IIA Audit Tool User Guide

Enterprise and Business Process Risks

Supports Implementation of the Global Internal Audit Standards™

Domain I | Domain II | Domain III | Domain IV | Domain V

Description

This user guide should be used with the companion Microsoft Excel workbook titled "Enterprise and Business Process Risks." The guide explains how internal auditors and other users can apply the workbook to support:

- Strategic and risk-based audit planning and effective engagement scoping.
- Insightful discussions with the board and senior management about the organization's risk appetite.
- Alignment between risks at the enterprise level and those at the business process level.
- Coordination among providers of assurance services.

Definition of Enterprise Risk Management

"Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."

COSO, *Enterprise Risk Management—Integrating with Strategy and Performance*, *Executive Summary*, p. 3.

The guide and workbook are designed to help with initiating and managing a structured enterprise risk management program, which includes the processes by which an organization identifies, assesses, manages, and monitors risks. The goal of enterprise risk management is to provide a holistic view of the organization's risks and identify strategies to mitigate them in alignment with the organization's risk appetite. According to The IIA's Three Lines Model, second line functions support risk management and control processes, while the internal audit function provides independent and objective assurance and advice on their effectiveness.

- ***Second line functions*** may use a risk matrix to assess, monitor, and report on risks across the organization. These functions also facilitate consistent risk evaluations, ensure key controls are identified, and support management in maintaining an up-to-date view of the risk landscape.
- ***The internal audit function*** may use a risk matrix to support its independent assurance and advisory services. Auditors can analyze the documented risks and controls as part of assessing the effectiveness of risk management practices. A matrix can help auditors identify areas where critical controls should be tested or improved, informing both audit planning and engagement performance.

The second line and internal audit functions can ensure alignment and comparability of risk information by using the same consistent methodology. This nonmandatory tool does not cover all the enterprise-level risks an organization may encounter. It may be edited to suit an organization's unique needs. Additional examples are included in The IIA's Global Practice Guide "Developing a Risk-Based Audit Plan."

The guide and workbook support the internal audit function in implementing:

- Standard 4.2 Due Professional Care
- Principle 9 and its standards for understanding governance, risk management, and controls processes; developing a strategy and risk-based internal audit plan; and coordinating with and relying upon providers of assurance services.
- Principle 13 and its standards for performing engagement risk assessments and effectively scoping engagements.

Workbook Overview

The figures in this user guide are excerpts from the tool's companion workbook.

Figure 1. Enterprise Risk Matrix

Figure 1 shows an excerpt of the workbook's "Enterprise Risk Matrix" tab to help explain how to use the worksheet.

							Optional	
Risk Identifier	Risk Category	Risk Description	Impact	Likelihood	Inherent Risk Leve	Strategy to Mitigate	Residual Risk	Strategy Importance
EL.1	Macroeconomic	Economic conditions inlcuding inflation may restirct growth opportunites and affect margins	5	2	10		5	5
EL.2	Macroeconomic	Increased labor costs affect profitability	2	7	14		12	2
EL.3	Macroeconomic	Adoption of emerging technologies (AI, automation, among others) will require skills the organization does not currently possess	8	8	64		10	54
EL.4	Macroeconomic	The current interest rate environment has a strong effect on the organization's cost of capital	7	3	21		18	3
EL.5	Macroeconomic	Volatility in global financial markets and exchange rates	5	6	30		26	4
EL.6	Macroeconomic	Another global pandemic occurs	9	9	81		20	61
EL.7	Macroeconomic	Shifts in perspectives related to social/DEI issues occur faster than the organization is able to manage effectively	2	3	6		5	1
EL.8	Macroeconomic	Stabilty of national and international markets may limit growth opportunities	8	9	72		56	16
EL.9	Macroeconomic	Wars and/or unstable governments may restrict growth/probability	10	10	100		10	90
EL.10	Macroeconomic	Ability to raise capital may limit growth	8	8	64		23	41

Risk Identifier – This column lists the unique identifier for each enterprise risk; for example, EL.1.

Risk Category – This column lists categories into which related risks are grouped. The risk categories set in the Excel workbook are "Macroeconomic," "Strategic," and "Operational." Additional risk categories may be added as desired to most accurately reflect the organization's approach.

Risk Description – This column describes identified enterprise-level risks. As a starting point, the column has been pre-populated with the top enterprise-level risks published by the NC State Poole College of Management ERM Initiative in collaboration with Protiviti Global Business Consulting.[1] Organizations should review these risks and may add or remove risks to suit their unique circumstances.

Impact – This data-validated column allows for the input of a number between 1 and 10 to indicate the impact the specific risk might have on an organization. An impact of 1 is minimal, while an impact of 10 is critical/high. Appendix A provides further details about scoring impact and likelihood.

Likelihood – This data-validated column allows for the input of a number between 1 and 10 to indicate the likelihood of the risk occurring. A likelihood score of 1 is very low (highly unlikely), while a likelihood of 10 is highly likely/certain. Appendix A provides further details.

Inherent Risk Level – This calculated column contains formulas that multiply impact (column D) by likelihood (column E) to determine the inherent risk score. The inherent risk score is the severity, or significance, of the risk before any controls or strategies are implemented to minimize the risk. The higher the score, the higher the risk to the organization. The column is conditionally formatted to indicate increasing risk severity/significance on a scale from green (lowest severity/significance) to yellow to red (highest severity/significance).

Strategy to Mitigate – This column provides space to document the strategies the organization uses to deal with risks. Enterprise-level risk strategies may be sorted into four general categories:

- ***Avoidance*** – Changing plans to circumvent a risk.
- ***Reduction*** – Implementing controls to reduce the likelihood or impact of a risk.
- ***Sharing/Transfer*** – Transferring the risk to a third party (for example, through insurance, outsourcing, or hedging).
- ***Acceptance*** – Deciding to accept the risk, typically because the cost of mitigation exceeds the potential impact.

1. NC State University's ERM Initiative and Protiviti. *2023-2032 Executive Perspectives on Top Risks*. Protiviti Inc., 2022. https://erm.ncsu.edu/resource-center/report-executive-perspectives-on-top-risks-for-2023-2032/.

Residual Risk Level (optional) – This column is used to define the risk level after mitigation strategies have been implemented. The more effective the strategies are, the lower this risk score should be. However, internal auditors or other users apply professional judgment to calculate the score. The higher the score, the more severe/significant the risk is to the organization. The column is conditionally formatted on a scale indicating increasing risk, from green (least severe/significant) to yellow to red (most severe/significant).

Strategy Importance (optional) – This calculated column contains formulas that subtract the inherent risk level column from the residual risk column to determine the degree to which the risk is reduced by implementing the mitigation strategy. The higher the strategy importance number, the more the organization relies on the strategy to mitigate risk. The column is conditionally formatted to indicate increasing importance on a scale from green (less important) to yellow (moderately important) to red (more important).

Figure 2. Enterprise Heat Map

Figure 2 shows an example of an enterprise heat map, a graphical representation of the risk level scores from the "Enterprise Risk Matrix" tab of the workbook. The heat map is a visual depiction that effectively communicates an overview of the average inherent risk scores. Each risk, with its corresponding risk identifier, is plotted along the axes of impact and likelihood, indicating its inherent risk score. The graph's color gradient visually depicts increasing levels of risk by progressing from green (low risk) to yellow (moderate risk) to red (high risk). (Note: if any risks have the same score, the user must manually adjust the data labels so that each risk identifier can be seen.)

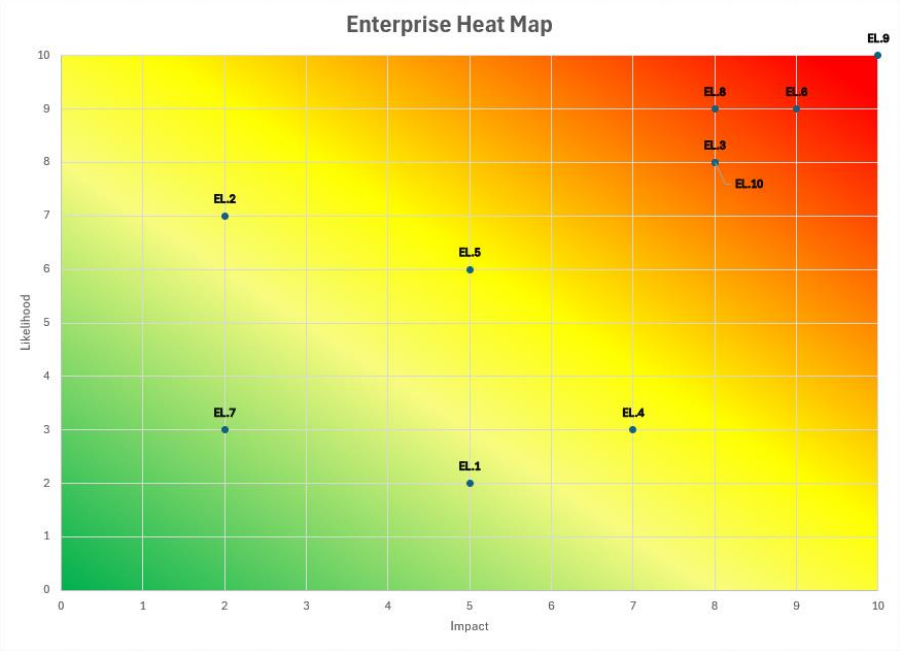


Figure 3. Business Process Risk Matrix

An excerpt of the Excel workbook's "Business Process Risk Matrix" tab helps illustrate how to use the worksheet. The purpose of each column is described below.

Business Process Risk Matrix											
							Optional				
Risk Identifier #	Risk Category	Risk Description	Impact	Likelihood	Inherent Risk Level	Control(s) to Mitigate	Residual Risk	Control Importance	Test Plan	Test Results	Notes
BP.1	Accounts Payable	Payments are not properly authorized	2	2	4		2	2			
BP.2	Accounts Payable	Payments are made to fraudulent invoices	4	5	20		10	10			
BP.3	Accounts Payable	Duplicate payments are made	7	9	63		8	55			
BP.4	Accounts Payable	Clerical errors result in errors in payment amounts	10	3	30		25	5			
BP.5	Accounts Payable	Payments are made late	9	9	81		45	36			

Risk Identifier – This column lists the unique identifier for each business process risk.

Risk Category – This column identifies the business process (for example, accounts payable, payroll, IT access management, and so forth) under which relevant risks are grouped. Additional risk categories may be added or the groupings may be adjusted to suit the organization's structure and conditions.

Risk Description – This column describes the identified business process risk and has been pre-populated with examples of business and IT general control process risks. Management and other functions (as needed) should review these risks and add or remove risks to suit the specific circumstances of the organization.

Impact – This data-validated column allows for the input of a number between 1 and 10 to indicate a risk's potential impact on the organization. An impact of 1 is minimal, while 10 is critical/high.

Likelihood – This data-validated column allows for the input of a number between 1 and 10 to indicate the likelihood of the risk occurring. A likelihood of 1 is very low (highly unlikely), while a likelihood of 10 is highly likely (certain to occur). See Appendix A for further details on scoring impact and likelihood.

Inherent Risk Level – This column contains formulas that multiply the "Impact" and "Likelihood" columns to determine an inherent risk score. The result is the risk level before any controls have been implemented to mitigate the risk. The higher the score, the higher the inherent risk to the organization. The column is conditionally formatted to indicate increasing risk scores on a scale from green (low risk) to yellow (moderate risk) to red (high risk).

Control(s) to Mitigate—This column provides blank cells for documenting the controls in place to mitigate the identified risks.

Residual Risk Level (optional) – This column is used to document the risk level after mitigating controls have been implemented. The more effective the controls are, the lower the residual risk score should logically be, but the score is ultimately based on the professional judgment of the internal auditor or other user calculating the score. The column is conditionally formatted to indicate increasing risk scores on a scale from green (low residual risk) to yellow (moderate residual risk) to red (high residual risk).

Control Importance (optional) – This calculated column contains formulas that subtract the level of "Residual Risk" column from that of the "Inherent Risk" column to determine the degree to which the corresponding controls reduce the risk. The higher the control importance number, the more the organization relies on that control to mitigate risk. The column is conditionally formatted to indicate increasing importance on a scale from green (less important) to yellow (moderately important) to red (highly important).

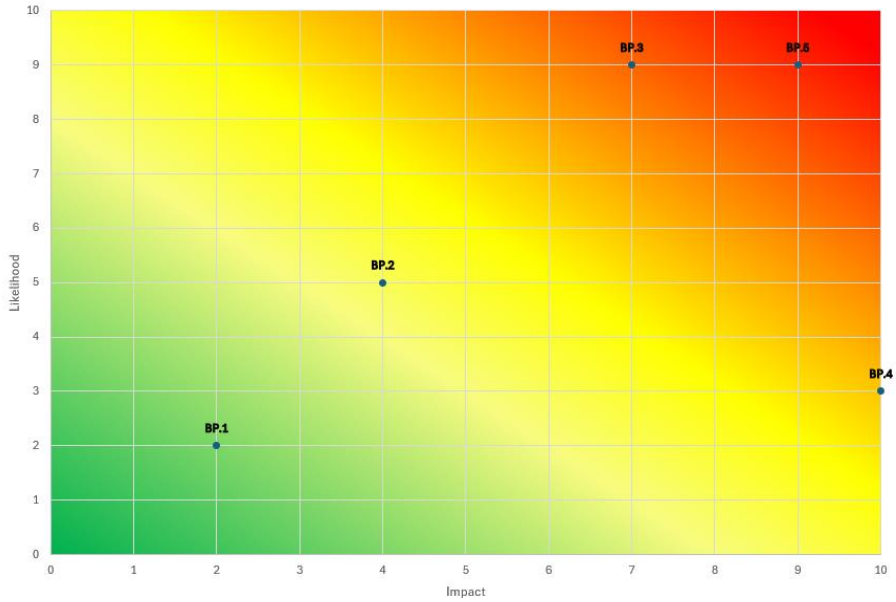
Test Plan – This column provides blank cells in which to briefly document a summary of the organization's plan for testing the control(s) noted in the "Control(s) to Mitigate" column.

Test Results – This column provides blank cells in which to document the high-level results of the tests described in the "Test Plan" column.

Notes – This column provides blank cells in which to document additional notes related to the risk, control(s), test plans, and test results.

Figure 4. Business Process Heat Map

Figure 4 shows an example of a business process heat map, a graphical representation of the risk level scores from the "Business Process Risk Matrix" tab of the companion Excel workbook. The heat map is an effective way to visualize risk levels. It plots each risk level score and labels it with the risk identifier. The graph's color gradient visually depicts increasing risk by progressing from green (low risk) to yellow (moderate risk) to red (high risk). (Note: if any risks have the same risk level, the user must manually adjust the data labels so that each risk identifier can be seen.)



How to Use the Workbook

To use the "Enterprise Risk Matrix" and "Enterprise Heat Map" tabs in the Excel workbook, internal auditors or other users should perform these steps:

1. The "Enterprise Risk Matrix" tab contains examples of risks to help start an enterprise risk management program. Internal auditors or other users of the worksheet should review these risks internally and with senior management to determine whether they apply to the organization and to identify any other risks that should be added.
2. Once the risks are finalized, a copy of the completed tab (worksheet) should be distributed to appropriate personnel, perhaps risk owners and others with direct responsibilities, depending on the organization's size and complexity. Reviewers should document their perceptions of the impact and likelihood of each identified risk. Reviewers should also add notes related to individual risks or any other risks that they believe should be included.
3. Once all the forms have been completed and returned, internal auditors or other users should consolidate the results by averaging the reviewers' responses (impact and likelihood scores) for each risk and adding the consolidated scores to the "Enterprise Level" tab. The product of the impact and likelihood scores should populate the "Inherent Risk Level" column.
4. In the "Strategy to Mitigate" column, reviewers should identify any strategies currently in use to address the risks.
5. Where strategies to mitigate risks have been noted, the "Residual Risk" column should be filled out. The residual risk is determined by reviewing the inherent risk, evaluating the effectiveness of the mitigation strategy, and determining the remaining risk.
6. The "Strategy Importance" column reflects the difference between the inherent and residual risks. Higher values indicate strategies that are more critical to reducing risk.
7. The risk scores should be plotted on the heat map, with the average impact represented along the X axis and average likelihood along the Y axis.
8. The involved stakeholders, including management, should determine the risk level threshold, which is the level at which a strategy is required to be implemented to either avoid, reduce, share, or accept the risk, depending on the organization's risk appetite. (This could be at a score of 50, 60, or 70, for example.) All risks above the threshold should be monitored and periodically reviewed to ensure the associated controls are operating as intended. Additionally, if the optional "Residual Risk" and "Strategy Importance" columns are used, the residual risk scoring should be determined through discussion with management.
9. This process may be repeated as frequently as the organization desires.

To use the "Business Process Risk Matrix" and "Business Process Heat Map" tabs in the Excel workbook, perform these steps:

1. Internal auditors or other users should review the example risks (provided in the Excel workbook) internally and with each business process owner to determine whether they apply to the business process and to identify any other risks that warrant being documented.
2. Once the risks are finalized, internal auditors or other users should schedule a meeting with business process owners and stakeholders to validate each risk and assign it an impact and likelihood score.
3. All controls applicable to each risk should be documented in the "Control(s) to Mitigate" column. Additionally, the "Residual Risk" and the corresponding "Control Importance" columns may be completed based on discussions with business process owners and stakeholders to further identify key controls in each business process. The higher the number in the "Control Importance" column, the more the organization relies on that control to mitigate risk.
4. The controls should be reviewed to ensure that they adequately mitigate the risk. Risks that do not have controls associated with them or are not adequately controlled should be identified, and appropriate controls for those risks should be created.
5. This process may be repeated as frequently as the organization desires.

Strategic Implications

The Enterprise and Business Process Risks Tool supports a consistent, strategic, and value-adding approach to assessing risks. Governance, risk oversight, and organizational resilience are strengthened when risk assessments are integrated across levels, governance-level risk appetite discussions occur, and the work of assurance providers is coordinated.

Enterprise Risk Matrix for Strategic Audit Planning

The enterprise risk matrix helps identify and evaluate risks across the organization, enabling:

- ***Prioritization*** based on inherent risk and the difference between inherent risk and residual risk, which this tool calls "Strategy Importance."
  - Inherent risk is the risk before any mitigation.
  - Residual risk is the risk after mitigation strategies have been implemented.
  - Strategy importance is the difference between inherent and residual risk. The greater this number, the greater the importance of the strategy is in mitigating risk. These strategic items of higher importance should be reviewed for proper implementation since they are key to mitigating the greatest risk.
- ***Classification of risk types*** (such as macroeconomic, strategic, operational), with suggested examples to guide alignment with the organization's risk universe.
- ***Use of regulatory, operational, and financial thresholds*** (see Appendix A) to anchor discussions on risk appetite with leadership. These thresholds offer a quantifiable reference for whether risk responses are required, accepted, or escalated. Additionally, the threshold examples noted in Appendix A should be discussed with the board and senior management. Their input helps determine whether the thresholds should be implemented.

Using the tool to collect this risk information facilitates effective risk-based audit planning, supporting the implementation of Principle 9 Plan Strategically, especially Standards 9.2 Internal Audit Strategy and 9.4 Internal Audit Plan.

Business Process Risk Matrix for Engagement Scoping

The business process risk matrix enables internal auditors or other users to:

- ***Determine risks and controls*** at the level of business processes.

- ***Assess inherent and residual risk***, providing a view into where and how control activities reduce risk.
- ***Determine control importance*** by evaluating the difference between levels of inherent and residual risk); knowing this information is critical to help tailor audit testing efforts.
- ***Record testing plans and results*** to document assurance on control effectiveness.

Together, these insights shape a focused and risk-informed engagement scope.

Aligning Enterprise Risk Management and Process-Level Risk Assessments

Using the worksheets together has several benefits:

- ***Shared scoring logic and risk impact definitions*** ensure that enterprise and business process risks are evaluated consistently.
- ***The "Residual Risk" and "Strategy/Control Importance" columns*** in both worksheets enable internal auditors and other users to track how effectively mitigation strategies operate across levels.
- ***Enterprise-level risks can be mapped to business processes***, creating a clear linkage and demonstrating how strategic risks manifest operationally.

This alignment improves audit and risk management consistency and reinforces the internal audit function's strategic value.

Supporting Dialogue on Risk Appetite

Organizations can use this tool to understand and evaluate governance, including the alignment of risks with the organization's risk appetite.

The tool supports this understanding and evaluation by:

- ***Providing a data-driven foundation*** for assessing whether current residual risk levels are within acceptable limits.
- ***Highlighting residual risks that exceed risk appetite***, prompting potential actions or governance discussions.
- ***Enabling illustrative financial and operational criteria*** (for example, >$25M financial loss or reputational damage) to make risk level thresholds explicit and tangible.

Understanding and evaluating governance also supports the internal audit function's conformance with the Global Internal Audit Standards. The internal audit function does not set the organization's risk appetite; rather, the function evaluates and challenges whether the risk appetite is accurately reflected in risk management and control practices.

Coordination Among Assurance Providers

This tool supports the internal audit function's conformance with Standard 9.5 Coordination and Reliance. and helps assurance providers coordinate their work by providing opportunities for:

- ***Coordination between the internal audit function and second line functions*** (such as compliance, cybersecurity, data governance) to facilitate sharing risk information and to prevent duplication of work.
- ***Relying on each other's assurance work,*** where risk coverage is strong and controls are deemed effective, thus conserving resources.
- ***Creating or contributing to an assurance map***, linking internal and external sources of assurance to specific risks and documenting the extent of reliance.
- ***Evaluating reliability*** using criteria such as provider independence, objectivity, and professional competence.

Second line functions assess and monitor risks, and the internal audit function independently evaluates the quality and effectiveness of those assessments and responses. This complementary approach strengthens overall risk coverage by ensuring the sound implementation of risk management and the provision of objective assurance by a function independent of management. For more information, see The IIA's Global Practice Guide, "Coordination and Reliance: Working with Other Assurance Providers."

Best Practices

To maximize the tool's effectiveness, users should:

- ***Use all the worksheets together.*** Applying a coordinated top-down and bottom-up approach ensures alignment: assessing risks at the enterprise level may be more appropriate for comprehensive audit planning, while assessing risks at the business process level may be better suited for planning individual engagements.
- ***Review and update regularly,*** such as during regular planning cycles and following significant organizational changes. Engagement findings and other audit results should also be incorporated into risk assessments.
- ***Document all assumptions and judgments.*** It is particularly important to document the professional judgment and rationale behind residual risk scores.
- ***Use strategy/control importance scores.*** These scores help focus testing on the most important controls.
- ***Share findings with risk owners and assurance providers*** to validate ratings and encourage coordination and reliance.
- ***Facilitate regular board discussions*** using dashboards or heat maps generated from both tools.

Appendix A. Impact and Probability Scoring Detail Examples

Risk Impact Scale and Criteria

Impact Description	Impact Score	Regulatory Criteria*	Operational Criteria*	Financial Criteria*
Catastrophic	9 - 10	Complex, highly regulated environment with strict enforcement; consequences for noncompliance likely to cause legal liabilities and penalties that may result in partial or complete shutdown. Significant financial and reputational impacts.	One or more business units or the entire organization may be unable to operate. Impact on reputation.	Greater than $25 million
Highly Significant	7 - 8	Complex regulatory environment; legal liabilities and penalties for noncompliance may receive public attention and have a lasting impact financially and reputationally.	Multiple business units may be significantly affected. Organization's ability to operate or serve customers may be severely reduced. Impact on reputation.	$10 million to $25 million
Significant	5 - 6	Laws and regulations are consistently enforced. Legal liabilities and penalties for noncompliance are material.	One or more business units may be materially affected. Organization's ability to operate or serve customers may be significantly reduced.	$5 million to $10 million (material)
Moderate	3 - 4	Active regulatory environment with small to moderate penalties for noncompliance.	Operational effectiveness and efficiency are moderately damaged.	$1 million to $5 million
Low	1 - 2	Regulatory environment is lax or penalty for noncompliance is small.	Operational effectiveness or efficiency could be improved, but operations proceed uninterrupted.	Less than $1 million

* These criteria are provided as an illustration only. They should be discussed with the board and senior management and adjusted based on the organization's size, risk appetite, and other conditions specific to the organization.

Risk Likelihood Scale and Descriptions

Rating	Score	Description	Criteria
Very high	9 – 10	Likelihood of risk occurring is very high relatively.	Operational processes are complex and controls are not effective.
High	7 - 8	Likelihood of risk occurring is high relatively.	Operational processes are complex and some control weaknesses are noted.
Moderate	5 - 6	Likelihood of risk occurring is moderate relatively.	Operational processes are moderately complex; minor control weaknesses are noted.
Low	3 - 4	Likelihood of risk occurring is low relatively.	Operational processes are not complex; controls are mostly effective.
Very low	1 - 2	Likelihood of risk occurring is very low relatively.	Operational processes are not complex; controls are effective.

About The Institute of Internal Auditors

The Institute of Internal Auditors® (The IIA®) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit www.theiia.org.

Disclaimer

Copyright

June 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Boulevard, Ste. 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101