell to expose the drop-down list of risk levels.

> Save your work.

STEP 2 - Complete the Risk Analysis to Determine a Due Diligence Plan

	Domains / Risk	1-Low	2-Moderate	3-High	Choose Estimated Risk Level
1	Use of Generative AI (gAI)	1L. Your organization is exploring the functionality of generative AI for educational purposes or R&D.	1M. Your organization's use of gAI is limited to vendors who integrate generative AI technology as a secondary/supplemental service.	1H. Your organization's intended use of gAI aligns with: 1) Utilizing the gAI to generate influential content for customers; or 2) Developing a custom application that relies on a publicly available generative AI model for core functionality; or 3) Utilizing the gAI to assist in code generation, or 4) Utilizing	Select one...
2	Business Integration	2L. The g AI outputs are not integrated with business processes.	2M. The gAI outputs may be integrated with non-financial business processes.	2H. The gAI outputs are integrated with financial business processes or critical non-financial business processes.	Select one...
3	Use of Confidential Data	3L. No customer or company confidential information is used as inputs or is otherwise stored, processed or transmitted by the system.	3M. No confidential customer data is used as inputs/prompts but inputs may include confidential company data. Company data is not used to train the foundational model.	3H. There is a high probability that customer or company confidential information will be used as inputs/prompts, is used to train the foundational model, or is otherwise stored, processed or transmitted by the	Select one... 1 2 3
4	Business Resiliency	4L. Downtime of the gAI functionality will not affect business operations.	4M. Downtime of the gAI functionality will not materially impact business operations. Reversion from gAI to human-driven activity is cost-effective and achievable within an acceptable	4H. Downtime could materially impact business operations. Reversion from gAI to human-driven activity is prohibitive from a cost and/or personnel perspective, or is not possible.	Select one...

Figure 4: Screenshot from the assessment model worksheet showing how to select risk levels for each of the five domains.

- The chosen risk levels are color-coded in the grid for easy reference.
- The recommended due diligence plan is based on the highest risk level selected for all domains. In the example below, the risk analysis is recommending a level 3 due diligence plan, which is the most comprehensive, because the Business Resiliency domain was scored at a risk level of 3 (i.e., high).

STEP 2 - Complete the Risk Analysis to Determine a Due Diligence Plan

	Domains / Risk	1-Low	2-Moderate	3-High	Choose Estimated Risk Level
1	Use of Generative AI (gAI)	1L. Your organization is exploring the functionality of generative AI for educational purposes or R&D.	1M. Your organization's use of gAI is limited to vendors who integrate generative AI technology as a secondary/supplemental service.	1H. Your organization's intended use of gAI aligns with: 1) Utilizing the gAI to generate influential content for customers; or 2) Developing a custom application that relies on a publicly available generative AI model for core functionality; or 3) Utilizing the gAI to assist in code generation, or 4) Utilizing	2
2	Business Integration	2L. The g AI outputs are not integrated with business processes.	2M. The gAI outputs may be integrated with non-financial business processes.	2H. The gAI outputs are integrated with financial business processes or critical non-financial business processes.	2
3	Use of Confidential Data	3L. No customer or company confidential information is used as inputs or is otherwise stored, processed or transmitted by the system.	3M. No confidential customer data is used as inputs/prompts but inputs may include confidential company data. Company data is not used to train the foundational model.	3H. There is a high probability that customer or company confidential information will be used as inputs/prompts, is used to train the foundational model, or is otherwise stored, processed or transmitted by the	2
4	Business Resiliency	4L. Downtime of the gAI functionality will not affect business operations.	4M. Downtime of the gAI functionality will not materially impact business operations. Reversion from gAI to human-driven activity is cost-effective and achievable within an acceptable period of time.	4H. Downtime could materially impact business operations. Reversion from gAI to human-driven activity is prohibitive from a cost and/or personnel perspective, or is not possible.	3
5	Potential for Regulatory, Compliance, Reputation or Operational exposure	5L. Low potential for regulatory, compliance or operational exposure resulting from your organization's use of generative.	5M. Moderate potential for regulatory, compliance or operational exposure resulting from your organization's use of	5H. High potential for regulatory, compliance or operational exposure could result from your organization's use of generative AI.	1
				Recommended Due Diligence Plan	3

Figure 5: Screenshot from the assessment model worksheet showing a completed risk analysis with color coding and the resulting recommended due diligence plan.

3 Step 3 | Accept or Adjust the Due Diligence Questions that Will Appear in Internal Stakeholder Questionnaire

- Use of the internal stakeholder questionnaire is encouraged, but optional. If the questionnaire is not utilized, the risk manager should select **No** from the menu as shown below. This signifies in the final report (your due diligence record) that the stakeholder questionnaire was not used. The risk manager is encouraged to provide a reason for not using the questionnaire.

Generative AI - Internal Stakeholder Questionnaire

Level 3

For Use by Assessment Administrator:
Was the Internal Stakeholder Questionnaire Used in this Assessment? **No** Reason not used:

Select one...
Yes
No

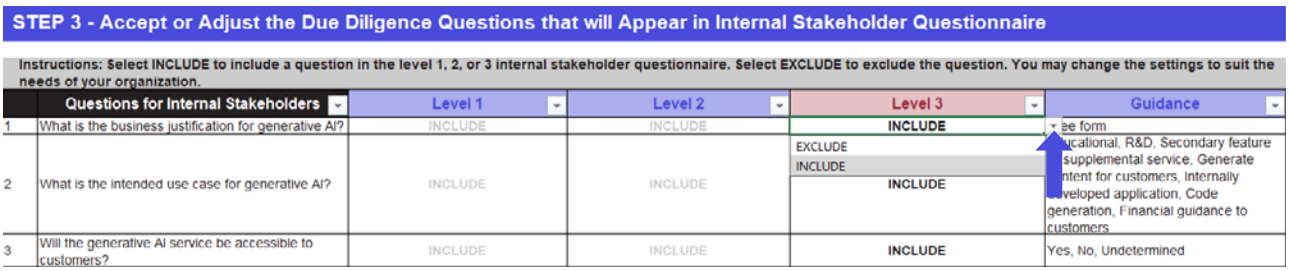
Third-Party Name:

Website: (example)

- The model offers three due diligence plans (Levels 1, 2, and 3). In the default model, Level 3 contains all questions from Levels 1 and 2, and Level 2 contains all questions from Level 1. **We recommend that you review the configuration before sending the internal stakeholder questionnaire.**
- Note that the assessment model is not the questionnaire, it is the place to configure the questionnaire, or accept the default configuration.
- To accommodate FIs with different risk appetites, the questions included in each due diligence level are customizable, i.e. the model can be configured to include a Level 3 question in a Level 1 due diligence plan or to remove a Level 3 question from a Level 3 due diligence plan, and so on.
- The FS-ISAC default model includes all internal stakeholder questions in all due diligence plans as it allows for the FI to better understand the requestor's use case and make a risk-based decision.

> To review or customize the questions included in each due diligence plan:

- Expand the selection [+].
- Each question may be included or excluded in a particular due diligence level by clicking each cell to expose the choices, as shown below:



STEP 3 - Accept or Adjust the Due Diligence Questions that will Appear in Internal Stakeholder Questionnaire

Instructions: Select INCLUDE to include a question in the level 1, 2, or 3 internal stakeholder questionnaire. Select EXCLUDE to exclude the question. You may change the settings to suit the needs of your organization.

	Questions for Internal Stakeholders	Level 1	Level 2	Level 3	Guidance
1	What is the business justification for generative AI?	INCLUDE	INCLUDE	INCLUDE	ee form
2	What is the intended use case for generative AI?	INCLUDE	INCLUDE	EXCLUDE INCLUDE INCLUDE	ucational, R&D, Secondary feature supplemental service, Generate ntent for customers, Internally veloped application, Code generation, Financial guidance to customers
3	Will the generative AI service be accessible to customers?	INCLUDE	INCLUDE	INCLUDE	Yes, No, Undetermined

Figure 6: Screenshot from the assessment model worksheet showing how to customize the questions that appear in the stakeholder questionnaire for each plan level. If no customization is required, no action is needed.

> The guidance column in the model reflects the responses from which the recipient can choose in the actual questionnaire. They are presented in the model for reference purposes.

4 Step 4 | Accept or Adjust the Due Diligence Questions that Will Appear in the Vendor Questionnaire

> The FS-ISAC default model contains a tiered approach to the due diligence process for vendors. **We recommend that you review the configuration before sending the vendor questionnaire.**

> Note that the assessment model is not the questionnaire, it is the place to configure the questionnaire, or accept the default configuration.

> The due diligence levels for the vendor questionnaire are described as follows:

- Level 1 is a basic set of questions for lower risk engagements, primarily for R&D or educational purposes. The questions are focused on basic risks centered around the use of GenAI, notices on data privacy, identifying the foundational model, information security questions, API integration, and Nth party risk. Included questions are customizable as indicated below.
- Level 2 is a more comprehensive set of questions for organizations that may integrate GenAI outputs with business processes, utilize confidential company data in prompts, or have moderate potential for regulatory scrutiny. These questions include all of the Level 1 questions. Additional questions in Level 2 include legal, regulatory, and compliance questions, vulnerability management, model validation, and vendor moderation. Included questions are customizable as indicated below.
- Level 3 is the most comprehensive set of questions. It is geared towards organizations that plan to use GenAI for generating customer-facing content, integrating with critical business processes, and have a high potential for regulatory risk. Level 3 questions include all of the Level 1 and Level 2 questions. Additional questions include data retention, change management, audit validation, security configuration, log management, DLP, and technology integration. Included questions are customizable as indicated below.

> As with the stakeholder questionnaire, the vendor questionnaire is customizable. To customize the vendor questionnaire:

- Expand the selection [+].

- Each question may be included or excluded in a particular due diligence level by clicking each cell to expose the choices, as shown below:

STEP 4 - Accept or Adjust the Due Diligence Questions that will Appear in the Vendor Questionnaire

Instructions: Select INCLUDE to include a question in the level 1, 2, or 3 internal stakeholder questionnaire. Select EXCLUDE to exclude the question. You may change the settings to suit the needs of your organization.

1	*General (Discovery)*	Level 1	Level 2	Level 3	Guidance
1.1	Does your organization leverage Generative AI?	INCLUDE	INCLUDE	INCLUDE	Yes - for product or service, Yes - for business development, Yes - for predictions based on ...erms, Yes - Other (Use comments to describe)
1.2	Does your organization use Generative AI in support of services provided to our Company?	INCLUDE	INCLUDE	EXCLUDE INCLUDE	Yes,No,Undetermined
1.3		IN THE VENDOR QUESTIONNAIRE, THIS LINE IS USED TO DISPLAY THE PROCEED/DO NOT PROCE			1 AND 1.2
1.4	[IF YES to 1.1 or 1.2] In what ways will our purchased product depend on Generative AI?	INCLUDE	INCLUDE	INCLUDE	Not dependent, Highly dependent, Key features only, Secondary features only
1.5	[IF YES to 1.1 or 1.2] Will the use of generative support any customer interactions or services?	INCLUDE	INCLUDE	INCLUDE	Yes, No

Figure 7: Screenshot from the assessment model worksheet showing how to customize the questions that appear in the vendor questionnaire for each plan level. If no customization is required, no action is needed.

> The guidance column in the model reflects the responses from which the recipient can choose in the actual questionnaire. They are presented in the model for reference purposes.

5 Step 5 | Accept or Adjust the Additional Considerations That Appear in the Final Report

> This questionnaire is not meant to replace a FI's regular TPRM process. Rather, it is a tool to assist with due diligence given the novel risks associated with GenAI and the potential security, privacy, and regulatory impact associated with GenAI.

> The vendor questionnaire is vendor agnostic. The FI is responsible for exercising due care when assessing questionnaire outputs and FS-ISAC is not responsible for the outputs or decisions of the FI.

> Some institutions may seek a more comprehensive due diligence process or at a minimum, seek additional awareness about the risks associated with GenAI. To that end, the Additional Considerations section provides additional topics and resources to consider in areas such as model risk analysis, federal guidance, legal, and TPRM.

> The Additional Considerations section is auto populated into the final report. You may customize the contents of Additional Considerations in the assessment model.

STEP 5 - Accept or Adjust the Additional Considerations that Appear in the Final Report

1	Additional Due Diligence	The FS-ISAC Artificial Intelligence Working Group has developed numerous resources to assist with learning the fundamentals, taxonomy, threats and countermeasures relevant to AI and Generative AI systems, with a focus on the Financial Services sector. In addition, there are numerous commercial and government entities that have created resources to facilitate deeper analysis of AI/generative AI system such as Shared Assessments (SIG), NIST, MITRE and others.)
2	Model Risk Analysis	When the output of the generative AI systems contributes to financial modeling or decisioning processes, consider seeking guidance from model risk experts in your organization.

Figure 8: Screenshot from the assessment model worksheet showing the Additional Consideration section. If no customization is required, no action is needed.

PREPARING TO SEND THE QUESTIONNAIRES

Formatting Considerations

> Pay attention to the formatting of the cells in the questionnaires to ensure that all content is visible (the due diligence levels change as cells expand and contract, which may affect the view). To ensure all text is visible:

- Highlight Column B in either questionnaire.

- In the Microsoft Excel ribbon, navigate to Home menu > Cells group > Format option and select AutoFit Row Height (your view may differ depending on the version of Excel or the operating system you use, but the concept is the same).

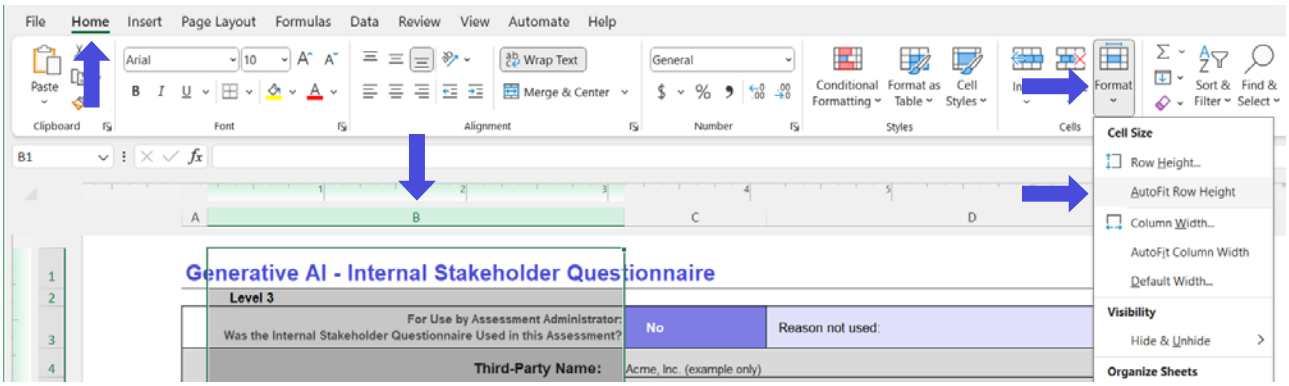


Figure 9: Screenshot showing how to use the AutoFit Row Height in Microsoft Excel to ensure contents are visible in the questionnaires before sending.

> In the final report, you must select all columns before using AutoFit Row Height, as shown below:

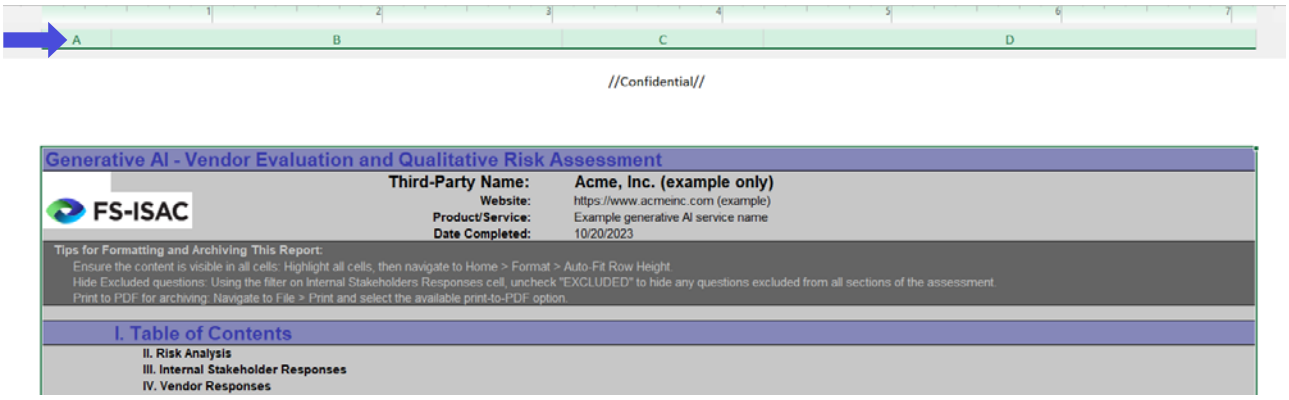


Figure 10: Screenshot showing how to use AutoFit Row Height in Microsoft Excel to ensure contents are visible in the final report before printing to PDF.

Hiding Excluded Questions

> Excluded questions are questions that were designated as excluded in the model. Excluded questions will be highlighted in red in the stakeholder and vendor questionnaires and in the final report.

> To hide the excluded questions, utilize the available column filter and uncheck the "excluded" option, shown to the right.

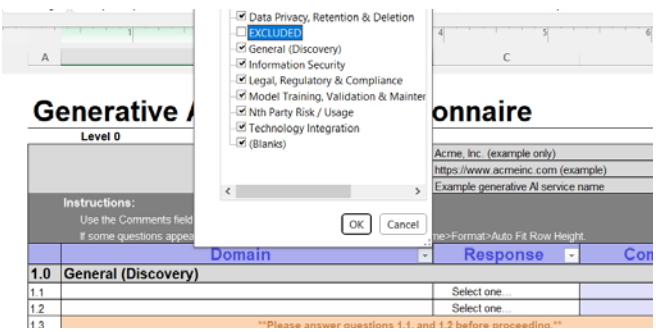


Figure 11: Hide excluded questions from the stakeholder and vendor questionnaires and final reports by using the appropriate column filters.

Hiding Worksheets for Certain Recipients

- When sending the questionnaires, we recommend hiding the tabs (worksheets) that are not intended for the recipient. While this will help keep the recipient's attention focused on the right place, it is not required and you can send the workbook as-is.
- **NOTE: Hiding the other worksheets is not a security control, it is a way to ensure the recipient stays focused on the intended task. When sending the workbook, do not include anything in hidden worksheets that would violate your organization's privacy or confidentiality policies.**
- As an example, before sending the vendor questionnaire, hide the assessment model, stakeholder questionnaire, and final report tabs by right clicking on each tab and selecting hide (you can unhide when you receive the workbook back from the vendor):

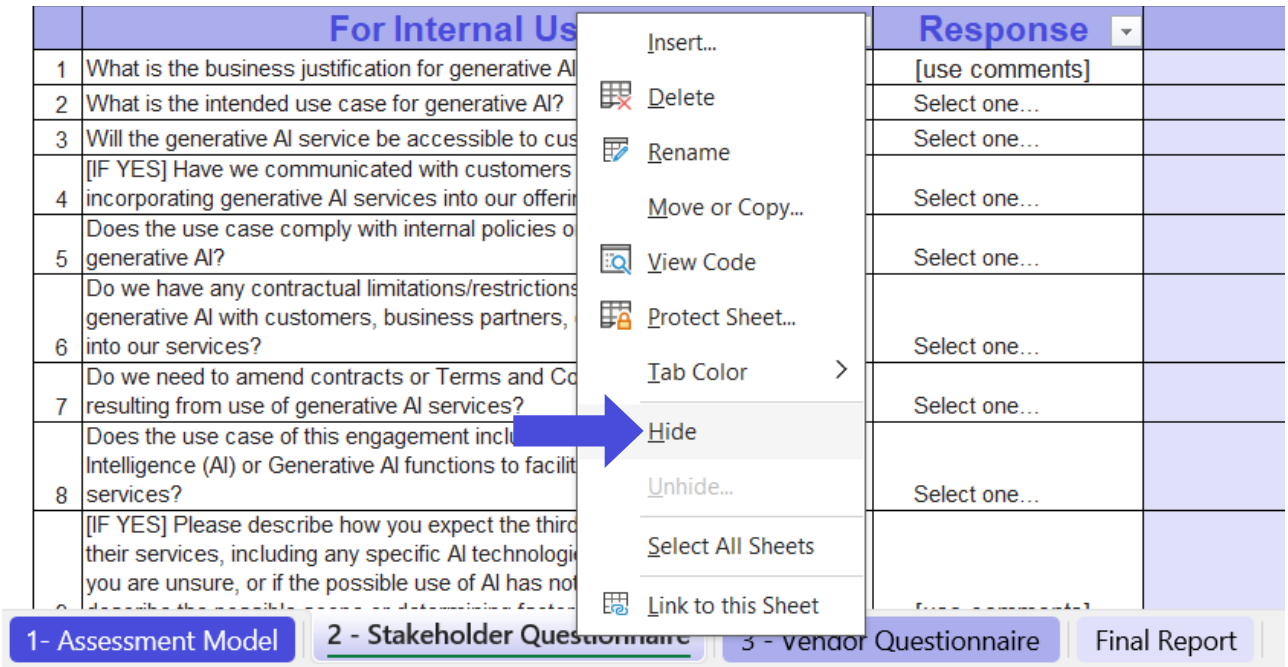


Figure 12: Screenshot showing how to hide a worksheet/ tab in the workbook by right clicking on the tab.

- After hiding the other tabs, the recipient (in this example, the vendor) will receive the workbook with only the following tabs visible:

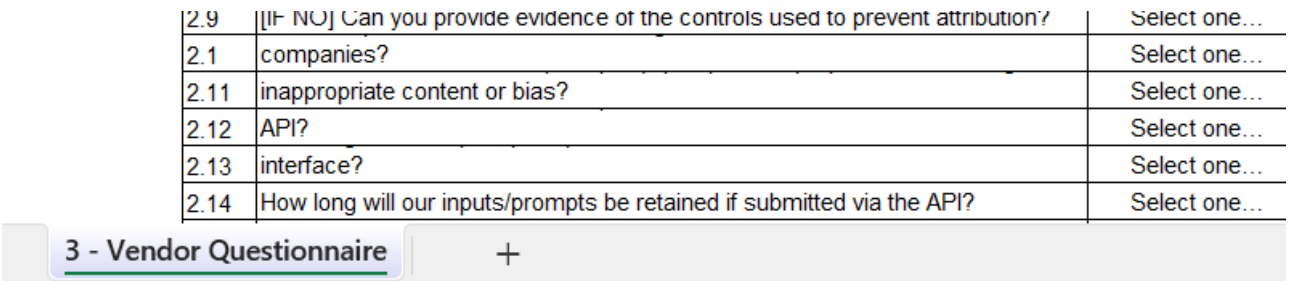


Figure 13: Screenshot showing the workbook with only the vendor questionnaire visible.

- When you receive the completed questionnaire back from the vendor, right click on the vendor questionnaire tab, select unhide, and choose the other worksheets (one at a time) to expose them again.

- You may repeat this process when sending the internal stakeholder questionnaire by leaving only the stakeholder questionnaire tab exposed and hiding the others.
- Again, this process is not required, but may help keep the recipient focused on the task.

THE FINAL REPORT AND ARCHIVING

About the Final Report

The final report worksheet is auto populated – you do not need to enter any data. The final report is designed to be memorialized as your point-in-time due diligence record by combining the responses from the risk analysis, responses from the internal stakeholder questionnaire (if used), responses from the vendor questionnaire, and the Additional Considerations section into a single document.

Depending on the internal risk management processes in your organization, the final report may be used as a basis for risk rating the GenAI product or service or complement additional due diligence material. Establishing a risk rating according to your organization's risk appetite and third-party risk management practices is your responsibility.

How to Preserve the Point-In-Time Due Diligence Record

One way to preserve the final report as a record of due diligence is to print the final report to PDF format as follows:

- First, ensure that the excluded questions are hidden from view in the final report by using the filter in the "III. Internal Stakeholders Responses" column (uncheck "Excluded"). See the previous section for an example.
- Make sure the Microsoft Excel application is focused on the final report tab by clicking on the final report tab.
- Go to the Microsoft Excel file menu and select the print option. Choose the print to PDF option that you have available.
- Make sure that "Print Active Sheets" is selected (typically the default option) to avoid printing the entire workbook.

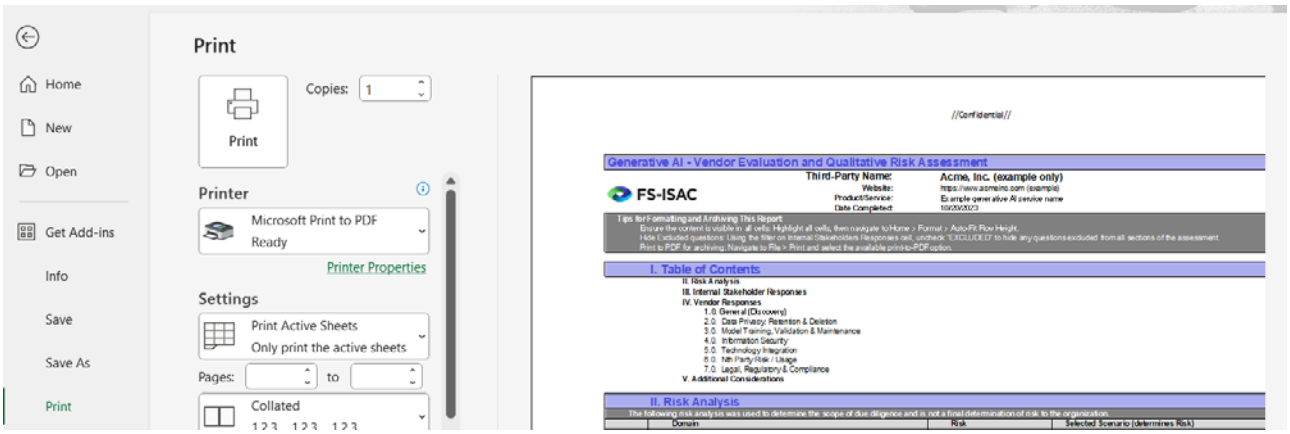


Figure 14: Printing the final report to PDF for record keeping/archiving purposes.

Periodic Re-Assessment

- Best practices in TPRM suggest that your GenAI assessment should be updated periodically, according to your risk management policies and procedures.
- At that time, save a new working copy of the last assessment, make any required changes by following the aforementioned workflow, and save the new final report to PDF.
- Repeat as often as your policy requires.

The views and opinions of the contributors are not necessarily those of their employers.

Group Chair

Benjamin Dynkin, Chair

Hiranmayi Palanki, Vice Chair

Contributors

Andrew Frisbie, *NBT Bancorp*

Ryan Beil, *Stellar Bank*

Lisa Matthews, *Ally Financial Inc*

Sebastian Fernandes, *Broadridge Financial Solutions*

Lincoln Guy, *Bank of Hope*

Ayo Adekunle, *Principal Financial*

Doug Reznick, *CME Group*

Chris Litas, *CME Group*

Dr Donnie Wendt, *Mastercard*

Hiranmayi Palanki, *American Express*

Tan Nguyen

Monica Maher, *Goldman Sachs*

Benjamin Dynkin, *Wells Fargo*

Mike Silverman, *FS-ISAC*

References and Resources

1 https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

Contact

fsisac.com

media@fsisac.com