International Journal of Production Research
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713696255

Analysing risks in supply networks to facilitate outsourcing decisions

Archie Lockamy III [a];Kevin McCormack [b]
[a] Brock School of Business, Samford University, Birmingham, Alabama, USA [b] College of Management, North Carolina State University, Raleigh, North Carolina, USA

Online publication date: 10 December 2009

To cite this Article Lockamy III, Archie andMcCormack, Kevin(2010) 'Analysing risks in supply networks to facilitate outsourcing decisions', International Journal of Production Research, 48: 2, 593 — 611

To link to this Article: DOI: 10.1080/00207540903175152

URL: http://dx.doi.org/10.1080/00207540903175152

International Journal of Production Research
Vol. 48, No. 2, 15 January 2010, 593–611

Analysing risks in supply networks to facilitate outsourcing decisions

Archie Lockamy III[a]* and Kevin McCormack[b]

[a]*Brock School of Business, Samford University, Birmingham, Alabama, USA;*
[b]*College of Management, North Carolina State University, Raleigh, North Carolina, USA*

(*Revision received July 2009*)

In an effort to achieve a competitive advantage via cost reductions and improved market responsiveness, organisations are increasingly employing outsourcing as a major component of their supply chain strategies. However, as organisations increase their dependence on the suppliers of outsourced raw materials and components, they become more susceptible to their risk profiles. Supplier risk profiles are comprised of risk events which are associated with the supply network, internal operations, or external factors. Suppliers with a high probability of risk event occurrences can have a substantial impact on an organisation's revenue stream. Thus, it is essential that organisations have the means to analyse the risks associated with a supplier of outsourced materials. This article presents a methodology for analysing risks in supply networks to facilitate outsourcing decisions. The methodology includes the development of a risk profile for a given supplier through the creation of Bayesian networks. The networks are used to analyse a supplier's external, operational and network risk probabilities, and the associated revenue impact on the organisation. The methodology can be used by supply chain professionals to facilitate outsourcing decisions with either current or prospective suppliers.

Keywords: outsourcing; supply networks; supply chain risks; risk events; Bayesian networks

1. Introduction

Increased intensity in the management of global supply networks has resulted in the adoption of outsourcing strategies by a growing number of organisations. The anticipated benefits of outsourcing are to improve profitability and operating efficiency (Gonzalez *et al*. 2005), reduce capital investment (Lynch 2004), improve business focus (Baldwin *et al*. 2001, Weerakkody *et al*. 2003), enhance flexibility (Jennings 2002, Lynch 2004), and to gain a competitive advantage (Clott 2004). However, as an organisation's dependency on outsourced materials increases, it becomes more susceptible to the risk profiles associated with their suppliers. Supplier risk profiles are comprised of risk events which are associated with the supply network, internal operations, or external factors. Suppliers with a high probability of risk event occurrences can have a substantial impact on an organisation's ability to generate revenue. Therefore, it is crucial that organisations have the capability to analyse the risks associated with a supplier of outsourced materials.

*Corresponding author. Email: aalockam@samford.edu

ISSN 0020–7543 print/ISSN 1366–588X online

DOI: 10.1080/00207540903175152
http://www.informaworld.com

1.1 *Purpose*

The purpose of this article is to present a methodology for analysing risks in supply networks to facilitate outsourcing decisions. The methodology employs the use of Bayesian networks for creating risk profiles of individual suppliers. The networks are used to analyse a supplier's external, operational and network risk probabilities, and the associated revenue impact on the organisation. This methodology can be adopted by supply chain managers to evaluate the level of risk associated with either current or prospective suppliers, and to assist them in making outsourcing decisions.

1.2 *Organisation*

The paper is organised as follows. The first section provided the motivation for and purpose of the paper. A discussion of supply chain management, outsourcing and supply chain risks is provided in Section 2. Section 3 contains a description of the research methodology used in this study. Section 4 contains the results of the research. Proposed managerial actions based upon the results of the study are provided in Section 5. Finally, conclusions and implications regarding study limitations and directions for future research are presented in Section 6.

2. Supply chain management

A growing number of firms are adopting supply chain management (SCM) to improve competitiveness (Singh *et al*. 2005, Li *et al*. 2006, Gunasekaran *et al*. 2008). SCM can be characterised as a philosophy based upon the belief that each firm in the supply chain directly and indirectly affects the performance of all the other supply chain members, as well as ultimately, overall supply chain performance (Cooper *et al*. 1997). The effective use of this philosophy requires that functional and supply chain partner activities are aligned with company strategy and are congruent with organisational structure, processes, culture, incentives and people (Abell 1999). Additionally, the chain-wide deployment of SCM practices consistent with the above-mentioned philosophy is needed to accrue maximum benefits to its members.

In order to realise the potential benefits of supply chain management, organisations are required to make fundamental changes to their business focus (Kopczak and Johnson 2003). These changes include an emphasis on cross-functional and cross-enterprise integration (Chen and Kang 2007); the effective management of the flow of physical goods through suppliers, manufacturers, distributors and retailers for increased value to end customers (Jammernegg and Reiner 2007); and the ability to acquire and manage reliable demand information (Croxton *et al*. 2002). In addition, outsourcing has increasingly become a key component of the SCM strategy for many firms. Factors leading firms towards the adoption of outsourcing include the potential for reductions in cost and capital investment, enhanced flexibility, and the ability to focus primarily on the firm's core competences (Lau and Zhang 2006).

2.1 *Outsourcing*

Outsourcing, generally defined as the shifting of work done 'in-house' to another company, is thought of as a key strategy for improving cost and competitiveness

(Kremic *et al*. 2006). The outsourcing of logistics, IT and production has shifted the role of many companies from a producer of goods to a coordinator of the industry value chain (Choy and Lee 2003). This increase in supplier dependence has highlighted the need to enhance the approaches to supplier management. Effective supplier selection, innovative supplier development and meaningful supplier performance assessment have become key competencies needed for success (Kannan and Tan 2002).

During the last decade, several events that impacted outsourced supply networks (i.e., earthquake in Kobe, Japan in 1995; terrorist attack on the World Trade Center in 2001; Severe Acute Respiratory Syndrome (SARS) in 2002–2003) have significantly disrupted supply chains and produced major losses for the lead companies involved (Tang 2006). Companies such as Ericcson, Hershey, Apple, Wal-Mart, and a host of other major companies who rely on timely delivery of products and services from outsourcing to meet customer needs have incurred major losses due to supply chain disruptions. Publicly traded firms experiencing supply chain disruptions, for example, have reported negative stock market reactions to announcements of such disruptive events, with the magnitude of the decline in market capitalisation being as large as 10% (Knight and Pretty 1996, Hendricks and Singhal 2005). For example, Ericsson reported a $400 million loss because it did not receive computer chip deliveries from a Philips plant in a timely manner (Latour 2001).

Although the true costs of any supply chain disruption can be difficult to quantify precisely, at least one firm surveyed by Rice and Caniato (2003) estimated that the daily cost impact of a disruption in its supply network to be in the neighbourhood of $50–$100 million. These recent events have highlighted the need to add supply risk management to the list of core competencies needed to manage an outsourced supply network.

2.2 *Supply chain risks*

The risk of disruptions caused both from factors within supply chains (SCs) and from outside environmental forces is of main concern to both practitioners and researchers. Supply chain risk management (SCRM) is therefore a field of growing importance and is aimed at developing approaches for the identification, assessment, analysis and treatment of areas of vulnerability and risk in supply chains (Neiger *et al*. 2009). Various trends that increase exposure to risks, such as the increased use of outsourcing, globalisation, supplier base reductions, reduced inventory buffers, increased demand for on-time deliveries and shorter product life cycles (Norrman and Jansson 2004) are elevating the importance of SCRM. This is highlighted by several practical examples of the high costs of improper preparation and response to various supply chain risk events cited by Chopra and Sodhi (2004).

Currently, SCRM approaches are attempting to measure either supplier attributes or supply chain structures to compare suppliers and predict disruptions. The results are then used to prepare proper mitigation and response strategies associated with these suppliers. Most often SCRM is a formal process that involves identifying potential losses, understanding the likelihood of potential losses, and assigning significance to these losses (Giunipero and Eltantawy 2004). A typical example of such an approach is the PRAM (Procurement Risk Assessment and Mitigation) methodology, developed by the Dow Chemical Company to measure SC risk and its impact. This approach examines the following factors of a supply chain: supply market risk, supplier risk, organisation risk, and supply strategy risk (Hackett Group 2007).

Due to the relative newness of the SCRM field, it is currently chaotic and somewhat disorganised. Currently, there are several different classifications for risks, along with assorted risk methodologies found in the literature. Often, only the disruptive events (such as bankruptcy, natural disaster or the possibility of the terrorist attack) are included in the classification schemes, while the softer factors between suppliers and customers (i.e., relationships, influence, leverage, information sharing, and cooperation) are ignored.

Risk is a concept that has applications in everything we do. It has several components, not the least of which is the lack of knowledge about the events that may impact us and our ability to manage them. In order to understand risk we first need to define and decompose it, specifically as it pertains to the supply chain.

Risk in general can be defined as a collection of pairs of *likelihood* (L) and *outcomes* (O):

$$Risk = \{(L_1, O_1), (L_2, O_2), \ldots, (L_n, O_n)\},$$

where O_i and L_i denote outcome i and its related likelihood. The distribution pattern of likelihood and outcome pairs is called a *risk profile* (Ayyub 2003). Definitions of risk must also have a *time dimension* or a specific time horizon (i.e., day, month, year, etc.) and a specific *perspective* or view that defines the unit of analysis (i.e., boundaries, etc.).

The International Organization for Standardization (ISO 2002) defines two of the essential components of risk: *losses* (along with related amounts) and *uncertainty* of their occurrence.

The research literature provides a number of approaches for defining risk in supply networks. For example, supply chain risk can be divided, according to its source, in the following manner: demand-side risks resulting from disruptions emerging from downstream supply chain operations (Suttner 2005); supply-side risks residing in purchasing, supplier activities, and supplier relationships; and catastrophic risks that, when they materialise, have a severe impact in terms of magnitude in the area of their occurrence (Wagner and Bode 2006). Additionally, Treleven and Schweikhart (1988) have classified risks into five categories, connected with disruption, price, inventories and schedule, technology, and quality.

Zsidisin *et al.* (2005) defines supply risk as the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety. Wu *et al.* (2006) states that inbound supply risk is defined as the potential occurrence of an incident associated with inbound supply from individual supplier failures or the supply market, resulting in the inability of the purchasing firm to meet customer demand and as involving the potential occurrence of events associated with inbound supply that can have significant detrimental effects on the purchasing firm. Finally, Nagurney *et al.* (2005) defines demand side risk as represented by the uncertainty surrounding the random demands which often occur at the retailer stage of the supply chain.

Handfield and McCormack (2007) classify supply chain risks from the perspectives of suppliers, customers, and the company. A *supplier facing* perspective examines the network of suppliers, their markets, and their risk relationships with the 'company'. A *customer facing* perspective examines the network of customers and intermediaries, their markets, and their risk relationships with the 'company'. Finally, an *internal facing* perspective examines risk relationships with respect to the company, its network of assets, processes, products, systems and people, as well as its markets. The purpose of this study is to present a methodology for analysing risks associated with suppliers of outsourced materials to facilitate outsourcing decisions. Therefore, this research study uses the supplier facing perspective in the analysis of supply chain risk. Additionally, this study further classifies risk into three categories: *operational*, *network*, and *external*. In the financial industry, *operational risk* is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events (Basel Committee on Banking Supervision 2006). Examples of operational risks are quality, delivery and service problems. *Network risk* is defined as risk resulting from the structure of the supplier network such as ownership, individual strategies of the suppliers, and the supplier's supply network agreements (Wu *et al*. 2006). *External risks* are defined as events driven by external forces such as weather, earthquakes, political, regulatory and market forces (Wagner and Bode 2006).

3. Research methodology

The research methodology for this study includes the use of surveys, the collection of data from both internal and external company sources, and the development of Bayesian networks used to create risk profiles for the study participants. A discussion on Bayesian networks, the assessment model, the study participants, and data collection procedures are provided in Sections 3.1, 3.2, and 3.3, respectively.

3.1 *Bayesian networks*

A Bayesian network is an annotated directed acyclic graph that encodes probabilistic relationships among nodes of interest in an uncertain reasoning problem (Pai *et al*. 2003). The representation describes these probabilistic relationships and includes a qualitative structure that facilitates communication between a user and a system incorporating a probabilistic model. Bayesian networks are based on the work of the mathematician and theologian Rev. Thomas Bayes who worked with conditional probability theory in the late 1700s to discover a basic law of probability which came to be known as Bayes' theorem. Bayes' theorem states that:

$$P(H|E,c) = \frac{P(H|c) \times P(E|H,c)}{P(E|c)}$$

The posterior probability is given by the left-hand term of the equation, $P(H|E,c)$. It represents the probability of hypothesis H after considering the effect of evidence E on past experience c. The term $P(H|c)$ is the a-priori probability of H given c alone. Thus, the a-priori probability can be viewed as the subjective belief of occurrence of hypothesis H based upon past experience. The likelihood, represented by the term $P(E|H,c)$, gives the probability of the evidence assuming the hypothesis H and the background information c is true. The term $P(E|c)$ is independent of H and is regarded as a normalising or scaling factor (Niedermayer 2003). Thus, Bayesian networks provide a methodology for combining subjective beliefs with available evidence.

In recent years, Bayesian networks have evolved as a powerful tool to analyse uncertainty (Pai *et al.* 2003, Cowell *et al.* 2007). When Bayesian networks were first introduced, assigning the full probability distributions manually was time intensive. Solving a Bayesian network with a considerable number of nodes is known to be a nondeterministic polynomial time hard (NP hard) problem (Dagum and Luby 1993). However, tremendous gains in computational power along with the development of heuristic search techniques to find events with the highest probability have enhanced the development and understanding of Bayesian networks. Correspondingly, the Bayesian computational concept has become increasingly popular in such areas as medical diagnosis and weapon tracking systems (Pai *et al.* 2003). The methodology has been shown to be especially useful when information about past and/or current situations is vague, incomplete, conflicting, and uncertain. A numerical example of a Bayesian network and how it can be used to analyse uncertainty is presented in Appendix 1.

Pai *et al.* (2003) were among the first researchers to analyse supply chain risks using Bayesian networks. The study examined the risk profile associated with a US Department of Defense (DoD) supply chain for trinitrotoluene (TNT). The supply chain comprised TNT recovery plants, storage facilities, and ammunition depots. Using Bayesian networks, the researchers were able to establish risk factors and acceptable risk limits for all assets contained in the DoD supply chain.

3.2 *Assessment model*

This study employs a risk assessment model used to evaluate the risks of each supplier within the supply network. The model identifies and quantifies the risk of a supply disruption using a framework that describes key supplier attributes, along with their relationships and interactions with the company performing the assessment. The framework consists of the following risk factors: relationship factors; supplier past performance; human resources factors; history of supply chain disruptions; environmental factors; disaster history; and, financial factors. The risk factors were developed based upon the literature illustrating approaches to supply chain risks cited in Section 2.2. Relationship factors include the level of influence, cooperation, power and shared interests which exist within the network. Quality levels and on-time delivery history are key factors in assessing risks based on past performance. Human resource factors include employee relations issues, employee compensation as compared to industry norms, and unionisation issues. The degree to which the supply chain has experienced disruptions is a key factor in assessing risks based upon its history. Additionally, the history of disaster events such as hurricanes, earthquakes, tornadoes, and floods are incorporated into the framework. Finally, funding sources, debt levels, cash flow analysis, and other indicators of financial health are utilised by the framework to assess financial risks. The risk assessment model is illustrated in Figure 1.

The model uses a set of measures and scales that apply to each risk construct. The measures were developed based upon key events which can directly impact a particular risk factor. The measures and scales are used to create supplier risk profiles. The profiles reflect the risk of a disruptive event involving a particular supplier. Supplier risk profiles are expressed as numerical scores ascertained as a result of applying the model and measures. The higher the risk profile score, the higher the disruption potential of the entity under review. Appendix 2 contains the actual measures used in this study. In order to apply the

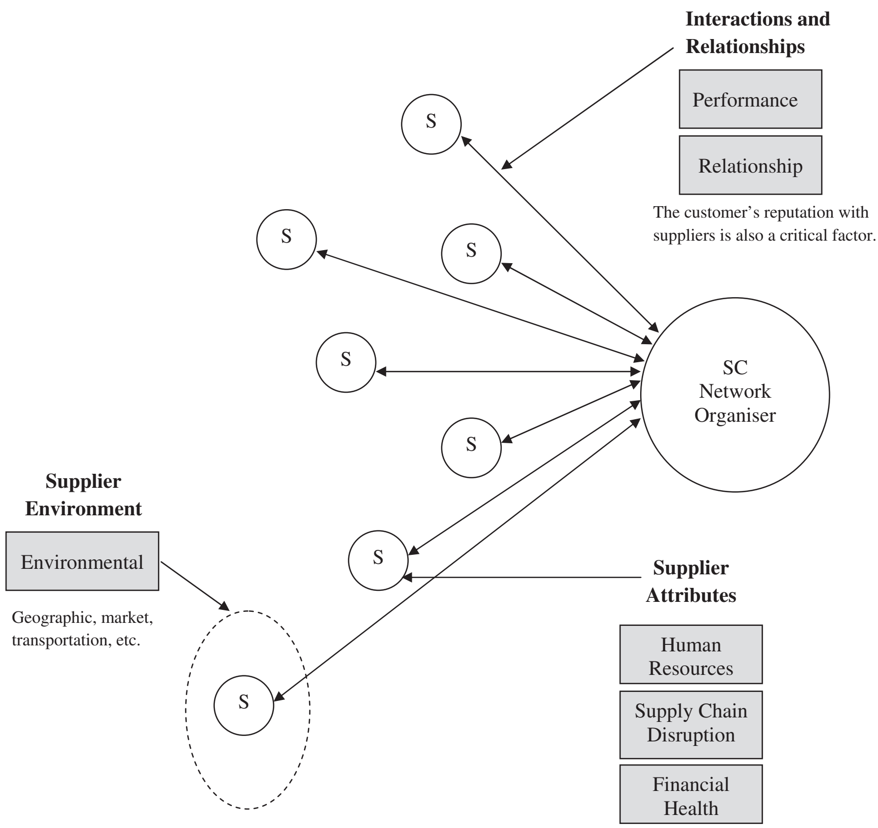


Figure 1. Risk assessment model.

risk results to potential events, the survey results were reorganised into operational, network and external risk-related measures, and the results were recalculated for each supplier. The reorganised measures are presented in Appendix 3. The revenue impact portion of the supplier risk profiles was calculated by: identifying the parts furnished by the supplier; mapping the parts to a finished product and gross revenue for that product; and, calculating the sum of associated monthly revenue for each supplier.

3.3 *Sample and data collection*

The data sample was a group of 15 automotive casting suppliers to a major automotive company in the US. The data was collected using a four-step process. First, the suppliers' representatives were interviewed to discuss the study and the supplier self-assessment online survey instrument to be completed by the representatives. The survey instrument links were then sent by email to the account representatives. Upon receiving the completed surveys, the next step was to conduct on-site interviews with key personnel in the supply chain departments to validate information collected via the survey instrument, and to obtain more specific details on their supply chain risk factors. The third step in the data collection process was to conduct interviews with commodity managers in the castings area in an effort to triangulate the data collected from the surveys and supply chain departments. Finally, off-site research was conducted to gather data regarding the following: market dynamics; mergers, divestitures, and acquisitions; regulatory issues; disasters; and transportation disruptions. This data was used to measure environmental risk factors. A five-point Likert scale was used for the rating of all risk factors, and a risk index was calculated for each supplier.

4. Results

Upon the collection of network, operational, and external risk data for each supplier, Bayesian networks were constructed to establish their risk profiles using a supplier facing perspective. Thus, the model examines the probability of a supplier's revenue impact on a company based upon the supplier's associated network, operational, and external risks. Network, operational, and external risks were determined based upon the *a priori* probabilities for risk events which directly influence them, as outlined in Appendix 3. These probabilities were ascertained via the data collection process. An illustration of the Bayesian network for Supplier 1 is provided in Figure 2.

The variables in the Bayesian network are represented by nodes. Each node contains states, or a set of probable values for each variable. The variables in the network illustrated

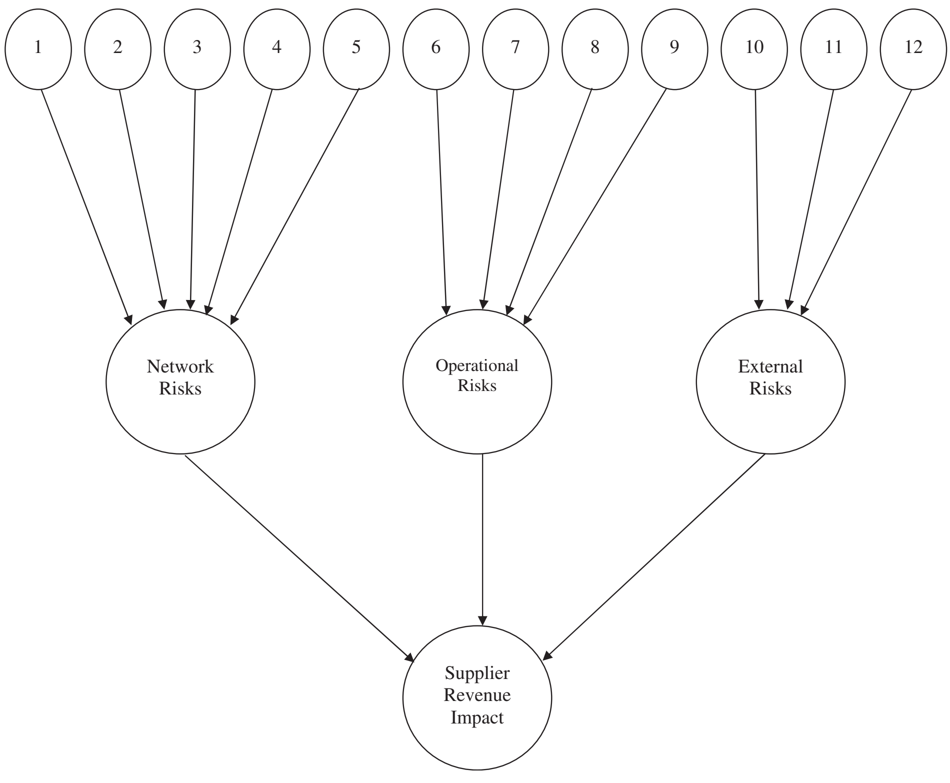


Figure 2. Bayesian network for Supplier 1. Note: network key: 1 = misalignment of interest; 2 = supplier financial stress; 3 = supplier leadership change; 4 = tier 2 stoppage; 5 = supplier network misalignment; 6 = quality problems; 7 = delivery problems; 8 = service problems; 9 = supplier HR problems; 10 = supplier locked; 11 = merger/divestiture; 12 = disasters.

in Figure 2 can exist at two states (yes or no). Nodes are connected to show causality with an arrow (known as an edge) indicating the direction of influence. When two nodes are joined by an edge, the causal node is referred to as the parent of the influenced (child) node. Child nodes are conditionally dependent upon their parent nodes. Thus, in Figure 2, the probability of Supplier 1 experiencing network risks is dependent on the *a priori* probabilities associated with the following variables: misalignment of interest; supplier financial stress; supplier leadership change; tier 2 stoppage; and supplier network misalignment. The *a priori* probabilities associated with the variables quality problems, delivery problems, and service problems directly influence operational risks. Finally, external risks are dependent upon the following variables: supplier HR problems, supplier locked (i.e., company cannot easily switch to another supplier), merger/divestitures, and disasters. The joint probabilities of the computed network, operational, and external risks are then used to determine the probability that a supplier will have an adverse impact on the company's revenue stream. The product of the supplier's revenue impact probability times its revenue impact is known as *value at risks*. Value-at-risk (VAR) is widely used by banks, securities firms, commodity merchants, energy merchants, and other trading organisations. Such firms track their portfolios' market risk by using historical volatility as a risk metric. VAR can also be used to evaluate and manage risks in the supply chain. The Supply Chain Council defines VAR as *the sum of the probability of events times the monetary impact of the events for the specific process, supplier, product or customer* (SCOR Model 9.0 2008). Thus, this metric allows for comparisons between suppliers to facilitate decisions regarding supply chain risk. This research study examines monthly value-at-risk dollars for the company based upon the risk profiles of each supplier.

The *a priori* probabilities for the 12 supply chain risk events which influence network, operational, and external risks are presented in Table 1 for each supplier. These values were used to generate a risk profile using Bayesian networks comprising network, operational and external risk probabilities along with the supplier's probability of revenue impact on the company. The supplier risk profiles are displayed in Table 2. The table reveals that Suppliers 1, 10 and 14 have the highest probability of revenue impact on the company, while Supplier 11 has the lowest probability of revenue impact. Computations illustrating the development of the risk profile for Supplier 1 are presented in Appendix 4.

4.1 *Sensitivity analysis*

A risk profile sensitivity analysis was conducted for each supplier to determine the effects of known risk events (i.e., network, operational, and/or external risk have a 100% probability of occurrence) on company revenues. An example of the analysis is illustrated for Supplier 1 in Table 3. The table shows that the simultaneous occurrence of risk events which result in network and external risks increases the probability of revenue impact from the base case of 41% to 83%. A comparison of the supplier risk profiles based upon *a priori* risk event probabilities and worst-case combinations of network, operational, and external risks (excluding the scenario where all three risks have a 100% probability of occurrence) along with corresponding value-at-risk results is provided in Table 4.

An examination of Table 4 reveals that the risk profile associated with Supplier 6 results in the largest value-at-risk dollars for both the base case ($148.80 million) and the worst-case risks combination ($376.65 million). The risk profile of Supplier 15 yields the smallest value-at-risk dollars for the base case ($2.13 million) and the worst-case risks combination ($5.74 million). The largest percentage increase in value-at-risk dollars

Table 1. *A priori* probabilities for risk event variables.

Supplier	Misalignment of interest	Supplier financial stress	Supplier leadership change	Tier 2 stoppage	Supplier network misalignment	Quality problems	Delivery problems	Service problems	Supplier HR problems	Supplier locked	Merger/ divestiture	Disasters
1	0.20	0.50	0.50	0.31	0.20	0.46	1.00	0.20	0.20	0.18	1.00	0.11
2	0.17	0.23	0.23	0.13	0.20	0.23	0.46	0.10	0.12	0.06	1.00	0.08
3	0.20	0.50	0.50	0.31	0.12	0.48	0.95	0.20	0.20	0.18	1.00	0.12
4	0.16	0.33	0.23	0.16	0.17	0.21	0.52	0.11	0.09	0.09	1.00	0.10
5	0.19	0.38	0.23	0.17	0.20	0.22	0.53	0.10	0.07	0.11	1.00	0.13
6	0.14	0.46	0.27	0.18	0.14	0.33	0.65	0.09	0.13	0.15	1.00	0.13
7	0.16	0.31	0.37	0.15	0.16	0.26	0.57	0.08	0.11	0.11	1.00	0.10
8	0.19	0.30	0.23	0.16	0.20	0.29	0.60	0.10	0.07	0.13	1.00	0.12
9	0.15	0.35	0.27	0.15	0.17	0.30	0.63	0.09	0.11	0.11	1.00	0.10
10	0.21	0.50	0.50	0.32	0.16	0.47	0.96	0.20	0.20	0.19	1.00	0.16
11	0.18	0.23	0.17	0.15	0.16	0.29	0.58	0.11	0.11	0.11	0.80	0.12
12	0.19	0.50	0.30	0.29	0.14	0.36	0.82	0.15	0.07	0.10	0.80	0.11
13	0.18	0.37	0.27	0.16	0.16	0.23	0.62	0.08	0.12	0.10	1.00	0.09
14	0.20	0.50	0.50	0.31	0.16	0.50	0.96	0.20	0.20	0.18	1.00	0.11
15	0.17	0.35	0.33	0.14	0.16	0.22	0.60	0.10	0.12	0.13	1.00	0.12

Table 2. Supplier risk profiles.

Supplier	Network risk probability	Operational risk probability	External risk probability	Probability of revenue impact
1	0.34	0.47	0.43	0.41
2	0.19	0.23	0.38	0.27
3	0.33	0.46	0.43	0.40
4	0.21	0.23	0.39	0.28
5	0.23	0.23	0.41	0.29
6	0.24	0.30	0.43	0.32
7	0.22	0.27	0.41	0.30
8	0.22	0.27	0.41	0.30
9	0.22	0.28	0.40	0.30
10	0.34	0.46	0.45	0.41
11	0.18	0.27	0.34	0.26
12	0.28	0.35	0.33	0.32
13	0.23	0.27	0.39	0.30
14	0.33	0.47	0.43	0.41
15	0.23	0.26	0.41	0.30

Table 3. Risk profile sensitivity analysis for Supplier 1.

Network risk probability	Operational risk probability	External risk probability	Probability of revenue impact
*0.34	*0.47	*0.43	*0.41
1.00	0.47	0.43	0.63
0.34	1.00	0.43	0.59
0.34	0.47	1.00	0.60
1.00	1.00	0.43	0.81
1.00	0.47	1.00	0.83
0.34	1.00	1.00	0.78

Note: *base case.

between a supplier's base case and worst-case combination risk profile is 67% for Supplier 11 ($11.92 million versus $35.75 million). However, the average percentage increase in value-at-risk dollars between these scenarios is 60% for all suppliers. Along with Supplier 11, Suppliers 2, 4, 5, and 7 exhibit the largest increases in value-at-risk dollars between their base case and worst-case risks combination (66%, 65%, 64%, and 64%, respectively). The smallest percentage increase in this area is 50%, as exhibited by the risk profiles associated with Suppliers 10 and 14. It is interesting to note that the risk profile of Supplier 10 resulted in two worst-case risk combinations: network risk-operational risk and network risk-external risk. These risk combinations both yielded a 0.82 probability of revenue impact value. Finally, the most prevalent worst-case combination for the 15 suppliers is the simultaneous occurrence of network and operational risk events. This combination resulted in the highest probability of revenue impact values for 11 suppliers. The network risk-external risk combination provided the highest probability of revenue impact values for five suppliers. The combination of simultaneous operational and external risk events failed to yield a worst-case combination for any supplier.

Table 4. Risk profile and value at risk sensitivity analysis for all suppliers.

Supplier	Network risk probability	Operational risk probability	External risk probability	Probability of revenue impact	Annual revenue impact (millions)	Monthly revenue impact (millions)	Value-at-risk (probability × monthly revenue impact)
1	*0.34	*0.47	*0.43	0.41	$225	$18.75	$7,687,500
	1	0.47	1	0.83	$225	$18.75	$15,562,500
2	*0.19	*0.23	*0.38	0.27	$375	$31.25	$8,437,500
	1	1	0.38	0.79	$375	$31.25	$24,687,500
3	*0.33	*0.46	*0.43	0.40	$2610	$217.5	$87,000,000
	1	0.46	1	0.82	$2610	$217.5	$178,350,000
4	*0.21	*0.23	*0.39	0.28	$2165	$180.42	$50,516,667
	1	1	0.39	0.80	$2165	$180.42	$144,333,333
5	*0.23	*0.23	*0.41	0.29	$900	$75.00	$21,750,000
	1	1	0.41	0.81	$900	$75.00	$60,750,000
6	*0.24	*0.30	*0.43	0.32	$5580	$465.00	$148,800,000
	1	1	0.43	0.81	$5580	$465.00	$376,650,000
7	*0.23	*0.26	*0.40	0.29	$1075	$89.58	$25,979,167
	1	1	0.40	0.80	$1075	$89.58	$71,666,667
8	*0.22	*0.27	*0.41	0.30	$210	$17.50	$5,250,000
	1	1	0.41	0.81	$210	$17.50	$14,175,000
9	*0.22	*0.28	*0.40	0.30	$3490	$290.83	$87,250,000
	1	1	0.40	0.80	$3490	$290.83	$232,666,667
10	*0.34	*0.46	*0.45	0.41	$1635	$136.25	$55,862,500
	1	1	0.45	0.82	$1635	$136.25	$111,725,000
	1	0.46	1	0.82	$1635	$136.25	$111,725,000
11	*0.18	*0.27	*0.34	0.26	$550	$45.83	$11,916,667
	1	1	0.34	0.78	$550	$45.83	$35,750,000
12	*0.28	*0.35	*0.33	0.32	$550	$45.83	$14,666,667
	1	0.35	1	0.79	$550	$45.83	$36,208,333
13	*0.23	*0.27	*0.39	0.30	$1135	$94.58	$28,375,000
	1	1	0.39	0.80	$1135	$94.58	$75,666,667
14	*0.33	*0.47	*0.43	0.41	$250	$20.83	$8,541,667
	1	0.47	1	0.82	$250	$20.83	$17,083,333
15	*0.23	*0.26	*0.41	0.30	$85	$7.08	$2,125,000
	1	1	0.41	0.81	$85	$7.08	$5,737,500

Note: *base case.

5. Managerial actions

There are several items which should be examined by the company for possible managerial actions based upon the results of this study. Given the potential impact that Supplier 6 could have on the company's revenue stream based upon its risk profile, it is imperative that the company take proactive measures to reduce its value-at-risk exposure with this supplier. For example, the company might engage in cooperative improvement projects with the supplier in an effort to reduce network and operational risks. On the contrary, the company may choose to discontinue its outsourcing relationship with this supplier, or apportion more of its business to one of the other 14 automotive casting suppliers exhibiting a less risky profile. In any event, the company should make reducing its revenue exposure to Supplier 6 a major priority.

An examination of Table 4 shows that one-third of the company's suppliers have the potential to increase their value-at-risk percentages by at least 64% through the occurrence of risk events resulting in worst-case combination scenarios. The company should also re-evaluate its outsourcing relationship with these suppliers. Finally, with a potential average percentage increase in value-at-risk dollars of 60% for all suppliers, it may be prudent for the company to conduct a 'make versus buy' analysis to examine the possibility of 'insourcing' this commodity. Given the magnitude and potential volatility of these dollars due to the suppliers' risk profiles, it may be more economical (and less risky) to furnish the castings via internal sources.

6. Conclusions and implications

We conclude that this study illustrates a methodology for analysing risks in supply networks which can be used to facilitate outsourcing decisions. Risk profiles can be developed using Bayesian networks for suppliers furnishing common raw materials or components which can be examined to analyse current and future outsourcing relationships. The profiles can also be used to determine the risk exposure of a company's revenue for its supplier base. Additionally, we conclude that the methodology could also be used to analyse risks associated with potential suppliers who are under consideration as part of a company's outsourcing strategy. Finally, we conclude that the methodology presented in this study could also serve as a tool for examining the viability of insourcing based upon an assessment of the aggregate risk profile of the supply network for the commodity.

6.1 *Limitations*

This study provided an examination of risk profiles associated with casting suppliers in the US automotive industry. Therefore, the results could be industry-specific in nature. In addition, the study examined only 15 suppliers in the US automotive industry, thus limiting the generalisability of outsourcing risks in this sector. A limitation to the use of the methodology presented in this study is the ability to access the necessary data needed to construct the Bayesian networks. Depending on the established relationship, some suppliers may be reluctant to share risk profile data with their customers. However, the most important potential limitation to the use of this methodology to assess risks in supply networks is the supplier's ability to provide accurate information regarding network, operational, and external risks as reflected in the 12 risk events outlined in Appendix 2. Suppliers must be willing to periodically update this information in order to construct a risk profile that is valid and reliable.

6.2 *Future research*

Risk profiles for suppliers and supply networks in other industries should be examined using the methodology illustrated in this study to determine if industry dynamics significantly influence supply chain risks. In addition, future researchers may choose to solely focus on the impact of network, operational, or external risks on supply networks. For example, what would be the value-at-risk for a company if it were possible to totally eliminate network risk? Finally, future researchers may examine the simultaneous occurrence of operational and external risk events to see if there are supply networks and/or industries where this combination results in the worst-case combination for a company based on value-at-risk dollars.

References

Abell, D., 1999. Competing today while preparing for tomorrow. *MIT Sloan Management Review*, 40 (3), 73–81.

Ayyub, B.M., 2003. *Risk analysis in engineering and economics*. Boca Raton, FL: Chapman & Hall/CRC Press, ISBN 1-58488-395-2.

Baldwin, L.P., Irani, Z., and Love, P.E.D., 2001. Outsourcing information systems: drawing lessons from a banking case study. *European Journal of Information Systems*, 10 (1), 15–24.

Basel Committee on Banking Supervision, 2006. *International convergence of capital and capital standards*. ISBN print: 92-9131-720-9; ISBN web: 92-9197-720-9. Available from: http://www.bis.org/ [Accessed 5 September 2006].

Chen, L. and Kang, F., 2007. Integrated vendor-buyer cooperative inventory models with variant permissible delay in payments. *European Journal of Operational Research*, 183 (2), 658–673.

Chopra, S. and Sodhi, M., 2004. Managing risk to avoid supply-chain breakdown. *Sloan Management Review*, 46 (1), 53–61.

Choy, K.L. and Lee, W.B., 2003. A generic supplier management tool for outsourcing manufacturing. *Supply Chain Management*, 8 (2), 140–154.

Clott, C.B., 2004. Perspectives on global outsourcing and the changing nature of work. *Business and Society Review*, 109 (2), 153–170.

Cooper, M., Lambert, D., and Pagh, J., 1997. Supply chain management: more than a new name for logistics. *The International Journal of Logistics Management*, 8 (1), 1–14.

Cowell, R.G., Verrall, R.J., and Yoon, Y.K., 2007. Modeling operational risk with Bayesian networks. *Journal of Risk and Insurance*, 74 (4), 795–827.

Croxton, K., *et al.*, 2002. The demand management process. *International Journal of Logistics Management*, 13 (2), 51–66.

Dagum, P. and Luby, M., 1993. Approximating probabilistic inference in Bayesian belief networks is NP-hard. *Artificial Intelligence*, 60 (1), 141–153.

Gonzalez, R., Gasco, J., and Llopis, J., 2005. Information systems outsourcing reasons in the largest Spanish firms. *International Journal of Information Management*, 25 (2), 117–136.

Giunipero, L. and Eltantawy, R., 2004. Securing the upstream supply chain: a risk management approach. *International Journal of Physical Distribution & Logistics Management*, 34 (9), 698–713.

Gunasekaran, A., Lai, K., and Cheng, T., 2008. Responsive supply chain: a competitive strategy in a networked economy. *Omega*, 36 (4), 549–564.

Hackett Group, 2007. Dow chemical company: supply risk management process is key to improving safety and security. *Procurement Executive Insight*, 9 October.

Handfield, R. and McCormack, K., 2007. *Supply chain risk management: minimizing disruptions in global sourcing*. Boca Raton, FL: Auberbach Publications.

Hendricks, K. and Singhal, V.R., 2005. The effect of supply chain disruptions on long-term shareholder value, profitability, and share price volatility. *Production and Operations Management*, 14 (1), 35–52.

ISO, 2002. *ISO/IEC guide 73 – risk management – vocabulary – guidelines for use in standards*. Geneva, Switzerland: International Organization for Standardization. [Visit http://www.iso.org for information.]

Jammernegg, W. and Reiner, G., 2007. Performance improvement of supply chain processes by coordinated inventory and capacity management. *International Journal of Production Economics*, 108 (1–2), 183–190.

Jennings, D., 2002. Strategic sourcing: benefits, problems and a contextual model. *Management Decision*, 40 (1), 26–34.

Kannan, V.R. and Tan, K.C., 2002. Supplier selection and assessment: their impact on business performance. *Journal of Supply Chain Management*, 38 (4), 11–21.

Knight, R. and Pretty, D., 1996. *The impact of catastrophes on shareholder value*. Research report. The Oxford Executive Research Briefings, Templeton College, University of Oxford, UK.

Kopczak, L. and Johnson, M., 2003. The supply-chain management effect. *MIT Sloan Management Review*, 44 (3), 27–34.

Kremic, T., Take, O.I., and Rom, W.O., 2006. Outsourcing decision support: a survey of benefits, risks and decision factors. *Supply Chain Management: An International Journal*, 11 (6), 467–482.

Lau, K.H. and Zhang, J., 2006. Drivers and obstacles of outsourcing practices in China. *International Journal of Physical Distribution & Logistics Management*, 36 (10), 776–792.

Latour, A., 2001. Trial by fire: a blaze in Albuquerque sets off major crisis for cell-phone giants-Nokia handles supply shock with aplomb as Ericsson of Sweden gets burned – was SISU the difference? *Wall Street Journal*, 29 January, A1.

Li, S., *et al*., 2006. The impact of supply chain management practices on competitive advantage and organizational performance. *Omega*, 34 (2), 107–124.

Lynch, C.F., 2004. Why outsource? *Supply Chain Management Review*, 8 (7), 44–49.

Nagurney, A., *et al*., 2005. Supply chain networks, electronic commerce, and supply side and demand side risk. *European Journal of Operational Research*, 164 (1), 120–142.

Neiger, D., Rotaru, K., and Churilov, L., 2009. Supply chain risk identification with value-focused process engineering. *Journal of Operations Management*, 27 (2), 154–168.

Niedermayer, D., 2003. *An introduction to Bayesian networks and their contemporary applications* [online]. Available from: http://www.niedermayer.ca/papers/bayesian/bayes.html [Accessed 18 March 2008].

Norrman, A. and Jansson, U., 2004. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management*, 34 (5), 434–456.

Pai, R., *et al*., 2003. Methods toward supply chain risk analysis. *In*: *Proceedings of the IEEE international conference on systems, man and cybernetics*, Vol. 5, 5–8 October Washington, DC, 4560–4565.

Rice, J.B. and Caniato, F., 2003. Building a secure and resilient supply network. *Supply Chain Management Review*, 7 (5), 22–30.

Singh, P., Smith, A., and Sohal, S., 2005. Strategic supply chain management issues in the automotive industry: an Australian perspective. *International Journal of Production Research*, 43 (16), 3375–3400.

SCOR Model 9.0, 2008. *Supply chain operations reference model version 9.0*. Washington, DC: Supply Chain Council. [Visit http://www.supply-chain.org for information.]

Suttner, U., 2005. Supply chain risk management: understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management*, 16 (1), 120–141.

Tang, C., 2006. Perspectives in supply chain risk management. *International Journal of Production Economics*, 103 (2), 451–488.

Treleven, S. and Schweikhart, B., 1988. A risk/benefit analysis of sourcing strategies: single vs. multiple sourcing. *Journal of Operations Management*, 7 (4), 93–114.

Wagner, S.M. and Bode, C., 2006. An empirical investigation into supply chain vulnerability. *Journal of Purchasing and Supply Management*, 12 (6), 301–312.

Weerakkody, V., Curries, W.L., and Ekanayahe, Y., 2003. Re-engineering business processes through application service providers. *Business Process Management Journal*, 9 (6), 776–794.

Wu, T., Blackhurst, J., and Chidambaram, V., 2006. A model for inbound supply risk analysis. *Computers in Industry*, 57 (4), 350–365.

Zsidisin, G., Melnyk, S., and Ragatz, G., 2005. An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, 43 (16), 3401–20.

Appendix 1. Bayesian network example

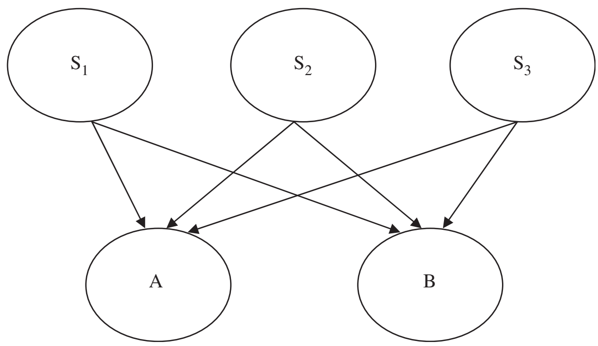
Suppose that the state of the US economy is classified into three categories: recession (S_1), stability (S_2), and prosperity (S_3). The business research department of a large firm is responsible for developing forecasts regarding the economic condition for the following year. The department makes two types of forecasts: optimistic (A) and pessimistic (B). Suppose further that based upon years of prior data, the proportion of times that optimistic and pessimistic forecasts were made in the preceding years are as follows:

$$P(A|S_1) = 0.1, \quad P(A|S_2) = 0.5, \quad P(A|S_3) = 0.8;$$
$$P(B|S_1) = 0.9, \quad P(B|S_2) = 0.5, \quad P(B|S_3) = 0.2.$$

It is also assumed that stability is twice as likely to appear as either recession or prosperity. The firm is interested in analysing the following issues:

(1) If the forecast for the next year is optimistic, what is the probability that the economy will be prosperous? (i.e., $P(S_3|A)$.)
(2) If the forecast for the next year is pessimistic, what is the probability that the economy will be in a recession? (i.e., $P(S_1|B)$.)

From the information provided in this example, the following Bayesian network can be constructed:



Bayesian networks can be used to perform inductive reasoning (diagnosing a cause given an effect) and deductive reasoning (predicting an effect given a cause).

A conditional probability table also containing the *a priori* probabilities for each state of the economy based on the provided data is given in Table A1.

A joint probability table is also developed by multiplying the *a priori* probabilities by the corresponding conditional probabilities for a given state of the economy, which is illustrated in Table A2.

Using Bayesian analysis, the following answers are obtained regarding the aforementioned issues:

(1) $P(S_3|A) = \dfrac{P(S_3 \cap A)}{P(A)} = \dfrac{0.200}{0.475} = 0.42;$

(2) $P(S_1|B) = \dfrac{P(S_1 \cap B)}{P(B)} = \dfrac{0.225}{0.525} = 0.43.$

Table A1. Conditional probability table.

A priori probability	State of the economy	Optimistic forecast (A)	Pessimistic forecast (B)
$P(S_1) = 0.25$	S_1	0.1	0.9
$P(S_2) = 0.50$	S_2	0.5	0.5
$P(S_3) = 0.25$	S_3	0.8	0.2

Table A2. Joint probability table.

State of the economy	Optimistic forecast (A)	Pessimistic forecast (B)
S_1	$P(S_1 \cap A) = 0.025$	$P(S_1 \cap B) = 0.225$
S_2	$P(S_2 \cap A) = 0.250$	$P(S_2 \cap B) = 0.250$
S_3	$P(S_3 \cap A) = 0.200$	$P(S_3 \cap B) = 0.050$
Total	$P(A) = 0.475$	$P(B) = 0.525$

Thus, the probability that next year's economy will be prosperous if the forecast is optimistic is 42%, while the probability that next year's economy will be in a recession if the forecast is pessimistic is 43%.

Appendix 2. Risk assessment measures

Behaviour	Relationship	Supplier revenue from industry segment
		Influence of revenue from company
		Supplier/company alignment
		Supplier/company information sharing
	Performance	Accreditation
		Engineering support
		Capacity utilisation
		Capacity change
		Delivery flexibility
		Manufacturing employees
		Service promptness
		MRR
		Audit date
		Audit score
		On-time delivery
	Human resources	Employee turnover
		Senior staff turnover
		Union issues
		Pay position
Structure	Supply chain disruption	Market power
		Tier 2 information sharing
		Tier 2 performance monitoring
		Disruption probability
		Risk management system
		Material sourcing base
	Financial health	Market growth
		Financial risk indicators
	Environmental	Market dynamics
		Merger and acquisition
		Regulatory
		Disaster
		Transportation
	Network	Supplier's customers
		Supplier customer relationships
		Alignment
		Supplier's supplier
		Supplier vendor relationships
		Vendor concentration
		Code of conduct

Appendix 3. Network, operational and external risk measures

Network risks	Misalignment of interest	Influence of revenue from company
		Supplier revenue from commodity category
		Supplier/company alignment
		Regulatory
	Supplier financial stress	Customer portfolio
		Business health indicators
		Segment portfolio
		Market growth
		Financial data sharing
	Supplier leadership change	Company ownership change likelihood
		Merger and acquisition
		Senior staff turnover
	Tier 2 stoppage	Process change likelihood
		Miscommunication between tiers
		Material change/obsolesce likelihood
		Risk management system
		Material sourcing base
		Market power
		Regulatory
		Regulatory change risk likelihood
		Inventory status sharing
		Tier 2 supplier information sharing
		Process/material change notification
	Supplier network misalignment	Supplier customer alignment
		Vendor concentration
Operational risks	Quality problem	Process change likelihood
		MRR (defects)
		Audit date
		Audit score
		Tier 2 performance monitoring
		Quality problems likelihood
		Manufacturing employees
		Accreditation
		Material change/obsolesce likelihood
		Process/material change notification
	Delivery problem	Performance data sharing
		On-time delivery
		Capacity utilisation
		Tier 2 information sharing
		Delivery flexibility
		Capacity shortage likelihood
		Manufacturing employees
		Capacity change
		Inventory status sharing
		Order fulfilment information sharing
		Production schedule sharing
	Service problem	Engineering support
		Service promptness
		Employee turnover
		Human resource issues likelihood
		New technology opportunity sharing
External Risks	Supplier HR problem	Union issues
		Employee turnover
		Pay position
	Supplier locked	Accreditation information sharing
		EPA and FDA report sharing
		Regulatory
		Accreditation
	Merger/divestiture	Market dynamics
		Merger and acquisition
	Disasters	Supplier is providing proof of insurance
		Disaster
		Transportation

Appendix 4. Risk profile for Supplier 1

Given the risk event relationships exhibited in the supplier Bayesian network illustrated in Figure 2 along with the *a priori* probabilities for risk event variables contained in Table 1, the following probability computations regarding network risks, operational risks, external risks, and revenue impact for Supplier 1 are provided:

$$\begin{aligned}
\text{P(network risks)} &= \frac{\sum(\text{probability of network risk event}) \times (\text{probability of event occurrence})}{\sum(\text{probability of event occurrence})} \\
&= \frac{[(0.20) \times (1)] + [(0.50) \times (1)] + [(0.50) \times (1)] + [(0.31) \times (1)] + [(0.20) \times (1)]}{1+1+1+1+1} \\
&= \frac{1.71}{5} \\
&= 0.034;
\end{aligned}$$

$$\begin{aligned}
\text{P(operational risks)} &= \frac{\sum(\text{probability of operational risk event}) \times (\text{probability of event occurrence})}{\sum(\text{probability of event occurrence})} \\
&= \frac{[(0.46) \times (1)] + [(1.00) \times (1)] + [(0.20) \times (1)] + [(0.20) \times (1)]}{1+1+1+1} \\
&= \frac{1.86}{4} \\
&= 0.47;
\end{aligned}$$

$$\begin{aligned}
\text{P(external risks)} &= \frac{\sum(\text{probability of external risk event}) \times (\text{probability of event occurrence})}{\sum(\text{probability of event occurrence})} \\
&= \frac{[(0.18 \times (1)] + [(1.00) \times (1)] + [(0.11) \times (1)]}{1+1+1} \\
&= \frac{1.29}{3} \\
&= 0.43;
\end{aligned}$$

$$\begin{aligned}
&\text{P(revenue impact)} \\
&= \frac{\sum\big[\,[\text{P(NR)} \times \text{P(occurrence)}] + [\text{P(OR)} \times \text{P(occurrence)}] + [\text{P(ER)} \times \text{P(occurrence)}]\,\big]}{\sum(\text{probability of risk occurrence})} \\
&= \frac{[(0.34 \times (1)] + [(0.47) \times (1)] + [(0.43) \times (1)]}{1+1+1} \\
&= \frac{1.24}{3} \\
&= 0.41.
\end{aligned}$$