Journal of Information Technology (1996) **11**, 309–319

Risk management for information systems development

PHILIP L. POWELL
Information Systems Research Unit, Warwick Business School, University of Warwick, Coventry CV4 7AL, UK

JONATHAN H. KLEIN
Centre for Risk Research, Department of Management, University of Southampton, Southampton SO17 1BJ, UK

This paper considers the application of project risk management techniques, methods and approaches to information systems development. The paper reviews current thinking on risk as it relates to information systems, and the approaches to risk that have been adopted in IS projects. The paper considers, in the context of IS, the processes of risk identification, structuring, assessment, and aggregation, and the use of such risk analysis to inform the process of risk management. The paper analyses available risk management techniques, and then proceeds to develop a comprehensive decision support system to aid risk analysis.

Introduction

This paper considers the application of project risk management techniques to information systems (IS) development projects. The motivation for such an approach is that the success rate of IS projects is currently low, and the belief that it might be raised considerably by due consideration of risks in a fashion intended to be both comprehensive and systematic. Risk management techniques allow such consideration. That the failure of IS projects is due to the manifestation of risks is almost tautologous; that this problem might be alleviated by risk management is an article of faith, but, given the degree of success in the context of general project management, not, it is argued, *blind* faith. This faith is backed, however, by the widespread use of risk management techniques in settings other than IS and thus *de facto* evidence of usefulness in this context.

This paper first reviews current thinking concerning the relationship of risk and IS projects. The overall conclusion is that, while the literature offers many useful insights, and it is clear that many researchers and practitioners take the consideration of risk seriously in their recommendations for IS project management, there remains much scope for the development of techniques and approaches to aid such consideration and their provision in a systematic way.

The paper considers current approaches to IS risk management. However, the majority of current attempts (for example, Liang and Tang, 1991, and Whiting *et al.*, 1993) to support risk management are partial since they tend to concentrate on environmental and macro-level risk while ignoring risks during development. An all-encompassing view needs to marry environmental and project risk at a level which aids development of new systems as well as evaluating extant ones.

The paper then proceeds to develop a framework for providing such aid, by characterizing IS project management as a specific instance of project management. It considers the component activities of risk analysis and management, and discusses approaches relevant to these activities. In addition, it highlights the role which decision support technology may have in supporting these activities and offers the elements of a decision support system for achieving this.

Risk and information systems

The failure rate of information systems projects is high. Estimates of the success rate put it as low as 20% (Mowshowitz, 1976) or lower (Willcocks and Griffiths, 1995). Developers lose effective control of perhaps as many as 30% of projects with efforts to control spending and duration repeatedly failing (Price Waterhouse, 1989). The estimated success rates for projects involving more advanced technologies, such as expert systems, are as low as one in ten (Keyes, 1989). It is not surprising that this has led to much research which seeks to identify the reasons for the failure of information systems projects. These reasons are typically classifications of failure types rather than causal explanations, such as those in Table 1. Seldom, however, are these reasons for failure explicitly related

to risks associated with projects, and seldom, therefore, is the development of systematic approaches to manage such risks considered. Willcocks and Margetts (1994) lament the lack of an anticipatory mode of thinking about risks by information systems developers.

Where it exists, consideration of risk in IS spans both the development of individual application systems and the provision of strategic information systems (SIS). There seems to be more recognition of the risks inherent in strategic systems than in lower-level operational ones, perhaps because of the greater evidence and perhaps visibility of failure for SIS and the more obvious centrality of various kinds of uncertainty in strategic contexts. For example, Ruohonen (1991) suggests that 'strategic information systems planning is . . . not well structured and requires considerable creativity and some risk-taking to be successful'. Similarly, Liang and Tang (1991) state that the risks associated with SIS are much higher, and the impact of system failure more severe, than for conventional DP systems.

For strategic information systems, Kemerer and Sosa (1991) identify a number of problems (or risks) which indicate the types of issues of relevance. For example, potential problems at the feasibility stage include the conception of SIS within the context of a non-supportive corporate environment, a lack of leadership, a lack of vision, and difficulties in inter-firm communication: inter-organizational systems require inter-organizational co-operation. In addition, systems must be technically feasible and there must be a real need for them. SIS are expensive, complex to develop, can be problematic to maintain and adapt, may be copied by competitors, may create over-subscription, and may create high barriers to exit. Likewise, Harris and Katz (1991) feel that 'investments in information technology represent a major source of business risk and this risk must be managed effectively through the link with the firm's strategy, the structure of the organization, the measurement and control system, the reward system, and the characteristics of the technology'. Harris and Katz (1991) base their work on an analysis of life assurance firms and they claim that their results are consistent with others who contend that how technology is used and managed is as important as the level of spending.

The work by Kemerer and Sosa (1991) reflects prevailing IS thinking, in which the major risks tend to be viewed as organizational, social and political rather than technical (Willcocks and Margetts, 1994), though any comprehensive risk management system would need to address all risk sources. The notion of risk also appears in other guises in discussion of information systems projects. For example, Vitale (1986) points to the danger that an IS project will succeed,

Table 1 Risk sources and probabilities (after Green, 1995)

Event	Occurrence from 300 disasters (%)
Electrical supply problem	15.1
Fire	13.2
Earthquake	12.8
Human error	12.8
Fraud/hacker	10.7
Virus	7.3
Flood/water pipe fracture	7.1
Computer hardware failure	4.8
Hurricane	3.8
Terrorism	3.4
Network failure	3.4
Computer software failure	3.3
Other	2.3

Source: Contingency Planning Research Inc.

in the sense that it is accepted and adopted, and that then 'the unintended and unanticipated organizational and competitive consequences of technical success could be catastrophic'; the way to avoid this, Vitale suggests, is by the consideration and management of risks. However, there are those (Ballantine *et al.*, 1996, for example) who question the notion of IS success, pointing out the multi-dimensional and complex nature of the concept. Ballantine *et al.* attempt to improve the understanding of the concept of IS success by separating success into three fundamental dimensions – the technical development level, the deployment to the user, and the delivery of business benefits. Clearly success at one level does not imply the system will be successful at another. Concomitantly, risks will be prevalent to different degrees at these different levels; again this stresses the need to consider risks beyond the technical.

Stahl (1989) finds empirically that the cost, risk-return balance and potential competitive advantage of an IS project are all significant in the decision to invest. Of these, cost is the least important to his sample. Harrison (1992) also highlights the importance of the balance between risk and return; he feels that the trade-off between risk and reward tends not to be systematically assessed in strategic decisions, but that CEOs are aware of the relationship. Wildemann (1988) sees risk as a major factor in the analysis of the strategic importance of flexible technologies. Some authors see consideration of risk as having broader benefits. For example, Krumm and Rolle (1992) see decision and risk analysis as 'particularly useful in helping decision makers to focus on shareholder value' as it ensures disciplined thinking and encourages involvement of key personnel in decisions. Benefits include tangible ones

Table 2 Risk sources (after Green, 1995)

- Water
  - Water Damage
  - Fire Detection/Protection Systems
  - Flood/Tidal Wave
  - Storm/Atmospheric Condition
  - Temperature/Humidity
  - Earthquake/Subsidence/Landslide
- Fire
  - Fire/Gas Explosion/Fuel Explosion
  - Arson
  - Forest Fire
  - Earthquake/Subsidence/Landslide
- Services Failure
  - Electrical Supply Problem
  - Water Supply Problem
  - Supplier Failure
  - Storm/Atmospheric Condition
  - Flood/Tidal Wave
  - Earthquake/Subsidence/Landslide
- Mechanical Breakdown or Software Failure
  - Software Problems
  - Hardware Problems
  - Local Area Network Problems
  - Communication Problems
  - Air-conditioning Problems
  - Plague/Pestilence
- Accidental or Deliberate Destruction of Property/assets
  - Error
  - Accidental Damage
  - Fraud
  - Malicious Physical Damage/Sabotage/Arson
  - Malicious Logical Damage/Hacking
  - Robbery/Burglary/Theft
  - Legal Action/Seizure of Assets
  - Fire Detection/Protection Systems
  - Loss of Historical Data
  - Computer Hardware Problems
  - Communications Problems
- Personnel Problems
  - Inadequate/Inaccurate Documentation
  - Incompetence/Lack of Training
  - Staff Shortage/Loss of Key Staff
  - Neglect of Duty/Lack of Commitment
  - Breach of Confidentiality/Disclosure
  - Strike
  - Demonstration/Picketing/Occupation
  - Kidnaps/Hostage
  - Plague/Pestilence
  - Blackmail/Bribery
- Environmental/Facility-Wide Damage
  - Industrial Accident
  - Aircraft/Train/Boat/Vehicle Impact
  - Installation Building Defect
  - Change in/New Legislation
  - Police/Military Action
  - Act of Terrorism
  - Espionage
  - War/Breaking of Diplomatic Ties
  - Coup/Change of Government
  - Pollution
  - Radiation
- Storm/Atmospheric Condition
  - Earthquake/Subsidence/Landslide

such as team building, increased attention being paid to new strategies, and the creation of commitment to action.

Those who do attempt to address risk systematically in IS either do so in a specific way, identifying, usually, a partial list of risk sources to focus attention upon (see, for example, Robson, 1994), or adopt a comprehensive categorization approach, which attempts to cover everything (see, for example, Green, 1995) (Table 2). The latter is a more general approach to risk management, but may not allow the system developer to consider risk flexibly, associating particular sources of risk with each stage of risk management, in that impact rather than categorization may be paramount. The comprehensive approach is utilized by Avison and Horton (1992), who suggest IS failure may be due to factors classified as technical, human resource, environmental, organizational and management. Willcocks (1992) lists a number of reasons for failure in IS evaluation practice which may be equated to risk sources: concealment of full costs by budgeting practice; failure to understand human, organizational and knock-on costs; overstatement of costs; inappropriate measures; neglecting intangible benefits; failure to fully investigate risks; failure to devote evaluation time and effort; failure to take into account the timescale of likely benefits; and failure to create a strategic climate in which investment in IT can be related to organizational direction. Categorizations of this type are a useful start in addressing risk but there

are a number of dangers. Four, in particular, are worth noting: first, that categorization of risks may be a substitute for management of them; second, that such categorizations are not as comprehensive as they might appear; and, third, that the gap between general categories of risk and the identification of risks specific to a project may be hard to bridge. Finally, the existence of a set of categories may stifle open debate about risk sources peculiar to any one project.

Current risk management aids

Current attempts to provide support for risk management tend to come in the form of stages or add-ons to project evaluation techniques. Liang and Tang's (1991) solution is VAR analysis, which comprises value analysis, advantage analysis, and risk analysis. The last component includes assessment of the uncertainties of outcomes and classification of risk types: technological, obsolescence, financial, opportunity costs, implementation (employee/customer resistance), and strategic. In other approaches, risk management *per se* is not included, but risk, once identified, is reduced by other strategies. Tate and Verner (1990), considering systems development methods, conclude that risk management is not explicitly related to the choice of particular development strategies. Prototyping and incremental development is often used to reduce project risks, for example, by developing knowledge (presumably, of the system and its capabilities), by breaking the project into digestible bits, by reducing time between specification and delivery, and by reducing the impact of change requests. They identify generic risks applicable to software products such as late fixes, error prone products, uncontrollable products and poor communications. Project-specific risks include inappropriate or undefined requirements, schedule risks, user acceptance, data quality and personnel shortfall (inappropriate skill-mix, etc.). They believe that risks can be controlled by the use of incremental development, use of data-centred development methodology, use of 4GLs, and by employing a mix of in-house and external personnel.

Some research has also been undertaken in designing risk management support systems. Within BT (a telecommunications company), Whiting *et al.* (1993) suggest that the role of a feasibility study is to look at risks, these being categorized as overall, people, project size, project control, complexity, novelty and stability of requirements. Again, Otway and Haastrup (1988) write of the development of risk analysis interest initially focusing on quantifying risks to allow comparison, then on risk-benefits analysis which tries to equate risks and benefits in similar units, then on

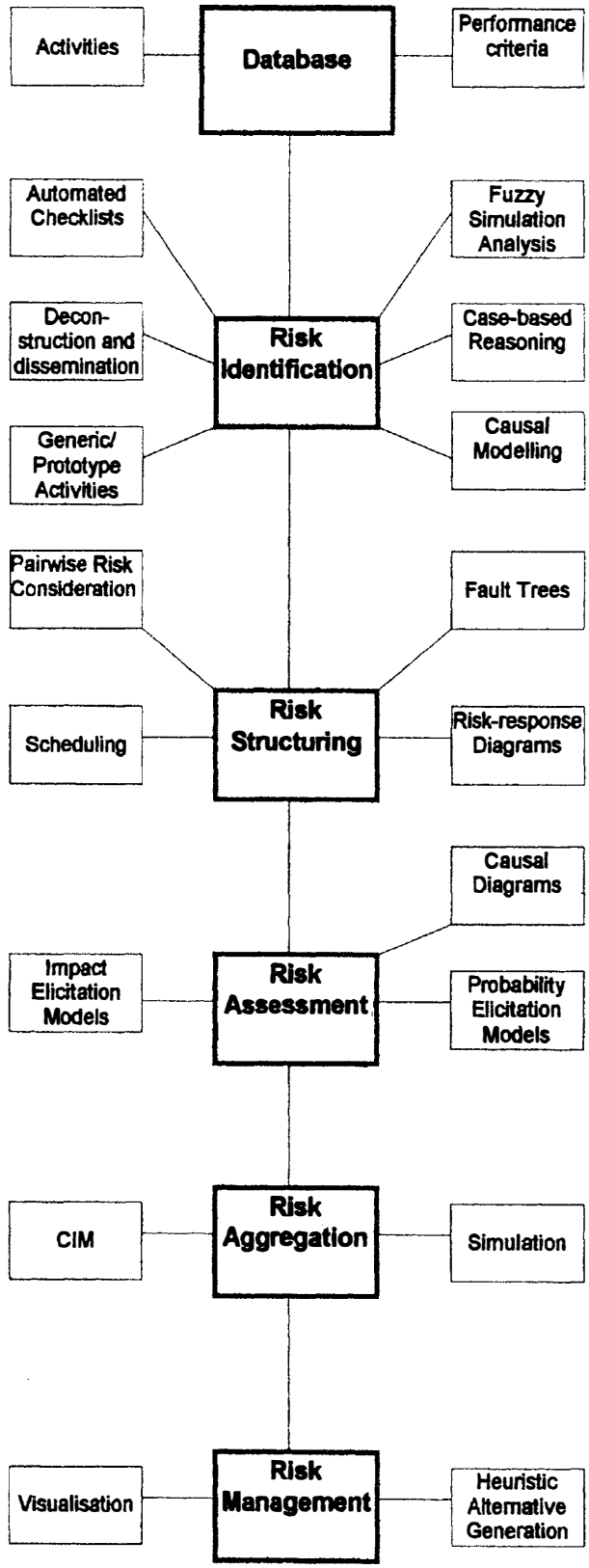

Figure 1 Conceptual schema of risk management DSS

risk communication which facilitates risk understanding, and finally on mediated conflict resolution where those subject to risks and those who either cause the risks or are in a position to mitigate them can mutually agree a policy. They describe their IRIMS system for risk analysis (initially for hazardous substances), which contains a database, simulation models of environmental impacts, risk analyses and optimization, and a user interface which is graphical. However, the system, at the time of writing, is a prototype/demo and the simulation models are based on pre-existing systems. Birch and McEvoy (1995) briefly review three other commercially available systems: RiskPAC, CRAMM and MARION. The first two are simple questionnaire-based systems, while the last is based on a database of past insurance claims. The authors go on to offer their own system, founded on models of process, information and technology, which aims to ensure that 'risk management becomes a discipline rather than an art'.

Von Winterfeldt (1988) suggests there are three approaches to a decision support system (DSS) for risk analysis – the operational research/management science (OR/MS) approach, decision analysis/multi-attribute utility theory (MAUT), and an artificial intelligence/expert system (AI/ES) route. In constructing a system, risk analysts may be conceived of as substantive experts or methodology experts, while risk managers may be strategists or technicians. Similarly, the affected groups may range from lay people to special interest groups, and the objectives for each group are clearly different. The OR/MS approach to risk management offers technical models of the process which generates risks, while multi-attribute utility theory would look at the decision maker's options, objectives, and uncertainties. Von Winterfeldt (1988) recognizes that different users will gain more or less from different approaches. For instance, a methodological expert gains most from a MAUT model and OR/MS techniques, while technical managers may find an AI/ES approach most useful. This work cautions a risk DSS developer that issues of complementary intelligence – the relative abilities of the user and system – are important in building such a tool.

Further, any risk-based DSS must take into account representation of the reasoning strategies of experts, which are often conceptualized as scenarios. Jungermann and Thuring (1993) suggest cognitive activity in constructing a scenario includes: activation of relevant problem knowledge in the expert's memory; construction of an internal model of the domain that maps its important features; drawing of inferences by 'running' of the mental model; and, composition of scenario knowledge by selecting the inference required by the task and/or the experts' intention. However, decision processes need to be thought of as mechanisms for generating knowledge not simply relying upon it.

In relation to IS projects, the ASA (1984) found that 41% of their members agree that they 'find it difficult to tell computer people what [they] need'. The problems these individuals highlight include: dependence on technical experts; lack of training; meeting needs/improving constraints; co-ordination of data and systems; and, security risks. Each of these might be addressed by the DSS, as outlined below, the prime purpose of which is to turn *ad hoc* into programmed decisions at the individual level. Yet, for Hotterstein and Dean (1992), risk management strategies may not be oriented to risk reduction – they are tools for successfully managing a project given its risk profile.

The following sections outline a comprehensive approach to risk management and detail the components of a DSS to support the risk management process. Its intention is to be comprehensive rather than partial, and to allow conceptualization of risks (particularly to IS) at a broad level. Figure 1 shows the resultant system which is discussed in depth below.

Risk management

The purpose of risk management is to select a course of action which provides an acceptable balance between likely benefits and exposure to risks. Generally, risk management assumes that activities take place in environments in which uncertainties of all kinds are prevalent, but in which efforts to gauge uncertainties and to plan for them are worthwhile. A simple case is that of trading off risk and return, in which the problem is to select a course of action which offers an attractive expected return, while reducing the possibility of an unattractive return to an acceptable level. Frequently, a higher expected return can only be obtained at the expense of increasing the possibility of an unattractive return. In its simplest form, risk management is the process of selecting the course of action that corresponds to an acceptable balance. However, at a more sophisticated level, risk management involves the identification of ways in which the trade-off between risk and return might be altered. For example, a small up-front expenditure, effectively reducing expected return by a small amount, might reduce exposure to risk dramatically. It is also not uncommon to be able to identify measures which can reduce risk exposure while not reducing expected return.

Most of the techniques and methods of management science that explicitly or implicitly recognize and

attempt to deal with uncertainty may be characterized as risk management techniques. However, there also exist several approaches which primarily address risk management in a variety of contexts (see, for example, those described by Ansell and Wharton, 1992).

One particular area for which risk management approaches have been developed is the management of projects. At the same time, the project is becoming increasingly commonly regarded as a suitable paradigm for much management activity. Gilbreath (1988) relates the 'projectization' of work to the turbulence of the work environment:

> In times of change the project orientation dominates all operational frameworks. The logic supporting this conclusion is inescapable, and we see it manifested with great frequency by business examples all about us. Perceptive managers know, then, that in times of change, for today and tomorrow, they will more often than not be managing projects. (Gilbreath, 1988, p.3)

In the project paradigm, operations are considered as projects, for each of which there is a management team. Such projects have life cycles, and involve planning, development and termination. Risk management within an organization may be considered in terms of risk management within the component management projects, and within the overall programme management of the portfolio of management projects.

Given that IS development and construction has long been carried out in project form, applying risk management to IS development may be based upon conceptualization of IS in terms of projects. The development of an integrated suite of information systems might be a portfolio of projects with each application a project in itself.

Effective project risk management implies a number of contributory activities. The active management of risk is facilitated by risk analysis, which is constituted of a number of component activities, including: the identification of risks to which a project is subject; the structuring of the inter-relationships between the risks; the assessment of the magnitude or seriousness of the risks; and the aggregation of the combination of risk assessments into an overall assessment.

Though inter-related, the four risk analysis activities, together with risk management, are distinct, and each has particular features. Each requires particular skills, and benefits from particular kinds of technique. Further, there is scope for support for the activities from appropriately designed decision support systems. The following sections of the paper examine the five activities in more detail, and consider the scope for DSS support.

Risk identification

In identifying the risks to which a project is subject, the fundamental problem for risk managers is to generate a list of risks which is complete: anything that might go wrong has been included in it. Completeness does not indicate that the risk list is stable, just that all potential risks at any point have been included. Much risk identification is undertaken by managers and associated staff without any aiding techniques: they rely solely on experience, intellect and imagination to generate a comprehensive risk list, though techniques such as brainstorming may assist. The most commonly used aid to risk identification is the checklist: a list of possible risks which the user may employ to generate a project risk list. Checklists may take a variety of forms. They can be quite general, simply suggesting a number of areas in which risks may be present. They can be highly specific to a particular project or class of projects. They may be expressed in terms of causes or goals. Checklists are generally used as a foundation for risk identification, and are rarely regarded as fully replacing the expertise of personnel.

A number of risk analysis techniques, for example SCERT (Chapman, 1992), rely, in part, on participants envisioning and developing scenarios which describe sources of risk or responses to identified risks. In the main this process is carried out in an informal way: it relies on the experience of the analyst and user to perceive possible scenarios.

It is relatively easy to generate a checklist of risks at a highly general level. For example, in Jenkins' (1990) list of risk categories in defence procurement, it is hard to imagine a risk which cannot be allocated to at least one of his eight categories. However, the problem with general checklists is that they may not be much help in assisting analysts to identify the specific risks to which their project is actually subject. More specific checklists clearly offer more help with this, but suffer from the problem that they are rarely fully comprehensive. Specific checklists tend to be generated from past projects of a similar nature to the one under current consideration. However, similarity tends to be in the eye of the developer and, indeed, characterizing a project, or part of a project, as similar to one experienced previously may be a significant source of risk in its own right. Ballantine *et al.* (1995) consider the issue of similarity in IS projects, pointing out its multidimensional and thus problematic nature. A number of techniques for assessing similarity exist, such as case-based reasoning and fuzzy approximate reasoning. Ribeiro *et al.* (1995) describe a system which incorporates these elements in a DSS to address uncertainty. The purpose of case-based reasoning is to store past cases or exemplars and to explain new cases by

reference to these. The main problem is to assign importance to attributes and components of the context-domain problem. Often these attributes are linguistic rather than numeric. Approximate reasoning allows inferences to be performed under uncertain conditions, and while the traditional approach has been probabilistic, a fuzzy approach offers greater flexibility (Ribeiro *et al.*, 1995).

A number of practices can be used to reduce the likelihood of omitting risks:

(1) Using documentation from previous risk analyses in similar areas as an input to the analysis.
(2) Including in the analysis team personnel with previous experience of risk analysis and management in the current project area.
(3) Including in the analysis team individuals with different skills, expertise and points of view.
(4) Duplication of an analysis, or critical parts of it, by an independent analysis team.
(5) Adoption of brainstorming-type approaches to risk identification.

Successful risk identification requires a clear understanding of project success criteria. The standard general criteria are costs, duration and performance; other, more specific criteria may be appropriate to specific projects. Though there is often an implication that all criteria may be incorporated in one overall criterion – usually cost – in practice, it is more effective to work with criteria which have some operational meaning in the context of the project, such as the duration of development or the quality of service, for example. The issue is exacerbated when, as is frequent, several different stakeholders are involved. Different criteria may be associated with different stakeholders. For example, a system developed by a public sector service organization for use by the public will have two obvious stakeholders, the organization and the users, and it would be naïve to imagine that the criteria which each possesses can be usefully combined into a single overall criterion.

A risk is a threat to one or more project success criteria, and makes little sense unless it is, at least implicitly (but preferably explicitly) defined as such. Particularly at the strategic level, IS developers may not be fully aware of the organizational objectives from which success criteria are effectively derived (Powell, 1994), but, rather, assume or interpret them from observed organizational behaviour. Thus, there may be incompatibility between actual organizational objectives and those upon which the IS developers build the system. Use of project teams will widen the input to determining objectives but it does not alleviate the problem of organizational objectives being tightly controlled by the top management team and not communicated. Further, if organizational strategy is not fully formed, there may not be explicit objectives to guide IS development.

Another prerequisite of risk identification is that the bounds of the risk management exercise have been identified, so that it is possible, in principle, to identify whether or not a particular risk falls within the scope of the exercise. The dangers of insufficient boundary identification are that risks beyond the boundary are considered or that risks are ignored because they are supposed to be beyond the bounds of the exercise, when in fact they are not. The former danger is a time-waster; the latter is potentially far more serious.

The decision support system outlined in Figure 1 facilitates risk identification and reduces its inherent dangers in a number of ways. The first is by the provision of risk checklists. Such checklists may range from the specific to the general. They may be integrated into a hierarchical structure, with particular risks being associated with particular components of a generic project structure. For example, such a structure is implicit in the technical risk assessment methodology (TRAM) described by Klein and Cork (1996). The checklist module of the DSS may range from the relatively passive, which simply provide a sequence of risks in a conveniently structured form, to the relatively active, which interact with the user and query the project context. The potential exists for the DSS to be developed into a form of expert system which puts together a risk list for a specific project, informed on the one hand by system-based expertise concerning risks and projects generally, and on the other by the specific knowledge of the users. This might use the case based and approximate reasoning processes outlined above.

A second tool is the provision of causal modelling methods. A cognitive mapping approach (Eden *et al.*, 1983) to risk modelling may be useful, enabling explicit articulation and exploration of the connections between overall objectives, success criteria, risks, and the conditions which exacerbate or moderate the risks. An example of the use of cognitive mapping in a risk identification context is provided by Klein (1993), demonstrating how the approach might be used to develop an understanding of the inter-relationships and trade-offs of uncertainties between project criteria of duration, cost and quality in a software project. General cognitive mapping software has existed for some time (see Eden *et al.*, 1983) though software dedicated to the elicitation and structuring of project risk needs to be developed.

Third, the use of DSS enhances the opportunity for pluralist analysis. Jackson and Carter (1992) emphasize

the need for 'deconstructing the texts' of risk analysis contexts, and hence permitting a multiplicity of interpretations which may lead to a more comprehensive identification of potential risks. Jackson and Carter (1992) give three examples of risk perception failure, the sinking of the Titanic, the Challenger space mission and the Hixon railway crossing accident. They demonstrate how deconstruction might have assisted. A DSS which facilitates the dissemination of a project description and the canvassing of a wide range of views as to risks to which the project is exposed, while removing the authority of any single 'correct' view, may result in more comprehensive risk identification. The use of multi-participant group DSS would enable pluralist analysis.

A final component, which has applicability in other modules too, is the use of generic or prototype activities. Klein *et al.* (1994) describe the use of prototype activities. This approach recognizes that all the activities of a project, or a substantial number of them, can be considered as variations on a prototype activity upon which detailed analysis is carried out. Perturbations of this analysis appropriate to each of the actual activities are then identified. A database of such prototypes invoked by the case-base or fuzzy approximation module to identify feasible ones would have merit.

Risk structuring

Risk structuring is the process of characterizing the inter-relationships between risks. Such inter-relationships include correlations (positive and negative) between the probabilities of risks occurring and between the impacts of risks if they do occur. Such correlations may arise because of underlying influences which affect a number of risks. For example, a wide variety of potential problems with a software development project might all be causally related to, among other influences, the degree of inexperience of the developers. In such cases, causal modelling may be valuable in identifying potential underlying causes. Alternatively, direct correlations between risks may be identified without explicitly invoking underlying causes. For example, a delay in the delivery of hardware components might be reckoned to increase the likelihood that the components will be faulty.

Some problems may only occur when particular combinations of conditions are present. For example, power supply problems to a system may only occur when both main and back-up power supplies are interrupted. This kind of risk may be usefully modelled using fault tree analysis, which provides a structure for representing the logic of such relationships and determining their implications.

Risk structuring may also involve classification of risks according to the stage of the project which they threaten (e.g., which component phases or activities) and their seriousness (e.g., minor or major). Another important characteristic of risk is the kind of responses that may be developed to deal with them. In some cases, the effects of several different risks may be mitigated by a single, general, response: for example all kinds of delays in early stages of a project may be responded to by increasing personnel at a later stage. Other risks may require quite specific specialized responses. Chapman (1992) uses risk-response diagramming to capture the logic of these kinds of relationships.

Clearly, risk structuring is closely related to risk elicitation. Much of the information that is generated in the course of risk elicitation is directly related to risk structuring, and, indeed, the process of risk structuring tends to elicit further risks. Systematic manual analysis has the disadvantage that elicitation and structuring can involve lengthy reiteration of generated information. One important benefit of the use of DSS to support consideration of risk would be the increased ability of users to integrate elicitation and structuring activities. Such a system would allow the development of a set of diverse but related models: a general PERT-style schedule indicating activities, risks and responses (i.e. a risk-response diagram), supplemented where appropriate by causal diagrams, fault trees and similar models. Ansell (1992) demonstrates the use of fault trees in a pipe flow example.

A more specific aid might concentrate on the identification of correlations between risks. At its simplest, this would involve pairwise consideration of all risks, and would invite the user to indicate degree of correlation (qualitatively or quantitatively) of probabilities and impacts. Such analysis would both inform and be informed by causal modelling. In practice, it is frequently the case that considerable uncertainty is attached to estimates of correlation between risks, and such uncertainty needs to be retained in the recording of correlations.

Risk assessment

Assessment of the seriousness of risks may be either qualitative or quantitative. The distinction between the two modes is rather less than might naively appear: qualitative assessments can be regarded as fuzzy quantitative assessments (see, for example, Kangari and Riggs, 1989).

A standard way of describing the magnitude of risk is in terms of a probability distribution of the

variable or criterion of interest: for example, a distribution describing the probability that the cost of a particular activity will overshoot (or undershoot) by particular amounts. This kind of description clearly lends itself to quantitative assessments. In practice, when making more qualitative assessments, assessors frequently find it easier to conceptualize a risk in terms of two measures: the probability that the risk will occur, and the impact of the risk if it does occur. Each measure may be characterized by a qualitative scale, for example, low, medium or high.

Quantitative evaluation of all risks, even if feasible in principle, is likely to be impractical. Therefore, many risk analysts tend to recommend initial qualitative risk assessment, followed by selective quantitative risk assessment of those risks seen to be potentially the most serious.

Estimation of both probabilities and impacts is fraught with difficulties. The problems of eliciting probabilities from people are well-documented: initial qualitative estimation reduces these problems (by fuzzifying the judgement scale) but does not actually eliminate it. The problems of eliciting impact data are similar. Various techniques have been suggested for assisting with these types of elicitation processes. These techniques tend to be straightforward conceptualization aids, such as the probability wheel for subjective probability elicitation: a disc with a pointer, in which the size of a sector of the disc is adjusted until the subject is indifferent between betting on a spun pointer coming to rest in the sector and the event of interest occurring. Goodwin and Wright (1991) review a number of such aids; most lend themselves to being implemented as part of a DSS. DSS would support risk assessment by implementations of one or more probability and impact elicitation methods.

All elicitation techniques, however, have their pitfalls and flaws. There is no generally recognized reliable way of eliciting subjective probability and impact data from people. At a deeper level, it is not even agreed as to what such a process might be or how its reliability and success might be judged. The problem is compounded because in most cases, such data is elicited from a number of individuals rather than a single person, and is frequently informed by historical data: in both cases, the issue of how data are combined must be confronted.

It is worth noting that often user confidence in elicitation of probabilities and impacts is raised by consideration of the components of a particular risk. Thus, it may be appropriate to refer back to fault trees and causal diagrams relating to particular risks, developed during risk identification and structuring, and retained by a DSS.

Risk aggregation

Risk aggregation is the process of combining risk assessments into an overall assessment of risk. Many tools exist for this purpose: most are based on Monte Carlo simulation techniques, but some are based on other techniques, and are applicable in relatively specialized circumstances (such as Chapman and Cooper's CIM technique, 1983). These two are used as examples in the risk aggregation module of the DSS in Figure 1.

The scope for developing systems which aggregate risk is still large. Specialist systems which are capable of aggregating risk with respect to particular criteria (e.g., cost and time) or for particular subsets of risks (e.g., those related to a particular activity) are valuable. Sensitivity testing is also valuable: for example, testing assumptions about the magnitudes of particularly serious risks, and concerning correlations between risks. Experience suggests that thorny problem of estimating the degree of correlation between risks may sometimes be vanquished by demonstrating, at the aggregation stage, that criteria are relatively insensitive to quite dramatic changes in correlation assumptions.

Risk aggregation is a process which, except in the simplest of cases, requires some kind of automation. The need is to enable the user to be able to control the aggregation process and test assumptions relatively easily and quickly. There is scope for improvement in the flexibility and ease of use of some of the standard software (often spreadsheet add-ons) used for aggregation purposes.

Risk management

In the general sense, risk management is the entire process of actively considering risk in a project context. In a more specialized sense, it is the process of using a risk analysis to make decisions concerning the project that result in an acceptable exposure to risk, while still achieving the aims of the project. It has been argued that risk management should not be regarded as an 'add-on' to project management, but as a central and integral part of the project management process: the goal of achieving acceptable risk exposure is part of the overall project aims.

Risk management (in the specialized sense) is informed by risk analysis. Therefore, to carry out risk management, a model of project risk that can be comprehended by managers is required. There are strong arguments (Klein, 1994) for basing this model on a visual framework. Thus, a DSS that is able to provide an iconic, or semi-iconic model of project risk

would be valuable. This concurs with the findings of Otway and Haastrup (1988) although they point to the problem of sophisticated graphical interfaces being accorded spurious accuracy by the system users.

Risk management involves the development and testing of alternative project management decisions in terms of risk exposure. Managers tend to develop alternatives on an *ad hoc* basis. However, complex projects invite the development of a more formal set of heuristics for trading-off risk exposure and the achievement of project criteria, analogous to the kinds of heuristics used to manipulate and smooth resource allocation in PERT. A set of such heuristics, when developed, would constitute an expert system. Incorporated and implemented within the DSS, these rules could considerably facilitate the process of risk management.

Conclusion

The tendency for information systems projects to fail or not to perform to expectations makes imperative the need to manage risk as an integral part of project management. As the paper indicates, there have been some developments in this direction. This paper has, however, demonstrated that scope exists for an integrated project risk management DSS for IS projects based upon the well-articulated principles of general project risk management. Such a DSS combines a number of support activities within a modular, interactive framework (Figure 1). Underlying such a DSS would be a model of project risk. The components of the model would be:

(1) The project, its activities, and its performance criteria.
(2) The risks to which the project is subject, their probabilities, and their impacts.
(3) The interrelationships between risks, their causal structure and underlying causes.
(4) The response to risks that may be made.

The benefits of the DSS-based risk management tool are the specific ones already identified in the body of this paper. Others, however, include more general features such as consistency and formalization, the ability to develop models which would allow simulation, prediction and control, the use of prototypes (Klein *et al.*, 1994) and the incorporation of user preferences for components such as attitude to risk. In addition, Willcocks and Griffiths (1995) suggest four key aspects which need to be considered as the starting point for controlling risk: governance – the organization of stakeholders, project management – balancing top-down and bottom-up, market need/economic survival as a motivator, and learning.

The system described in this paper allows consideration of the project management element, assists learning and may have an impact on governance via formalization of the process. Economic survival should flow from better consideration of the other aspects.

References

Ansell, J. (1992) Reliability: independent risk assessment, in *Risk: Analysis, Assessment and Management*, Ansell, J. and Wharton, F. (eds) (Wiley, Chichester) pp. 105–22.

Ansell, J. and Wharton, F. (eds) (1992) *Risk: Analysis, Assessment and Management* (Wiley, Chichester).

Australian Society of Accountants (ASA) (1984) *Survey on the Use of Information Technology by Accountants*.

Avison, D. and Horton, J. (1992) *Evaluation of Information Systems*, University of Southampton Working Paper.

Ballantine, J., Galliers, R. and Powell, P. (1995) Daring to be different, capital appraisal and technology investments in *Proceedings of the 3rd European Information Systems Conference*, Athens, Greece, Doukidis, G., Galliers, R., Jelassi, T., Krcmar, H. and Land, F. (eds) pp. 87–97.

Ballantine, J., Bonner, M., Levy, M., Martin, A., Munro, I. and Powell, P (1996) The 3-D Model of Information Systems Success: the Search for the Dependent Variable Continues, *Information Resource Management Journal* (forthcoming, October).

Birch, D. and McEvoy, N. (1995) Structured risk analysis for information systems, in *Hard Money – Soft Outcomes*, Farbey, B., Targett, D. and Land, F. (eds) (Alfred Waller, Henley) pp. 29–52.

Chapman, C.B. (1992) A risk engineering approach to risk management, in *Risk: Analysis, Assessment and Management*, Ansell, J. and Wharton, F. (eds) (Wiley, Chichester) pp. 5–39.

Chapman, C.B. and Cooper, D.F. (1983) Risk engineering: basic controlled interval and memory models, *Journal Operational Research Society*, **34**, 51–60.

Eden, C., Jones, S. and Sims, D. (1983) *Messing About in Problems* (Pergamon, Oxford).

Gilbreath, R.D. (1988) Working with pulses, not streams: using projects to capture opportunity, in *Project Management Handbook*, Cleland, D. and King, W. (eds) (Van Nostrand Reinhold, New York).

Goodwin, P. and Wright, G. (1991) *Decision Analysis for Management Judgement* (Wiley, Chichester).

Green, J. (1995) *Business Resumption Planning*, Unpublished MSc Thesis, University of Warwick.

Hotterstein, M. and Dean, J. (1992) Managing risk in advanced manufacturing technology, *California Management Review*, 112–26.

Harris, S. and Katz, J. (1991) Firm size and the IT investment intensity of life insurers, *MIS Quarterly*, **15**(3), 333–52.

Harrison, E. (1992) Some factors involved in determining strategic decision success, *Journal of General Management*, **17**(3), 72–87.

Jackson, N. and Carter, P. (1992) The perception of risk, in *Risk: Analysis, Assessment and Management*, Ansell, J. and Wharton, F. (eds) (Wiley, Chichester) pp. 41–54.

Jenkins, N. (1990) Guide-lines for risk assessment and risk management in MoD procurement programmes, in *Risk and Risk Analysis: the Royal Aeronautical Society Seminar*, London, July (Royal Military College of Science, Shrivenham).

Jungermann, H. and Thuring, M. (1993) The labyrinth of experts' minds: some reasoning strategies and their pitfalls, *Annals of Operational Research*, **16**, 117–30.

Kangari, R. and Riggs, L.S. (1989) Construction risk assessment by linguistics, *IEEE Transactions on Engineering Management*, **36**, 126–31.

Kemerer, C. and Sosa, C. (1991) Systems development risks in strategic information systems, *Information and Software Technology*, **33**(3), 212–23.

Keyes, J. (1989) Why expert systems fail, *AI Expert*, November, 50–3.

Klein, J.H. (1993) Modelling risk trade-off, *Journal Opl Research Society*, **44** 445–60.

Klein, J.H. (1994) Cognitive processes and operational research: a human information processing perspective, *Journal Opl Research Society*, **45**, 855–66.

Klein, J.H., Powell, P. and Chapman, C. (1994) Project risk assessment based on prototype activities, *Journal Opl Research Society*, **45**(7), 749–57.

Klein, J.H. and Cork, R.B. (1996) An Approach to Technical Risk Assessment, in preparation.

Krumm, F. and Rolle, C. (1992) Management and application of decision and risk analysis in Du Pont, *Interfaces*, **22**(6), 84–93.

Liang, T-P. and Tang, M-J. (1991) VAR analysis: a framework for justifying strategic information systems projects, *Database*, **23**(1), 27–35.

Mowshowitz, A. (1976) *Information Processing in Human Affairs* (Addison-Wesley, Reading, Mass).

Otway, H. and Haastrup, P. (1988) Designing risk management support systems, *Annals of Operational Research*, **16**, 439–46.

Powell, P. (1994) Fuzzy strategy, crisp investment, in *Hard Money – Soft Outcomes: Evaluating and Managing the IT Investment*, Farbey, B., Targett, D. and Land, F. (eds) (Alfred Waller, Henley-on-Thames) pp.173–92.

Price Waterhouse (1989) *Information Technology Review*, Grindley K. (ed) (Price Waterhouse, London).

Ribeiro, R., Powell, P. and Baldwin, J. (1995) Uncertainty in decision making: an abductive perspective, *Decision Support Systems*, **13**, 183–94.

Robson, W. (1994) *Strategic Management and Information Systems* (Pitman, London).

Ruohonen, M. (1991) Stakeholders of strategic information systems planning: theoretical concepts and empirical examples, *Journal of Strategic Information Systems*, **1**(1), 15–28.

Stahl, M. (1989) *Strategic Executive Decisions* (Quorum Books, New York).

Tate, G. and Verner, J (1990) Casestudy of risk management, incremental development and evolutionary prototyping, *Information and Software Technology*, **32**(3), 207–14.

Vitale, M. (1986) The growing risks of information system success, *MIS Quarterly*, **10**(3), 327–34.

Von Winterfeldt, R. (1988) Expert systems and behavioral decision research, *Decision Support Systems*, **4**, 461–71.

Whiting, F., Davies, J. and Knul, M. (1993) Investment appraisal for IT systems, *BT Technology Journal*, **11**(2), 193–211.

Wildemann, H. (1988) Analysis and evaluation of basic strategies in investment planning for modern flexible technologies, *Annals of Operational Research*, **16**, 447–64.

Willcocks, L. (1992) Evaluating information technology investments: research findings and reappraisal, *Journal of Information Systems*, **2**(4), 243–68.

Willcocks, L. and Griffiths, C. (1995) Evaluating risk in major IT projects, in *Hard Money – Soft Outcomes*, Farbey, B., Targett, D. and Land, F. (eds) (Alfred Waller, Henley) pp. 29–52.

Willcocks, L. and Margetts, H. (1994) Risk assessment and information systems, *European Journal of Information Systems*, **3**(2), 127–38.

Bibliography

Philip Powell is Director of the Information Systems Research Unit, Warwick Business School and an ICAEW Academic Fellow. He has authored books on information systems and financial modelling, and has published in Omega, JORS, Accounting and Business Research, Information Systems Journal, British Journal of Management, Organizational Computing, Journal of Strategic Information Systems, Journal of Management Systems, and Decision Support Systems amongst others. He is associate editor of the Information Systems Journal, the Journal of Strategic Information Systems and OR Insight. His main interests are the organizational impacts of IS and IT, especially decision support systems and expert systems, and the ways such systems might be evaluated throughout the project cycle.

Jonathan H. Klein is a Senior Lecturer in the School of Management at the University of Southampton. His research interests include risk analysis and management, the organizational context of information systems and management cognition. He has published in Omega, the Journal of the Operational Research Society, Information and Software Technology, the European Journal of Operational Research, Investigação Operacional and the Journal of Management Systems amongst others. He is associate editor of OR Insight and UK editor of International Abstracts in Operations Research. He has undertaken consultancy for a variety of organizations, notably in the area of risk analysis and management.

Address for correspondence: P.L. Powell, Information Systems Research Unit, Warwick Business School, University of Warwick, Coventry CV4 7AL, UK.