



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A STUDY OF RISK MANAGEMENT AND RESILIENCE

J.B.CHATRIK VARMA¹, Y. Surya Narayana Murthy²

¹ Department of Business Administration, KL Business School, KLEF, Vaddeswaram, Guntur, AP.

Mail Id: jampanachatreekvarma222022@gmail.com

² Assistant Professor, BBA, KL Business School, KLEF

Mail id: bobby.yamijala@gmail.com

ABSTRACT :

This article discusses how folks responded to questions on risk management and how strong their organizations are when facing challenges. It covers well-known ideas like risk management best practices, artificial intelligence, real-time monitoring, thinking ahead and predicting, and risks tied to things like climate change, cybersecurity, and Enterprise Risk Management (ERM). We used quantitative, descriptive research with the data in Excel, based on 10 sets of 100 responses and ten multiple-choice knowledge questions. Out of 1000 chances to answer, 850 were right, or 85.0%. On average, each person got 8.50 correct answers (SD=1.24; median=9). The percentage of correct answers was between 80% and 91%, showing that some ideas were recognized more easily than others. This short analysis shows that most people picked up on key points like climate-related risks, predictive risk management, and cybersecurity, but the results here shouldn't be used as proof of organizational resilience or cause-and-effect; even names and email addresses were removed for privacy in this report. Risk management, resilience, corporate resilience, enterprise risk management, artificial intelligence, cyber risk, climate risk, prescriptive risk management, and questionnaire.

1.INTRODUCTION

Business exists in a world full of uncertainty, fast-changing technology, tough competition, climate risks, cyber threats, and connected supply chains. Risk management is a step-by-step way to find, analyze, sort out, handle, and keep track of risks that could affect your goals. Businesses can't get rid of all uncertainty, but they need to figure out which risks matter most and what to do about them.

Resilience is really helpful for managing risks. Resilience means being able to see problems coming, handle them when they hit, adjust how things are done, and bounce back—all while keeping important services running. Being resilient isn't just about having a risk register; it means building up strong leadership, good communication, flexible ways of working, skilled employees, solid information, and backup plans.

Technology can help with risk management today by handling lots of data, finding unusual patterns, and making it easier to keep track of things quickly. Predictive analytics and AI might help us spot problems sooner, but they don't get rid of risk and shouldn't take the place of good judgement. Good risk management means making sure people know who's responsible, keeping track of the right info, staying on top of things often, and watching out for any new risks that might pop up.

I'll use the style from the reference paper that's attached. It will follow that approach for risk management and resilience, and will only use the uploaded spreadsheet for numbers. Since the spreadsheet just has sample responses and doesn't actually measure organizational resilience, the paper will look at which answers were picked and what those choices say about the respondents' knowledge.

2.REVIEW OF LITERATURE

ISO 31000:2018 says risk management means having a set of organised ways and steps to deal with risk, built into how a company runs and makes decisions. It says that risk management should be designed for each situation and kept up-to-date over time.

The COSO Enterprise Risk Management framework connects strategy, performance, and risk. When organizations include risk in how they set goals, assign resources, and review performance, it shifts risk management from just a compliance task.

Resilience research and international disaster-risk guides often stress being ready, adapting, staying operational, and recovering.

Basically, it means spotting when something might go wrong, trying to keep it from causing too much trouble, making sure the most important things still work, and learning from what happens.

New developments have given risk managers more tools to work with. AI, data analysis, connected sensors, and real-time monitoring can help spot risks early and make decisions faster. But the outcome will also rely on things like data quality, management, clarity, security, and how well people are able to control it.

Climate change can mess with buildings, transport, supply chains, insurance, and financing, while cyber threats can affect data, systems, processes, and even your reputation—so organizations need to link up how they handle these risks. These risks can be linked together, and when that happens, they can affect financial, operational, legal, and reputational areas.

So, the literature shows two main research paths: risk management, which helps people make clear decisions when things are uncertain, and resilience, which is about being strong, flexible, and able to bounce back from disruptions

.3. Research Gap

For a student study, it's important to find out if people recognize common risk-management ideas when dealing with different current issues. Risk frameworks cover broad ideas, but a person will know certain specifics—like risk prioritization, predictive analytics, climate risk, cyber risk, and ERM. This sample questionnaire helps show if these concepts have the same rate of correct answers.

Right now, we don't have data on company recovery time, how well business continuity works, resilience maturity, or real-life work outcomes. So, this paper points out a smaller gap in what we know and suggests some ideas that might need more research out in the field.

4. Objectives of the Study

Here's the breakdown of their background and work profile from 100 people who responded.

To check how well people grasped the main points about handling risk in an organisation.

Check for AI detection with live tracking and steps to manage risks before they happen.

To figure out how much people think they know about climate risks, use the Cybersecurity and Enterprise Risk Management scale.

The goal is to give clear ways to boost awareness of risk management and help make the organization more resilient.

5. Conceptual Framework of the Study

The article uses a simple model to show how being aware of risk management helps people understand how an organization handles risk, including identifying risks, assessing them, monitoring, early warnings, predicting risks, and integrating everything with ERM. If leadership, communication, resources, and learning include them, they can help an organization get ready for change and bounce back. The Excel questionnaire checks if people know about certain practices, but it doesn't measure actual resilience in the end.

6. Hypotheses / Research Questions

Since the questionnaire only gathers multiple choice answers and doesn't measure resilience in a reliable way, the analysis is just descriptive. The analysis will focus on these research questions:

- RQ1: Which risk management ideas did people get right most often, and which ones did they struggle with the most?
- RQ2: How well can people recognize and keep track of risks using technology?
- RQ3: How well do people recognize concepts related to climate, cybersecurity, and ERM?
- RQ4: What learning priorities can we figure out from these behaviours?

They aren't testing any causal hypothesis. There's no evidence that being aware leads to resilience, or that any technology actually changes what happens in an organization.

7. Research Methodology

7.1 Research Approach

We used a quantitative method because the data includes grouped respondent profiles and their answers, which can be counted and shown as percentages.

7.2 Research Design

This study describes things as they are and uses a cross-sectional approach. The sample sums up the answers in one spot, then compares the percentage of people who picked the right answer for each question.

7.3 Population and Sample

There are 100 responses recorded in the workbook. Respondents share different ages, backgrounds, work histories, and job details from their industries. The workbook doesn't say how people were chosen or recruited, so we can't know if the group represents everyone.

7.4 Sampling Technique

The file doesn't say how the samples were collected. The records aren't claimed to be a probability sample.

7.5 Source and Instrument of Data Collection

The Excel worksheet named "100 Responses" that each user submits is the only source of data. The worksheet has some fields for the respondent's profile and ten multiple choice questions about risk management and resilience. There are direct identifiers, but we didn't use the respondents' names or email addresses in this report.

7.6 Variables and Measurement

The profile includes variables like sex, age, education, experience, job, occupation, firm size, firm income, and region of residence. The main thing measured was whether each of ten knowledge questions was answered correctly or not (correct=1, incorrect=0, n=168), and the total knowledge score is just the sum of up to ten right or wrong answers.

7.7 Statistical Tools Used

Counts and percentages for profile summaries and answers to each question. Mean, median, and standard deviation for the overall correct-answer score. Bar charts showing sector distribution, age profile, correct response rates, and score spread. There are no inferential tests to support a causal claim.

7.8 Ethical Considerations

Names and email addresses in the workbook were taken out of all the tables and figures because they can identify people. The report just includes summary data. Since the file doesn't record consent, recruitment, or if the people are real, the data should be used carefully, and you need to mention that the dataset is synthetic or a sample when submitting the paper

8. Data Analysis and Interpretation

8.1 Respondent Profile

Gender distribution

Category	Frequency	Percentage
Female	52	52.0%
Male	40	40.0%
Prefer not to say	5	5.0%
other	3	3.0%

Interpretation: The largest category for gender distribution is Female (52 respondents; 52.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Age distribution

Category	Frequency	Percentage
20–30 years	50	50.0%
31–40 years	19	19.0%
Below 20 years	14	14.0%
41–50 years	14	14.0%
Above 50 years	3	3.0%

Interpretation: The largest category for age distribution is 20–30 years (50 respondents; 50.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Educational qualification

Category	Frequency	Percentage
Undergraduate	44	44.0%
Postgraduate	23	23.0%
Higher Secondary	20	20.0%
Professional Qualification	10	10.0%
Other	3	3.0%

Interpretation: The largest category for educational qualification is Undergraduate (44 respondents; 44.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Work experience

Category	Frequency	Percentage
1–3 years	37	37.0%
Not Applicable	18	18.0%
4–6 years	17	17.0%
Less than 1 year	13	13.0%
7–10 years	10	10.0%
More than 10 years	5	5.0%

Interpretation: The largest category for work experience is 1–3 years (37 respondents; 37.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Occupational position

Category	Frequency	Percentage
Student	35	35.0%
Executive/Staff	31	31.0%
Supervisor	9	9.0%
Senior Manager	9	9.0%
Other	9	9.0%
Manager	7	7.0%

Interpretation: The largest category for occupational position is Student (35 respondents; 35.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Industry/sector

Category	Frequency	Percentage
Retail	15	15.0%
IT/Technology	14	14.0%
Other	13	13.0%
Manufacturing	13	13.0%
Banking/Finance	12	12.0%
Healthcare	12	12.0%
Education	11	11.0%
Logistics/Supply Chain	10	10.0%

Interpretation: The largest category for industry/sector is Retail (15 respondents; 15.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Organization size

Category	Frequency	Percentage
Medium	46	46.0%
Large	23	23.0%
Small	22	22.0%
Not Applicable	9	9.0%

Interpretation: The largest category for organization size is Medium (46 respondents; 46.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

Location distribution

Category	Frequency	Percentage
urban	63	63.0%
Rural	21	21.0%
Semi-Urban	16	16.0%

Interpretation: The largest category for location distribution is urban (63 respondents; 63.0%). These profile data describe the composition of the supplied sample but cannot establish that it represents a wider population.

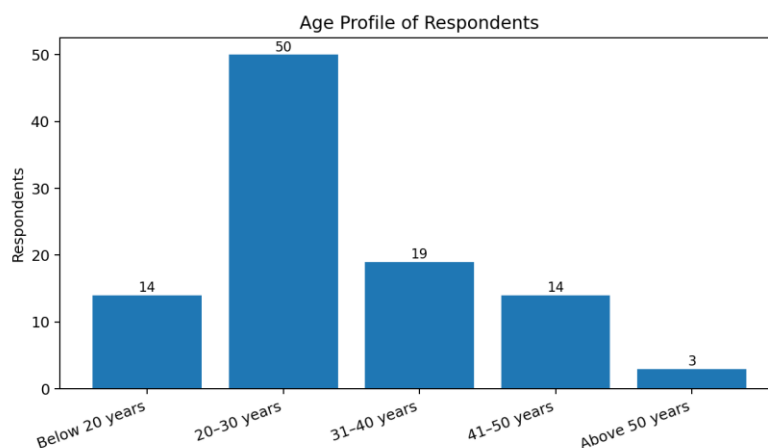


Figure 2. Age profile of respondents.

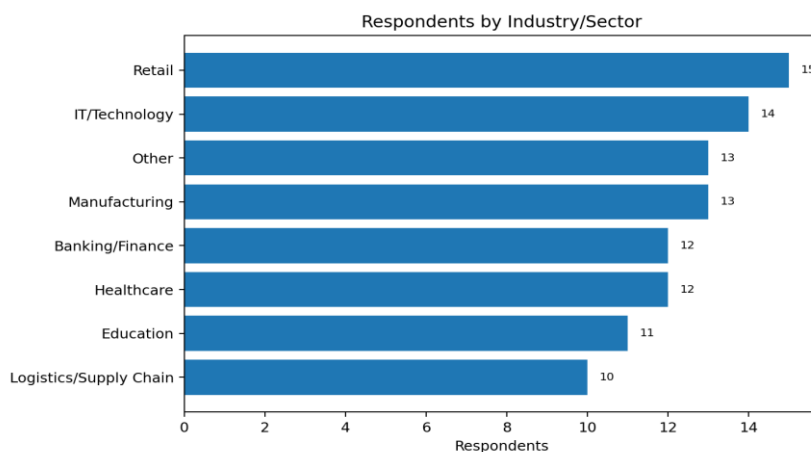


Figure 3. Respondents by industry/sector.

8.2 Correct Responses by Question

Question area	Designated correct answer	Correct (n)	Correct (%)
Major risk-management challenge	Uncertainty in the business environment	81	81.0%
Effect of organizational complexity	Makes risks harder to identify/manage	85	85.0%
AI for risk identification	Analyses large amounts of data	86	86.0%
Real-time risk monitoring technology	Artificial intelligence	86	86.0%
Purpose of proactive risk management	Identify/address risks before they occur	85	85.0%
Predictive risk management	Anticipates potential future risks	88	88.0%
Climate-change impact	Operational and financial risks	91	91.0%

Cybersecurity-related risk	Data breaches and information loss	87	87.0%
Purpose of ERM	Manage risks across the organization	80	80.0%
ERM response to changing risks	Integrated risk-management approach	81	81.0%

Interpretation: The highest correct-response rate was for “Climate-change impact” (91.0%), while the lowest was for “Purpose of ERM” (80.0%). All ten questions had a majority selecting the designated correct answer, with rates ranging from 80.0% to 91.0%.

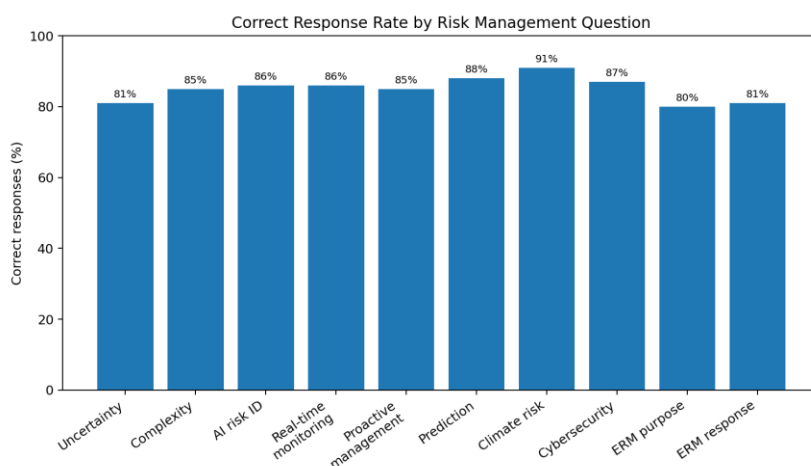


Figure 4. Correct-response rate by risk-management question.

8.3 Overall Knowledge Score

Correct answers (out of 10)	Respondents	Percentage
5	3	3.0%
6	3	3.0%
7	16	16.0%
8	17	17.0%
9	41	41.0%
10	20	20.0%

Measure	Result
Number of respondents	100
Questions per respondent	10
Total answer opportunities	1000
Total correct answers	850
Overall correct-answer rate	85.0%
Mean score (out of 10)	8.50
Median score	9
Standard deviation	1.24

Interpretation: Across all responses, the overall correct-answer rate was 85.0%. The mean respondent score was 8.50/10 (median 9; SD 1.24). This is a descriptive measure of performance on this particular ten-question questionnaire; it should not be interpreted as a validated scale of risk-management competence.

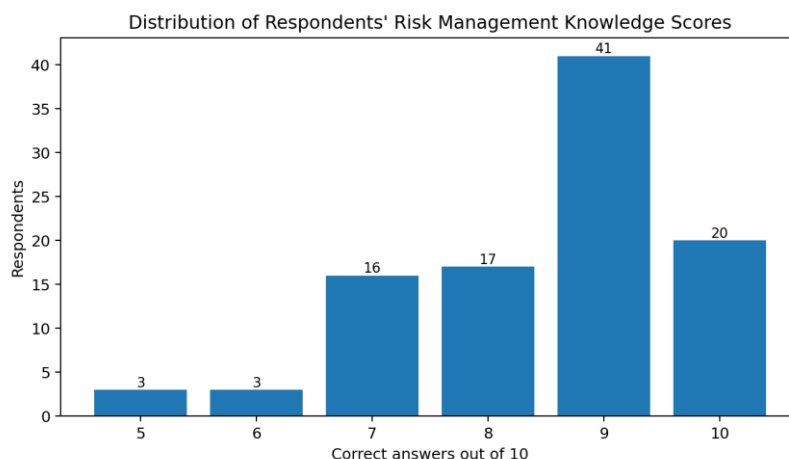


Figure 5. Distribution of total knowledge scores.

8.4 Thematic Interpretation

81.0% said that uncertainty in the business environment is a big challenge.

This shows that most people know risk-management processes are often uncertain.

Eighty-five percent knew risks are tougher to spot and handle when systems are complicated; eighty-six percent pointed to large-scale data analysis.

Keeping an eye on things and stopping problems before they start. 86.0% of people said AI could help keep an eye on risks as they happen, and 85.0% know that preventative risk management is all about stopping risks before they start.

Expecting something might go wrong. 88.0% said that predicting future risks is the main job of risk management.

Climate and cybersecurity. 91.0% recognized climate change as an operational and financial risk, while 87.0% saw data breaches and lost information as cybersecurity risks.

Enterprise resource planning. 80.0% said organizations use ERM to handle risks throughout the whole business, and 81.0% said an integrated ERM approach helps organizations deal with changing risks.

9. Major Findings

The dataset has a hundred respondents, and each one answered ten questions about risk management.

Out of 1000 tries, 85% of the answers were right, and the average score was 8.5 out of 10.

The toughest set of questions was about climate-change impact, with 91.0% answered correctly.

The purpose of erm had the lowest correct percentage at 80.0%. We might need to talk more about this or provide extra training.

No one identified any financial or operational risks from climate change.

No one said that data breaches and information loss are a top cybersecurity risk.

Nobody said that ERM covers the whole organization instead of just one type of risk.

The questionnaire looks at the decisions made about knowledge instead of focusing on how organizations handle resilience, preparedness, recovery, and adaptation.

10. Suggestions and Practical Implications

Give short training sessions on risk identification, assessment, prioritization, and response, using real examples from organizations.

Show how reactive, proactive, and predictive risk management are different, and talk about the limits of forecasts, since data is always a bit flawed.

Create a single risk register that covers strategic, operational, financial, climate, cyber, compliance, and supply-chain risks.

Use technology and real-time monitoring to help make decisions, making sure accountability is clear and that people review any alerts or recommendations.

Boost your cyber resilience by using access controls, backup routines, response plans, training for staff, and practicing recovery drills.

Think about how climate change could affect your business, like your buildings, transportation, suppliers, insurance, and expenses, and make sure to include these in your continuity plan.

Create and test plans for keeping things running and bouncing back—figure out what services matter most, who your backup suppliers are, how you'll communicate, and which people are crucial.

In a brainstorming session, go over incidents and near misses that have happened, write down what you learned, and update your controls and response plans.

Give the questionnaire again after training and look at the average combined knowledge scores, but make sure to note that you'll need a better-validated tool before using this for research.

In future studies, collect information about how long recovery takes, whether the continuity plan gets tested, leadership support, adaptability, and getting services up and running again.

11. Conclusion

This Excel dataset from the study showed how well the respondents understood risk management and resilience ideas . On average, respondents answered 85% of the questions correctly and scored 8.5 out of 10 on the multiple choice test. The responses show people understand uncertainty, tech-based risk spotting, looking ahead and predicting risks, climate risk, cybersecurity, and managing

You need to look at the results with the dataset in mind . The workbook doesn't mention how sampling was done, and it doesn't include any direct data on resilient organizations or business performance. The analysis can't tell if knowing about resilient organizations has a positive impact, and it also can't look at cause-and-effect relationships. A stronger future study should use a clear sampling method, along with proven ways to measure preparedness, adaptation, continuity, and recovery.

12. Limitations and Scope for Future Research

There are 100 records in the data, but it doesn't say how people were recruited or what group was sampled.

The questionnaire has ten multiple choice questions, but it doesn't show how much the respondents really know.

In this case, the study design's answer key is used to decide what's correct, and the way the questions and answer choices are worded can influence the results.

The data doesn't cover resilience, how mature the risk management is, readiness, response time, or operational results.

Future studies should use a better, clearly defined sample, stick to clear age groups, rely on proven measurement tools, follow proper ethics, and gather both numbers and stories for their data.

13. REFERENCES

- Committee of Sponsoring Organizations of the Treadway Commission, 2017. Enterprise Risk Management—How It Fits with Strategy and Performance COSO stands for Committee of Sponsoring Organizations of the Treadway Commission.
- International Organization for Standardization. (2018). ISO 31000:2018 Risk management—Guidelines. Looking for it.
- UN Office for Disaster Risk Reduction (UNDRR).(2015). Sendai Framework for Disaster Risk Reduction, 2015 to 2030. United Nations Organization.
- Hopkin, P., 2018. Fundamentals of Risk Management: What It Is, How to Assess It, and How to Put Good Risk Management in Place (5th edition). Kogan Page.