



**AICPA® & CIMA®**

Together as the Association of International  
Certified Professional Accountants

# Risk Heat Map

An Updated Risk  
Assessment Tool

## **About the Association of International Certified Professional Accountants, and AICPA & CIMA**

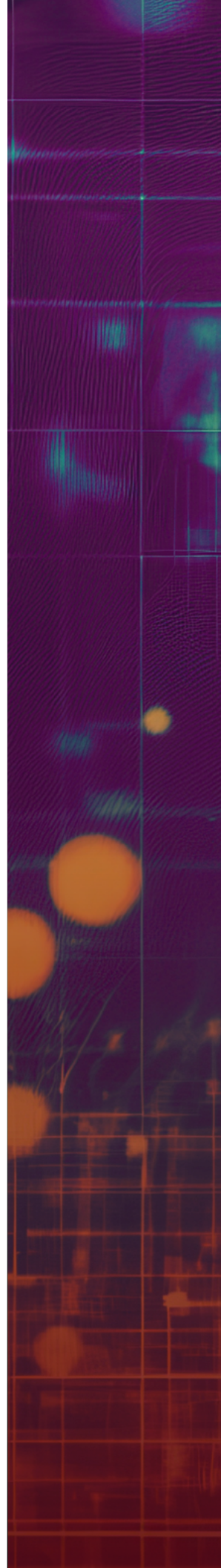
The Association of International Certified Professional Accountants® (the Association), representing AICPA® & CIMA®, advances the global accounting and finance profession through its work on behalf of 597,000 AICPA and CIMA members, students and engaged professionals in 188 countries and territories. Together, we are the worldwide leader on public and management accounting issues through advocacy, support for the CPA license and specialised credentials, professional education and thought leadership. We build trust by empowering our members and engaged professionals with the knowledge and opportunities to be leaders in broadening prosperity for a more inclusive, sustainable, and resilient future.

The American Institute of CPAs® (AICPA), the world's largest member association representing the CPA profession, sets ethical standards for its members and U.S. auditing standards for private companies, not-for-profit organisations, and federal, state, and local governments. It also develops and grades the Uniform CPA Examination and builds the pipeline of future talent for the public accounting profession.

The Chartered Institute of Management Accountants® (CIMA) is the world's leading and largest professional body of management accountants. CIMA works closely with employers and sponsors leading-edge research, constantly updating its professional qualification and professional experience requirements to ensure it remains the employer's choice when recruiting financially trained business leaders.

# Contents

- 2 **What is a risk heat map?**
- 4 **Benefits of risk heat maps**
- 4 **Questions to consider when implementing a risk heat map**
- 5 **Risk do's and don'ts**
- 6 **Appendix – sample populated risk heat map**
- 7 **Lead author**



# What is a risk heat map?

A risk heat map is a visual, often colour-coded tool used to assist in rating risks, enabling discussions and decision-making throughout the risk assessment process.

Whether conducted as part of a broad-based enterprise risk management process or as a more narrowly focused internal control process, mapping each risk is a critical step in addressing risk management. This assessment involves evaluating the likelihood and potential impact of identified risks that are both financial and nonfinancial in nature.

Heat maps are a way of representing the resulting qualitative and quantitative evaluations of the probability of risk occurrence and the impact on the organisation in the event it experiences a particular risk.

The development of an effective heat map has four critical elements:

1. A common and understood set of terms.
2. A common understanding of the company's risk appetite.
3. Definitions for varying levels of impact should a risk occur. This includes assisting in determining what is material for the entity, division, or department.
4. Assignment of probabilities and likelihood of the occurrence of the risk and its potential impacts.

Whether arranged in a 3x3 grid or a 5x5 grid, a heat map is used to provide a picture of the various ranges in risk characteristics. Any organisation can map probability ranges to common qualitative characteristics of risk-event likelihood and develop a ranking scheme for potential impacts. For example, risks can be ranked on the impact based on what is material in financial terms or in relation to the achievement of strategic objectives. In the following 5x5 grid, risks are prioritised using a simple multiplication formula.

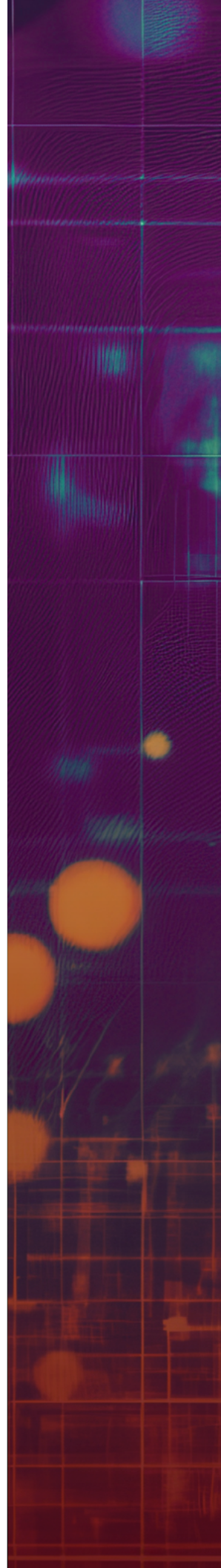
Many organisations visualise risks on a heat map using a 'residual risk' basis that considers the extent to which risks are currently mitigated, reduced by internal controls, or affected by other risk response strategies. Whether using a numeric system (generally, one being the lowest possibility to 25 being the highest possibility) or a language-based system (mild-moderate-critical), a grid will easily identify those most critical risks.

Numeric 5x5 grid

POTENTIAL IMPACT	Extreme	5	10	15	20	25
	High	4	8	12	16	20
	Medium	3	6	9	12	18
	Low	2	4	6	8	10
	Negligible	1	2	3	4	5
		Remote	Unlikely	Possible	Likely	Probable
	% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%
		LIKELIHOOD				

Language-based 5x5 grid

PROBABILITY	Almost Certain	Moderate	Major	Major-Critical	Critical	Critical
	Likely	Moderate	Major	Major	Major-Critical	Critical
	Possible	Moderate	Moderate	Major	Major	Critical
	Unlikely	Minor	Moderate	Moderate	Major	Critical
	Rare	Minor	Minor	Moderate	Moderate	Major
		Insignificant	Minor	Important	Concerning	Extreme
		IMPACT				



## Benefits of risk heat maps

- **Quick** and **efficient** visual to enable decision-making
- A visual, **big picture**, holistic view to share while making strategic **decisions**
- Improved **management** of risks and governance of the risk management process
- Allows for **increased focus** on the company's risk appetite and risk tolerance
- Added **precision** in the risk assessment process
- Additional considerations related to main risks
- **Identification** of gaps in the risk management and control process
- Greater **integration** of risk management across the enterprise and embedding of risk management in operations.

## Questions to consider when implementing a risk heat map

- How much risk are we willing to accept?
- What thresholds do we want to monitor and use to alert to action?
- What constitutes a material risk for our company?
- What is the range of acceptable variance from our key performance and operating metrics?
- What thresholds do we want to monitor and use to alert to action?
- How will we define our terms to evaluate the likelihood of risk events, as well as their impact on our business, so that we can map our potential risk events to our heat map?
- What types of risk will immediately affect our continuity? How long can we sustain our business in the event a critical risk occurs?
- Have we considered mitigation activities on the rating of risks? What risks are we willing to accept?

# Risk do's and don'ts

## Actions to take/do's

- Conduct risk self-assessment workshops with various departments to take advantage of the insights of managers.
- Prepare an initial risk library to use as a starting point.
- Get consensus on risk tolerances – acceptable levels of missing targets.
- Identify thresholds for action.
- Clarify terms used to establish probability estimates.
- Establish participants' understanding of the effectiveness of controls and other risk responses used in the organisation.
- Look outside your entity to the industry and the world for potential identification of risks.

## Actions to avoid/don'ts

- Don't rely on surveys to capture initial thoughts about risk.
- Avoid getting stuck in root cause analysis.
- Don't forget to look outside the box.
- Don't forget to quantify risks in terms of potential financial impact on the organisation in terms of cash, earnings, etc.
- Don't forget to consider the state of controls and other risk management practices in place in the organisation.

# Appendix – sample populated risk heat map

Populating a risk heat map provides a visual aid for identification of the greatest opportunities and challenges for senior management to consider.

The following risks are mapped out on two sample heat maps below:

XYZ Corporation is an international entity engaged in sustainable manufacturing of a patented widget that is required for production within all areas of the transportation industry. XYZ has six production facilities: two in the US, and one each in the UK, Italy, Poland, and Japan. They have identified the following risks:

- 1 Supply chain disruption to any of the facilities. This is deemed to be a low-moderate or low-medium risk based on the ability of the other facilities to ramp up production and incur low to medium delivery impacts to customers.
- 2 As the only patent-holding entity on this very specific line for the transportation industry, the risk of another entity

developing a similar item at a lower price point and obtaining a patent is deemed to be moderate or medium risk.

- 3 The eastern U.S. plant, located in North Carolina, has had a high level of natural disaster occurrence in the past years, and this continues to be a concern. Disruption to operations from wildfires, tornados, and flooding can have a significant impact.
- 4 Cybersecurity risks within their global organisation are deemed possible, but a low risk. XYZ has obtained the services of several international technology and security organisations to prevent this risk or to minimise the impact if it occurs.
- 5 Regulations around reporting, policy, and requirements change as globally new administrations are in place.

Sample populated risk heat map using language-based 5x5 grid

PROBABILITY	Almost Certain	Moderate	Major	Major-Critical	Critical	Critical
	Likely	Moderate 5	Major	Major 2	Major-Critical	Critical 3
	Possible	Moderate	Moderate	Major	Major	Critical
	Unlikely	Minor 4	Moderate	Moderate 1	Major	Critical
	Rare	Minor	Minor	Moderate	Moderate	Major
		Insignificant	Minor	Important	Concerning	Extreme
		IMPACT				

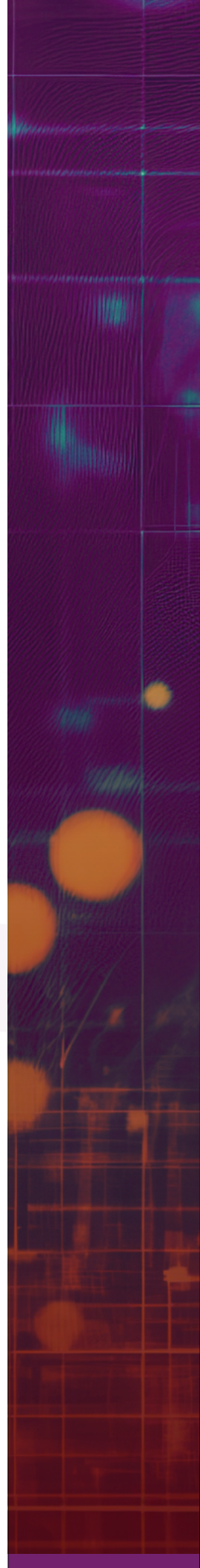
Sample populated risk heat map using numeric 5x5 grid

POTENTIAL IMPACT	Extreme	5	10	15	20	25
	High	4	8	12	16 3	20
	Medium	3	6 5	9 2	12	18
	Low	2	4 4	6 1	8	10
	Negligible	1	2	3	4	5
		Remote	Unlikely	Possible	Likely	Probable
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%
		LIKELIHOOD				

Lead author

Lori A. Sexton, CPA, CGMA,  
 Associate Technical Director, Management Accounting  
 The Association of International Certified Professional Accountants

Publication date: May 2025



For information about obtaining permission to use this material other than for personal use, please email [copyright-permissions@aicpa-cima.com](mailto:copyright-permissions@aicpa-cima.com). All other rights are hereby expressly reserved. The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. Although the information provided is believed to be correct as of the publication date, be advised that this is a developing area. The Association, AICPA and CIMA cannot accept responsibility for the consequences of its use for other purposes or other contexts.

The information and any opinions expressed in this material do not represent official pronouncements of or on behalf of the AICPA, CIMA, or the Association of International Certified Professional Accountants. This material is offered with the understanding that it does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date of issuance has been made, no guarantee is or can be given regarding the applicability of the information found within to any given set of facts and circumstances.



Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

© 2025 Association of International Certified Professional Accountants. All rights reserved. AICPA and CIMA are trademarks of the American Institute of CPAs and The Chartered Institute of Management Accountants, respectively, and are registered in the US, the EU, the UK and other countries. Globe Design is a trademark of the Association of International Certified Professional Accountants. 2503-005758