Risk Matrices

2

There is no doubt that risk management is an important and growing area in the uncertain world. Chapter 1 discussed a number of recent events where events made doing business highly challenging. Globalization offers many opportunities, but it also means less control, operating in a wider world where the actions of others intersect with our own. This chapter looks at enterprise risk management process, focusing on means to assess risks.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an accounting organization concerned with enterprise risk management (ERM). They define ERM as a process designed to identify potential events that may affect the organization, and manage risk to be within that organization's risk appetite in order to provide reasonable assurance of accomplishing the organization's objectives.[1] Risk identification and mitigation are a key component of an organization's ERM program. Table 2.1 outlines this risk framework:

This table is compatible with the overall risk management framework we gave in Chap. 1:

- Risk identification
- Risk assessment and evaluation
- Selection of risk management strategy
- Implementation
- Risk monitoring/mitigation

Risk Management Process

An important step is to **set the risk appetite** for the organization. No organization can avoid risk. Nor should they insure against every risk. Organizations exist to take on risks in areas where they have developed the capability to cope with risk. However, they cannot cope with every risk, so top management needs to identify

D.L. Olson, D.D. Wu, *Enterprise Risk Management Models*, Springer Texts in Business and Economics, DOI 10.1007/978-3-662-53785-5_2

Table 2.1 COSO risk management framework

Concept	Elaboration
Mission, strategy, objectives	What are the organization's mission, strategy, and objectives?
Risks	What are the significant risks?
Risk appetite	What is the organization willing to tolerate?
Likelihood	What is the likelihood of the risk occurring? (How can you measure?)
Impacts	What is the potential impact of the risk?
Risk mitigation	What are available defense strategies?
Residual risk	What is the risk remaining (beyond control)?
Risk response and effectiveness	How effectively does the organization manage its individual risks?
Risk maturity	How robust is the current ERM program?

the risks they expect to face, and to identify those risks that they are willing to assume (and profit from successfully coping).

The **risk identification** process needs to consider risks of all kinds. Typically, organizations can expect to encounter risks of the following types:

- Strategic risk
- Operations risk
- Legal risk
- Credit risk
- Market risk

Examples of these risks are outlined in Table 2.2:

Each manager should be responsible for ongoing risk identification and control within their area of responsibility. Once risks are identified, a risk matrix can be developed. Risk matrices will be explained in the next section. The **risk management** process is the control aspect of those risks that are identified. The adequacy of this process depends on assigning appropriate responsibilities by role for **implementation**. Effectiveness can be monitored by a risk-screening committee at a high level within the organization that monitors new significant markets and products. The **risk review** process includes a systematic internal audit, often outsourced to third party providers responsible for ensuring that the enterprise risk management structure functions as designed. One tool to aid in risk assessment and evaluation is a risk matrix.

Risk Matrices

A risk matrix provides a two-dimensional (or higher) picture of risk, either for firm departments, products, projects, or other items of interest. It is intended to provide a means to better estimate the probability of success or failure, and identify those

Table 2.2 Enterprise risk management framework

Strategic risks	Is there a formal process to identify potential changes in markets, economic conditions, regulations, and demographic change impacts on the business? Is new product innovation considered for both short-run and long-run impact? Does the firm's product line cover the customer's entire financial services experience? Is research & development investment adequate to keep up with competitor product development? Are sufficient controls in place to satisfy regulatory audits and their impact on stock price?
Operations risks	Does the firm train and encourage use of rational decision-making models? Is there a master list of vendor relationships, with assurance each provides value? Is there adequate segregation of duties? Are there adequate cash and marketable securities controls? Are financial models documented and tested? Is there a documented strategic plan to technology expenditures?
Legal risks	Are patent requirements audited to avoid competitor abuse as well as litigation? Is there an inventory of legal agreements and auditing of compliance? Do legal agreements include protection of customer privacy? Are there disturbing litigation patterns? Is action taken to assure product quality sufficient to avoid class action suits and loss of reputation?
Credit risks	Are key statistics monitoring credit trends sufficient? How are settlement risks managed? Is their sufficient collateral to avoid deterioration of value? Is the incentive compensation program adequately rewarding loan portfolio profitability rather than volume? Is exposure to foreign entities monitored, as well as domestic entity exposure to foreign entities?
Market risks	Is there a documented funding plan for outstanding lines? Are asset/liability management model assumptions analyzed? Is there a contingency funding plan for extreme events? Are core deposits analyzed for price and cash flow?

activities that would call for greater control. One example might be for product lines, as shown in Table 2.3.

The risk matrix is meant to be a tool revealing the distribution of risk across a firm's portfolio of products, projects, or activities, and assigning responsibilities or mitigation activities. In Table 2.3, hedging activities might include paying for insurance, or in the case of investments, using short-sale activities. Internal controls would call for extra managerial effort to quickly identify adverse events, and take action (at some cost) to provide greater assurance of acceptable outcomes. Risk matrices can represent continuous scales. For instance, a risk matrix focusing on product innovation was presented by Day.[2] Many organizations need to have an ongoing portfolio of products. The more experience the firm has in a particular product type, the greater the probability of product success. Similarly, the more experience the firm has in the product's intended market, the greater the probability of product success. By obtaining measures based on expert product manager

Table 2.3 Product risk matrix

	Likelihood of risk low	Likelihood of risk medium	Likelihood or risk high
Level of risk high	Hedge	Avoid	Avoid
Level of risk medium	Control internally	Hedge	Hedge
Level of risk low	Accept	Control internally	Control internally

Table 2.4 Product/technology risk assessment

	1- Fully experienced	2-	3- Significant change	4-	5- No experience	Score
Current development capability			X			3
Technological competency		X				2
Intellectual property protection				X		4
Manufacturing & service delivery system	X					1
Required knowledge			X			3
Necessary service		X				2
Expected quality			X			3
Total						18

Table 2.5 Product/technology failure risk assessment

	1- Same as present	2-	3- Significant change	4-	5- Completely different	Score
Customer behavior				X		4
Distribution & sales			X			3
Competition					X	5
Brand promise					X	5
Current customer relationships					X	5
Knowledge of competitor behavior				X		4
Total						26

evaluation of both scales, historical data can be used to calibrate prediction of product success. Scaled measures for product/technology risk could be based on expert product manager evaluations as demonstrated in Table 2.4 for a proposed product, with higher scores associated with less attractive risk positions:

Table 2.5 demonstrates the development of risk assessment of the intended market.

Table 2.6 Innovation product risk matrix—expert success probability assessments

	Failure <10	Failure 10–15	Failure 15–20	Failure 20–25	Failure 25–30
Technology 30–35	0.50	0.40	0.30	0.15	0.01
Technology 25–30	0.65	0.50	0.45	0.30	0.05
Technology 20–25	0.75	0.60	0.55	0.45	0.20
Technology 15–20	0.80	0.70	0.65	0.55	**0.30**
Technology 10–15	0.90	0.85	0.80	0.65	0.45
Technology <10	0.95	0.90	0.85	0.70	0.60

Table 2.6 combines these scales, with risk assessment probabilities that should be developed by expert product managers based on historical data to the degree possible.

In Table 2.5, the combination of technology risk score of 18 with product failure risk score 26 is in bold, indicating a risk probability assessment of 0.30.

Color Matrices

Risk matrices have been applied in many contexts. McIlwain[3] cited the application of clinical risk management in the United Kingdom arising from the National Health Service Litigation Authority creation in April 1995. This triggered systematic analysis of incident reporting on a frequency/severity grid comparing likelihood and consequence. Traffic light colors are often used to categorize risks into three (or more) categories, quickly identifying combinations of frequency and consequence calling for the greatest attention. Table 2.7 demonstrates the use of a risk matrix that could be based on historical data, with green assigned to a proportion of cases with serious incident rates below some threshold (say 0.01), red for high proportions (say 0.10 or greater), and amber in between.

While risk matrices have proven useful, they can be misused as can any tool. Cox[4] provided a critique of some of the many risk matrices in use. Positive examples were shown from the Federal Highway Administration for civil engineering administration (Table 2.8), and the Federal Aviation Administration applied to airport operation safety.

The Federal Aviation Administration risk matrix was quite similar, but used qualitative terms for the likelihood categories (frequent, probable, remote, extremely remote, and extremely improbable) and severity categories (no safety effect, minor, major, hazardous, and catastrophic). Cox identified some characteristics that should be present in risk matrices:

Table 2.7 Risk matrix of medical events

	Consequence insignificant	Consequence minor	Consequence moderate	Consequence major	Consequence catastrophic
Likelihood almost certain	Amber	Red	Red	Red	Red
Likelihood likely	Green	Amber	Red	Red	Red
Likelihood possible	Green	Amber	Amber	Amber	Red
Likelihood unlikely	Green	Green	Amber	Amber	Red
Likelihood rare	Green	Green	Green	Amber	Amber

Table 2.8 Risk matrix for Federal Highway Administration (2006)

	Very low impact	Low impact	Medium impact	High impact	Very high impact
Very high probability	Green	Yellow	Red	Red	Red
High probability	Green	Yellow	Red	Red	Red
Medium probability	Green	Green	Yellow	Red	Red
Low probability	Green	Green	Yellow	Red	Red
Very low probability	Green	Green	Green	Yellow	Red

Extracted from Cox (2008)

1. Under weak consistency conditions, no red cell should share an edge with a green cell
2. No red cell can occur in the left column or in the bottom row
3. There must be at least three colors
4. Too many colors give spurious resolution

Cox argued that risk ratings do not necessarily support good resource allocation decisions. This is due to the inherently subjective categorization of uncertain consequences. Thus Cox argues that theoretical results he presented demonstrate that quantitative and semi-quantitative risk matrices (using numbers instead of categories) cannot correctly reproduce risk ratings, especially if frequency and severity are negatively correlated. Levine suggested that scales in risk matrices are often more appropriately logarithmically scaled rather than linear.[5]

Quantitative Risk Assessment

It would be ideal to go deeper than risk matrices allow, to be able to identify costs and benefits of risk actions. Risk matrices are simple and useful tools because most of the time, detailed cost and probability data is not available. However, if such data is available, more accurate risk assessment is possible.[6]

Risk can be characterized by the attributes of threat, vulnerability, and consequence, each of which can be expressed in terms of probability. Each of these is uncertain, and in fact these three aspects of risk may be correlated. A normative argument is that if these measures are important but are not known, the organization should invest in obtaining them. Levine demonstrated risk management of computer network security with an example comparing different types of attack in terms of frequency, consequence, and risk. Table 2.9 provides hypothetical data:

In Table 2.9, Risk is defined as the product of frequency and consequence, a common approach. The risk matrix in this case can overlay treatments with cells, as in Table 2.10.

In this case the most attention would be given to identity theft. The others either are relatively low consequence (web vandalism) or relatively low frequency (cyber espionage, denial of service). Looking at the quantitative scale of risk, a bit different outcome is obtained, with cyber espionage and identity theft both being very high, closely followed by denial of service. Web vandalism is lower on this scale. Generally, moving to a more quantitative metric is preferable, with the tradeoff of requiring more data with accuracy an important factor.

To demonstrate, assume the context of a construction firm with a portfolio of ten jobs, involving some risk to worker safety. The firm has a safety program that can be applied to reduce some of these risks to varying degrees on each job. Cox addressed four different levels of risk evaluation, depending upon the level of

Table 2.9 Hypothetical computer network security data

Attack type	Label	Frequency	Consequence	Risk
Cyber espionage	CE	10^2 per year	$\$10^7$ per event	$\$10^9$ per year
Denial of service	DS	10^2 per year	$\$10^6$ per event	$\$10^8$ per year
Identity theft	IT	10^4 per year	$\$10^5$ per event	$\$10^9$ per year
Web vandalism	WV	10^3 per year	$\$10^2$ per event	$\$10^5$ per year

Table 2.10 Risk matrix for computer network security

	Consequence $<\$10^3$/event	Consequence $\$10^3$–$\leq\$10^5$/event	Consequence $\geq\$10^6$/event
Frequency $>10^3$ per year	Green	Amber **IT**	Red
Frequency $>10^2$–10^3 per year	Green **WV**	Amber	Amber
Frequency $\leq 10^2$ per year	Green	Green	Green **CE DS**

Table 2.11 Hypothetical construction data

Job	Liability risk (k$)	Prob {injury} (frequency)	Expected loss (risk)	Reducible	Savings (k$)	Cost of reducing	RRPUC
1	250	0.30	75.0	0.7	52.50	25	2.100
2	300	0.20	60.0	0.5	30.00	20	1.500
3	320	0.15	48.0	0.6	28.80	25	1.152
4	340	0.20	68.0	0.3	20.40	15	1.360
5	370	0.11	40.7	0.5	20.35	20	1.018
6	410	0.18	73.8	0.6	44.28	25	1.771
7	440	0.33	145.2	0.4	58.08	20	2.904
8	460	0.25	115.0	0.7	80.50	30	2.683
9	480	0.20	96.0	0.5	48.00	20	2.400
10	530	0.08	42.4	0.4	16.96	18	0.942

Table 2.12 Hypothetical risk matrix

	Liability risk low	Liability risk medium	Liability risk high
Prob{injury} high	Assign safety	Assign safety	Subcontract
Prob{injury} medium	Insurance only	Assign safety	Assign safety
Prob{injury} low	Insurance only	Insurance only	Assign safety

data available. The risk matrices that we have been looking at require little quantitative data, although as we have demonstrated in Table 2.6, they are more convincing if they are based on quantitative input. Table 2.11 provides full raw data for the ten construction jobs:

In Table 2.11, column 2 is the potential liability due to injury in thousands of dollars. Column 3 is the probability of an injury if no special safety improvement is undertaken. Column 4 is the product of column 2 and column 3, the expected loss without action. Column 5 is the proportion of the injury probability that can be reduced by proposed action, which leads to savings in column 6 (the product of column 4 and column 5). Column 7 is the amount of budget that would be needed to reduce risk. Column 8 (RRPUC) is risk reduction per unit cost.

Table 2.12 gives the risk matrix in categorical terms, using the dimensions of probability of injury {below 0.19; 0.20–0.25; 0.26 and above) and liability risk {below 399; 400–599; 600 and above).

For each combination of injury probability and liability risk has a mitigation strategy assigned. Insurance is obtained in all cases (even for subcontracting). Assigning extra safety personnel costs additional expense. Subcontracting sacrifices quite a bit of expected profit, and thus is to be avoided except in extreme cases. This table demonstrates what Cox expressed as a limitation in that while the risk matrix is quick and easy, it is a simplification that can be improved upon. Cox suggested three indices, each requiring additional accurate inputs.

Table 2.13 Ranking by index

Risk index ranking	Budget (k$)	Risk reduction index ranking	Budget (k$)	RRPUC ranking	Budget (k$)
Job 7	20	Job 8	30	Job 7	20
Job 8	30	Job 7	20	Job 8	30
Job 9	20	Job 1	25	Job 9	20
Job 1	25	Job 9	20	Job 1	25
Job 6	25	Job 6	25	Job 6	25
Job 4	15	Job 2	20	Job 2	20
Job 2	20	Job 3	25	Job 4	15
Job 3	25	Job 4	15	Job 3	25
Job 10	18	Job 5	20	Job 5	20
Job 5	20	Job 10	18	Job 10	18

Table 2.14 Risk reductions achieved by index

Budget	Risk index	Risk reduction index	RRPUC
$100k	247.936	247.936	247.936
$150k	326.260	324.880	326.961

The first index is to use risk (the expected loss column in Table 2.11), the second risk reduction (savings column in Table 2.11), the third the risk reduction per unit cost (RRPUC column in Table 2.11). These would yield different rankings of which jobs should receive the greatest attention. In all three cases, the contention is that there is a risk reduction budget available to be applied, starting with the top-ranked job and adding jobs until the budget is exhausted. Table 2.13 shows rankings and budget required by job.

If there were a budget of $100k, using the risk ranking jobs 7, 8, 9, and 1 would be given extra safety effort, as well as a 20 % effort on job 6. With the risk reduction index as well as the RRPUC index, a different order of selection would be applied, here yielding the same set of jobs. For a budget of $150k, the risk index would provide full treatment to job 6, add job 4, and 75 % of job 2. The risk reduction index would also provide full treatment to job 6, add job 2, and provide 40 % coverage to job 3. The RRPUC index also would again provide full treatment to job 6, add job 2, and 2/3rds coverage to job 4. The idea of all three indices is much the same, but with more information provided. Table 2.14 shows the expected gains from these two budget levels for each index:

Given a budget of $100k, the risk index would reduce expected losses by $58.08k on job 7, $80.50k on job 8, $48k on job 9, $52.50k on job 1, and $8.856k on job 6, for total risk reduction of $247.936k. As we saw, this was the same for all three indices. But there is a difference given a budget of $150k. Here the risk index actually comes out a bit higher than the risk reduction index, but Cox has run simulations showing that risk reduction should provide a bit better performance. The RRPUC has to be at least as good as the other two, as its basis is the

sorting key. The primary point is that there are ways to incorporate more complete information into risk management. The tradeoff is between the availability of information and accuracy of output.

Strategy/Risk Matrix

Risk matrices can be applied to capture the essence of tradeoffs in risk and other measures of value. In this case, we apply a risk matrix to a construction industry study where the original authors applied an analytic hierarchy model.[7] The model is relatively straightforward. The construction context included a number of types of work, each with a relative rating of supply risk along with a similar weighting of strategic impact. Data is given in Table 2.15:

Figure 2.1 displays a scatter diagram of this data:

Table 2.15 Construction work risk and impact

Type	Supply risk	Strategic impact
Cement	0.05	0.34
Workforce	0.09	0.40
Aggregate	0.11	0.58
Transport	0.12	0.18
Demolition	0.12	0.38
Painting	0.15	0.25
Misc	0.15	0.28
Steel	0.15	0.65
Insulation	0.16	0.18
Travel	0.17	0.29
Cast iron	0.18	0.23
Excavation	0.20	0.26
Locksmith	0.21	0.36
Floor cover	0.22	0.23
Infrastructure	0.23	0.58
Sanitary	0.23	0.70
Ceilings	0.25	0.24
Geotechnical	0.25	0.29
Electrical	0.25	0.57
Climate	0.26	0.34
Aluminum	0.31	0.24
Formwork	0.31	0.31
Concrete	0.46	0.92
Mosaic	0.51	0.26
Carpentry	0.54	0.24
Special forming	0.56	0.31
Stone	0.59	0.24
Scaffolding	0.62	0.29

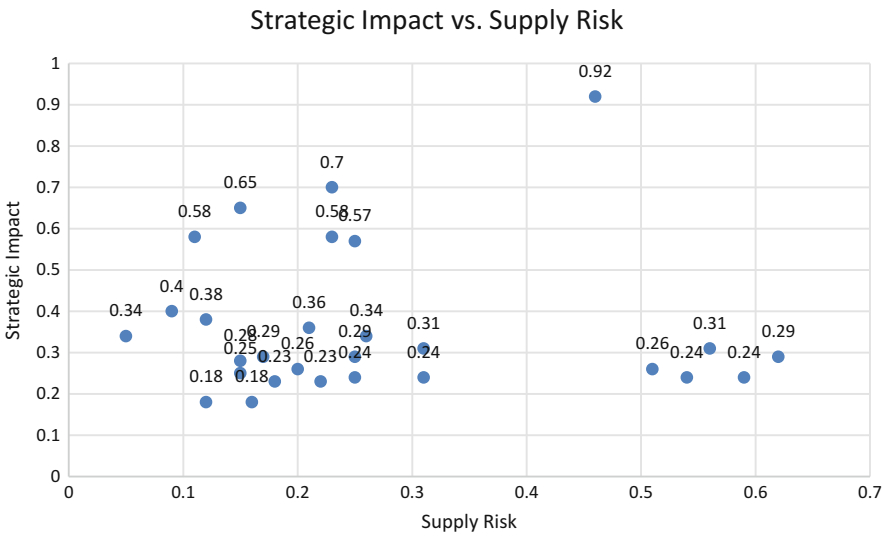

Fig. 2.1 Strategic impact plotted against supply risk

Table 2.16 Risk matrix of risk/strategic impact tradeoff

	Supply risk ≤0.2	Supply risk >0.2– ≤ 0.5	Supply risk >0.5– ≤ 0.8	Supply risk >0.8
Strategic impact >0.8	Add risk control	Outsource	Outsource	Outsource
Strategic impact >0.5– ≤ 0.8	Add risk control	Add risk control	Outsource	Outsource
Strategic impact >0.2– ≤ 0.5	Normal operation	Normal operation	Add risk control	Outsource
Strategic impact ≤0.2	Normal operation	Normal operation	Normal operation	Add risk control

Construction contexts could differ widely, but we will assume an operation where the greatest profit is expected from conducting operations normally. Risk can be reduced by spending extra money in the form of added inspection and safety supervisors, but this would eat into profit. The least profit would be expected from an option to outsource construction, placing the risk on subcontractors. The criteria can be sorted in a risk matrix considering both dimensions, as in Table 2.16:

In this case, this policy would result in outsourcing (subcontracting) concrete work, which has a supply risk rating of 0.46 and a very high strategic impact of 0.92. Added risk control would be adopted for ten other types of work: aggregate, steel, infrastructure, sanitary, electrical, mosaic, carpentry, special forming and scaffolding, and stone.

Conclusions

The study of risk management has grown in the last decade in response to serious incidences threatening trust in business operations. The field is evolving, but the first step is generally considered to be application of a systematic process, beginning with consideration of the organization's risk appetite. Then risks facing the organization need to be identified, controls generated, and review of the risk management process along with historical documentation and records for improvement of the process.

Risk matrices are a means to consider the risk components of threat severity and probability. They have been used in a number of contexts, basic applications of which were reviewed. Cox and Levine provide useful critiques of the use of risk matrices. That same author also suggested more accurate quantitative analytic tools. An ideal approach would be to expend such measurement funds only if they enable reducing overall cost. The interesting aspect is that we don't really know. Thus we would argue that if you have accurate data (and it is usually worth measuring whatever you can), you should get as close to this ideal as you can. Risk matrices provide valuable initial tools when high levels of uncertainty are present. Quantitative risk assessment in the form of indices as demonstrated would be preferred if data to support it is available.

Notes

1. Prasad, S.B. (2011) A matrixed assessment. *Internal Auditor* 68(6), 63–64.
2. Day, G.S. (2007). Is it real? Can we win? Is it worth doing? Managing risk and reward in an innovation portfolio, *Harvard Business Review* 85:12, 110–120.
3. McIlwain, J.C. (2006). A review: A decade of clinical risk management and risk tools, *Clinician in Management* 14:4, 189–199.
4. Cox, L.A. Jr. (2008). What's wrong with risk matrices? *Risk Analysis* 28:2, 497–512.
5. Levine, E.S. (2012). Improving risk matrices: The advantages of logarithmically scaled axes. *Journal of Risk Research* 15(2), 209–222.
6. Cox, L.A., Jr. (2012). Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities. *Risk Analysis* 32(7), 1244–1252.
7. Ferreira, L.M.D.F., Arantes, A. and Kharlamov, A.A. (2015). Development of a purchasing portfolio model for the construct6ion industry: An empirical study. *Production Planning & Control* 26(5), 377–392.