Identifying risks during information system development: managing the process

Stuart Maguire
Lecturer in Information Systems, Sheffield University Management School, Sheffield, UK

Keywords
Risk management, Information systems, Contingency planning

Abstract
Developments in information and communications technology have allowed many organisations to implement systems that directly link to customers and suppliers. In a number of instances, this has allowed them to gain a competitive advantage over their business rivals. The changeover to a new information system may appear seamless to the customer. The general public should not be disadvantaged by the implementation of a new system in the public sector. The tight coupling of systems, especially with customers, puts extra responsibility on information system developers to try and ensure a smooth transition from the old to the new system. Failure to do this may result in the customer being unfairly penalised and may result in subsequent loss of business. This paper attempts to show that there are many areas of potential risk within the process of information system development (ISD) and these need to be carefully analysed and managed. It also reveals that certain popular risk management methodologies do not reflect the risk elements identified within the ISD process.

Introduction
Further developments in information and communications technology have given many organisations the opportunity to derive direct business benefits through linking with their customers. The success of this interaction is dependent on the effectiveness of the information system(s) that is being used. Any breakdown in the relationship between the customer and supplier of services may lead to subsequent loss of business. A critical time in this relationship is when the provider of services decides to upgrade their information systems. The firm developing the system is hoping for a seamless implementation and the customer expects that there will be no break in business transactions. However, there are many opportunities for things to go wrong during the development of a new information system and organisations take a number of risks when embarking on this course of action.

Most information systems are implemented with the anticipation of being successful though there appears to be an increasing caseload of examples where systems go live and then have negative consequences for those people who use them. This may be increasingly significant when systems are implemented in areas that have a direct influence on business success. The use of fast-tracking techniques, and the tighter coupling between customers and suppliers enabled by improved information and communication technologies, may actually increase the risks of such developments.

This article attempts to show that:

- there is a need for risk analysis and risk management methodologies to reflect these issues.

The article will review the current literature on risk and security, trying to identify the issues seen as critical to successful information system implementation. The article focuses on an information system that has been rolled out nationally. The system replaced another computer system that was working successfully for both users and customers. This article will attempt to identify through the use of this case study the potential problems faced by organisations and how there is a need to develop a risk management methodology to address some of the key weaknesses in the system development process.

The project in question was not underpinned by any risk management as it was assumed the system development would be successful. In retrospect an industry-standard risk management methodology, the Central Computing & Telecommunication’s Agency risk analysis and management methodology (CRAMM), is applied to see whether it would have made any difference to the outcome of the project. Various areas of the system development are highlighted including:

- project management;
- system design;
- hardware and software issues;
- use of system development methodologies;
- capabilities of the system;
- integrity and security;
- training; and
- the business environment.

Background
Many information system developments involve organisations in the outlay of several...
millions of pounds. For many organisations it may be their highest capital outlay in a given financial year. It is usually anticipated that this investment will derive a return that will accrue to the organisation. This will normally be outlined in the original cost-benefit analysis for the system or possibly in a more detailed business case. The risk factor attached to the system development process has not always been seen as an important area of discussion. Organisations hope to implement systems successfully while still undertaking their normal business processes. However, new systems are not implemented in a vacuum and many authors agree that the first step in developing a business continuation plan is to carry out a risk assessment. This should be more than identifying the potential risks to the organisation’s computer systems (Robson, 1997).

Business impact analysis should be able to identify loss of revenue; loss of customers; business credibility; and an inability to recover. Many firms will be aware that this business credibility may include not only customers and suppliers but also other business partners who are influenced by a failure of systems. Organisations should consider every option in trying to take some of the risk out of the system development process.

A number of high profile IT failures may put risk management higher up the agenda of prospective project management teams. This is not a recent phenomenon as the National Audit Office’s examination of a selection of computer projects planned and developed mainly between 1990 and 1999 identified poor standards of project management, with insufficient attention paid to users’ needs. The following issues were highlighted: incomplete feasibility studies; loose contractual arrangements; inadequate planning; weak control; and absence of post-implementation reviews (National Audit Office, 1999).

When these failures have direct external consequences for the organisation further pressure will be placed on system developers to try and take the risk out of IT implementation. It is clear that risk assessment and management is of critical importance for many IT investments (Ward and Griffiths, 1996). The risk of computer systems failing requires organisations to put in place countermeasures to combat the effects of an interruption to business. The Computer Services Association defines a business disaster as:

any accidental, natural or man-made malicious event which threatens to or does disrupt normal operation or service for a sufficient time to affect significantly, or to cause failure of, the organisation (cited in Home Office, 1997).

Other writers view a disaster as being the failure to access mission critical information for significant periods (Toigo, 1996). In many instances business disasters may be personal to every individual organisation. However, business continuity plans should concentrate on mission-critical or core systems (Fitzgerald, 1994) where failure equates directly to lost business. Many companies do not have business continuity plans in place even though the relevance and importance of risk management procedures may never have been more significant (Renkema, 2000). The purpose of these plans should be to ensure the business survives rather than just the recovery of their computer systems (Edwards, 1994). Organisations should be able to absorb the effect of a system disruption on its business. Varcoe (1994), viewed risk planning as, carrying out a risk assessment; undertaking a business impact assessment; and preparing a business continuity plan. Heng (1996), viewed the approach as, performing an impact analysis; determining processing requirements; and, finally, risk analysis. Karakasidis (1997), went into more detail about raising awareness of the business recovery process:

1. define the objectives, scope and success factors of the business continuity process;
2. manage the development of all required business recovery procedures for core business activities;
3. support business recovery testing and maintenance; and
4. support a business recovery awareness programme.

Point four should be communicated to senior management so that they can see the value of the effort expended in this area (Moore, 1995). Many organisations find it difficult to admit that there may be potential problems with future system developments. The following section introduces risk assessment as a way of isolating system-related problems.

### Risk management in information systems

It appears that many organisations are taking a risk with the development of their information systems. In essence they are acting without regard to the business risks involved. The majority of writers in the area of information systems view risk as something to be addressed once the system is up and running, i.e. fire, fraud, computer

---

**Stuart Maguire**  
Identifying risks during information system development: managing the process  
failure and unauthorised access (Awad, 1988; Zwass, 1992; Hussain and Hussain, 1997; Curtis, 1998; Laudon and Laudon, 1998; Simon, 2001). This appears to align with the focus adopted by many current risk management methodologies.

The significant increase in the number of distributed systems environments, with nearly every employee having access to systems, has made the security issue more critical (Zwass, 1997). Systems auditors may be interested in safeguarding assets, data integrity, system efficiency and effectiveness (Weber, 1998). It would be wrong to assume that just because a risk assessment can be undertaken that it can then be controlled (Laudon and Laudon, 1998).

However, there are many risk factors to consider before the information system goes live. Some writers believe that the implementation process is as important for IS success as the information system itself (Kwon and Zmud, 1987). There are many things that can go wrong during the process of system development and organisations should be simultaneously attempting to reduce risk and increase security during system implementation. The integrity of organisational information systems needs to be seen as a high priority. It will also question whether current risk management methodologies, i.e. CRAMM, are relevant to the wider process.

One downside of adopting an external methodology is that internal resources are expended in learning and understanding it thoroughly (Dorey, 1994). It may also fail to integrate into the organisational culture of the organisation (Edwards, 1994).

Risk assessment should be used at the start of a project, and at least before system design, to determine the level of risk and to formulate plans for reducing that risk (Bocu et al., 1999; Curtis and Cobham, 2002). It may just be necessary to ensure that the project is organised so that it is completed within time and cost constraints (Schultheis and Sumner, 1992). Security for the project can then be provided by the systems computer steering committee. This group will have the authority to establish the overall direction of the organisation’s information systems (Scott, 1986). The technology can then be implemented to try and avoid all unnecessary risk (O’Brien, 1999).

However, the measurement of potential computer threats may be dependent on historical information that does not exist. For developments using new computer platforms there may be major problems with the uncertainty surrounding known metrics (Madnick, 1987; Avison and Fitzgerald, 1995). Using heuristic approaches to analyse risk gauge can only be successful if the project team has the necessary experience to undertake valid “scenario-building”. It is also crucial that the project team admit that there may be a risk in certain areas (Curtis and Cobham, 2002).

The extra pressure placed on information systems resources has made this investment often large and risky (Jackson et al., 1997). Many organisations have totally integrated systems that also link with customers and suppliers. The financial consequences of system failure make it necessary to develop a strong link between risk and cost-benefit analysis (Remenyi, 1991; Curtis and Cobham, 2002). This could be an important part of the strategic planning process. Risk could then be assessed under different headings:

- risks associated with new technology;
- risks associated with project size;
- risk of failure, i.e. the damage that can be done to the firm if the project fails.

If a project is ambitious, i.e. a business process re-engineering (BPR) project, the risk of failure may increase proportionately (Stair and Reynolds, 1999). The success of the system development may be dependent on the organisation’s ability to manage change (Brooke and Maguire, 1998). If the system can be copied quickly by competitors there may be financial risks in investing too heavily in a new project (Hicks, 1993). In a particular business sector it may be difficult to sustain even a short-term competitive advantage. It may be difficult to successfully implement and maintain profitable information systems. However, without systems innovation an organisation could find itself at a strategic disadvantage. Before investing in a new information system management should assess the company’s position in relation to:

- monetary resources;
- technological sophistication; and
- organisational flexibility (Kemerer and Sosa, 1991).

Basic questions may need to be asked, i.e. does the firm have enough capital to complete the information systems project? Is the firm a leader or follower in relation to technological innovation? Can the firm react quickly to environmental changes? An organisation’s information systems may require constant and continual innovation (Hicks, 1993). The success or otherwise of a firm’s introduction of an information system may depend on understanding the complexities of its internal and external environments (Kwon and Zmud, 1987).
At the very least information systems development should be viewed as an organisational system that needs to be managed (Maguire, 2000a; Harry, 2001). Management should be in a better position to understand the factors influencing implementation success (Kwon and Zmud, 1987). A significant number of writers have identified the need to take a more long-term, strategic view in relation to risk and security. Some writers have viewed risk management as the ability to anticipate what might go wrong in a project (Hoffer et al., 1998). They state that:

- large projects are riskier than small projects;
- a system in which the requirements are easily obtained and highly structured will be less risky than one in which requirements are messy, ill-structured, ill-defined, or subject to the judgement of an individual;
- the development of a system employing commonly used or standard technology will be less risky than one employing novel or non-standard technology; and
- a project is less risky when the user group is familiar with the systems development process and application area.

In many cases a system development may only be one of several different initiatives that need to be prioritised. Part of this process will be trying to gauge the likely success of the project (Wetherbe and Vitalari, 1994; Ward, 1995). This could be dependent on the threat of competition (Anderson, 2000). A major risk in the development of a new system might be the use of unproven technology or the need by information systems staff to master new technology (Gordon and Gordon, 1996). Ward and Griffiths (1996) who identify six broad categories for identifying risks within a project confirm this. Their level of impact will depend on the nature of the system being developed:

1. project size;
2. project complexity;
3. people issues;
4. project control;
5. novelty; and
6. requirements stability.

The following section gives a brief outline of the CCTA’s risk analysis and management methodology (CRAMM).

### A risk analysis and management methodology

In 1986 the CCTA, which is responsible for providing IT advice and guidance to government departments decided to adopt a risk analysis method and to recommend its use across all government departments. However, no product then available developed a relationship between the value of risk and the selection of appropriate countermeasures. In view of this the CCTA concluded that it would be preferable to design and develop a more comprehensive method from basic principles.

In any risk-analysis exercise there are two major tasks to be carried out:

1. The elements of risk, which are specific to the area under study, have to be identified.
2. Those elements of risk have to be measured and the risk itself given a value.

The identification of assets is straightforward in theory, i.e. software, hardware, and data. Hardware and software assets may be valued by estimated replacement costs. Data, however, may need to be valued separately for each impact type. When data assets are identified each user is asked to define a “worst-case scenario” for each of four impact types:

1. denial of access to data;
2. destruction of data;
3. disclosure of data; and
4. modification of data.

It is the data valuation criteria that may be of the most benefit to organisations developing information systems that link directly to customers. This criteria includes, financial loss; business disruption; loss of reputation or goodwill; failure to meet legal obligations; infringement of personal privacy; danger to personal safety; and disclosure of commercial information. It is with this framework in mind that the following case study has been analysed.

### The case study

This organisation has been established for over 150 years and employs over 100,000 staff. It has been trying to establish new business ventures for several years as it has come under increased competition from new entrants to the sector. This part of the business had been profitable and it was expected to grow significantly in the next few years. However, it was believed that the current system was inflexible and could not meet this future expansion. It was, however, functional and well understood by users. It was anticipated that the new information system would satisfy the business requirements of the organisation into the second decade of the twenty-first century.
The author was approached to undertake an independent review by the current project board (Maguire, 2000b). A total of 24 staff involved in the project management, development and use of the system were interviewed. Access was also gained to relevant documentation and a technical review of the system was undertaken.

The original aim of the project was to improve the system that currently allowed clients to book the delivery of advertising material at agreed times and within agreed areas. This booking took place at sales centres across the UK. Original estimates indicated that the previous system took an average of over a day to confirm a customer booking whereas the new system should be able to undertake this task in less than an hour. It was hoped that this project would ease the pressure on bookings both now and into the future.

It was generally understood that the previous system was being phased out because it could not meet future demand and any future enhancements were going to be expensive. The organisation perceived that it was relatively inflexible and was concerned that some competitors may have better systems. The new system could be justified on financial grounds because of the marked increase in business activity within this sector. The new system went through user acceptance testing to ensure that it met the original requirements. Data was converted from the old to the new booking system. There was a phased conversion process for the new system although the original plans had been changed to move away from a “big-bang” approach.

### The review findings

This section isolates particular areas of concern that were identified during the review process. These can be likened to the elements of risk that were mentioned earlier.

#### Project management

The project had a large number of different stakeholders interested in its progress. There were several project managers during its life. This may have inevitably lead to a change of focus within the project as well as a lack of coherence and some breakdown in communication between the various stakeholders.

#### System design

The initial recommendation by the project sponsor was for a mainframe system. Several staff believed that the final decision for the new system was taken away from the IT staff. The system design needed to be a transaction-oriented system that supported over 60 users and was able to:

- build and manage queues; and
- manage complex business transactions.

One group of staff expressed concern that there were three sets of technical views being input into the project. Different stakeholders had different expectations about what the system should be able to do. Several staff thought that the development team only knew the basic requirements of the new system.

#### Project and system development methodologies

It was felt in some quarters that there had not been a strict adherence to the projects in a controlled environment (PRINCE) project management methodology though it did follow its broad guidelines. The new system was not developed using a recognised system development methodology, i.e. SSADM. This project appears to have suffered from the classic project management problems, such as changes in key personnel, that would inevitably lead to the loss of some continuity.

#### Piloting

There appeared to be no safety net with the new system. Initially it was suggested that there would be parallel running with the previous system. Concerns were expressed about the testing and piloting of the system at the sales centres. However, a decision had to be made at an early stage about requirements otherwise every division would require a separate system. It was felt at the sales centres that the development team had not fully understood the business requirements for a new system. Staff suggested that this outcome showed that the new system was purely an IT solution.

#### Capabilities of the system

The migration from a mainframe environment to Windows NT was a relatively new venture for the IT department. Several different sources confirm that the new system was crashing with fewer than ten users using the system. Some feedback suggested that more time should have been spent investigating the volumetrics surrounding the system. There were a number of problems with multitasking that it was hoped would be solved with a later release of Windows NT. It was originally anticipated that the new system would support up to 60 users in the longer-term although a revised version of 32 was now
being accepted as reasonable. Feedback suggested that this would be very difficult to achieve.

**Integrity and security issues**
It was generally accepted that for the new system to be successful the accuracy of its data was crucial. Errors at the interface between the customer and user were not acceptable. Several staff affirmed that security issues were not viewed as critical.

**Interfacing with other systems**
A majority of interviewees believed that the new system would be integrated with other systems. In reality this did not occur. It was accepted that the original specification from financial staff did envisage it interfacing with other accounting systems.

**Risk management and contingency planning**
At first there appeared to be no contingency plan for the new system. Staff believed that the new system had a contingency attached to it but this had not been adequate. A significant number of staff stated that they were told that there was 99 per cent confidence with the new system and that the previous system was not seen as part of any contingency plan. User testing had taken place and it had worked. However, this had only been undertaken with six users and this may have given a false sense of security. There was a lot of confidence with the new system when it went live. There was a general feeling shared by both project team members and users that it should not have taken several months to realise that the system was not delivering anticipated benefits. However, the new system went through a full acceptance testing operation and was still withdrawn.

**User issues**
The new system had been sold to customers as a faster, more efficient system. In most cases customers require a lot more information. One of the reasons that expectations were high among users was because it was expected that it would interface with other systems. There was a general feeling that it would take a lot of effort to win back the confidence of users towards the system, as the internal perception of it is already poor. There was a major disparity in the feedback from the training process. This ranged from it being successful to it being useless. It was generally expressed in the sales centres that the decision to revert back to the previous system should have been taken much earlier.

It would also be difficult to give reassurances to users and customers that a relaunched system would be successful.

As shown in Table I most of the problems encountered in the case study occurred during the information systems development process – often referred to in the textbooks as the system development life-cycle (SDLC). The numbers refer to issues identified in the research and can be cross-referenced with the list in the conclusions. Some issues occur more than once in the list. It can be seen that a significant majority of these occurred during the information system development process. Only one occurred when the system had gone live. However, CRAMM is generally regarded to be useful when the system is up and running. A significant number of risk analysis and risk management methodologies concentrate on protecting physical assets when the system has gone live.

### Applying the methodology
As indicated earlier, elements of risk have to be isolated, measured and given a value. Hardware and software may be valued by estimated replacement costs but most organisations are primarily concerned with issues surrounding data. It is now that the relevance of “worst-case scenarios” becomes apparent. Your organisation may view denial of access to data; destruction of data; disclosure of data; or modification of data as all being important issues to consider. Referring to the case study, if the first impact type – denial of access to data – was considered, a series of “worst-case scenarios” could be built up using the data valuation criteria.

### Table I

<table>
<thead>
<tr>
<th>Problems encountered in the case study</th>
<th>The system development life-cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inception</td>
</tr>
<tr>
<td></td>
<td>Feasibility study</td>
</tr>
<tr>
<td></td>
<td>Systems analysis</td>
</tr>
<tr>
<td></td>
<td>Systems design</td>
</tr>
<tr>
<td></td>
<td>System building</td>
</tr>
<tr>
<td></td>
<td>Testing</td>
</tr>
<tr>
<td></td>
<td>Changeover</td>
</tr>
<tr>
<td>After the system has gone live</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>System evaluation and review</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
The numbers refer to issues identified in the research and can be cross-referenced with the list in the conclusion.

CRAMM is generally regarded as being useful when the system has gone live.
All the data valuation criteria would lead to some financial loss. In essence this should be the easiest area to quantify. Organisations, however, find it difficult to calculate accurate figures. There is often a wave of optimism with IS/IT projects that is often strengthened by the project management team. Any negative talk is usually frowned upon. This can often make it difficult for members of the project management team to even begin formulating a “worst-case scenario”. The case study organisation suffered financial loss in several key areas, with existing customers; potential future customers; and also with the cost of developing the new system.

There was a considerable breakdown in the service that was offered by this organisation over a period of several months. It was also the customers who suffered because of the failed implementation. If customers require strict contractual agreements it will put extra pressure on organisations to reduce risk during system developments.

In a number of instances new and existing customers were told that they would be better going to rival companies to get their business fulfilled. This had a significant effect on current business levels. It was also an acute embarrassment to the organisation. If effective information systems are the cornerstone of an organisation’s business any failure in this area may have long-term consequences.

The contractual arrangements surrounding customer orders are sometimes blurred. The customer requests a business transaction to take place, usually at a stipulated time. In many instances the organisation was unable to meet these commitments. In another situation the threat of litigation may have been more pronounced. The repercussions in relation to this case were not grave but one could envisage a situation where the customer suffers a serious business loss leading to bankruptcy.

Your organisation may also view infringement of personal privacy; disclosure of commercial information; and danger to personal safety as being important data valuation criteria, i.e. in the aftermath of the implementation of computer aided despatch within London Ambulance Service the National Union of Public Employees (NUPE) issued a document stating that, “introducing an untested computer to deal with 999 calls … has directly led to patients dying” (South West Thames Regional Health Authority, 1993). These final three criteria have not been viewed as particularly important for the case company though it could be argued that knowing an organisation is in difficulty with a computer project conveys very useful commercial information to competitors.

It is quite difficult to map CRAMM onto the case company as it does not appear to be relevant in many areas. Table 1 has shown that most of the risk elements in this information system development were encountered before the system went live.

### Conclusions

The field of information systems is not delivering the expected returns for organisations in relation to the expenditure on new system developments. There are many possibilities for things to go wrong. This article has shown through the use of a live case study that there are many risks that can confront an organisation during the information systems development process. A number of risk analysis methodologies, i.e. CRAMM, concentrate on quantifying the costs of system disruption once the information system has gone live. However, through the case study this article has shown that there is a need to develop a risk analysis methodology that incorporates the key issues that need to be addressed before a system goes live. The increasing caseload of information systems failures is reflected by current literature taking a wider perspective on the process issues surrounding risk.

With risk analysis the elements of risk have to be isolated at an early stage. It is only when this has taken place that “worst-case scenarios” can be formulated. Unfortunately, there appear to be many elements of risk when developing new information systems. The following is a list of potential risk elements extracted from the case study:

1. Use of a previously unused platform – failure to deal with known and unknown bugs.
2. Multi-tasking capabilities – inability to handle user numbers and response times.
3. Changes to the development team – several project managers.
4. Lack of rigorous testing – inability to test in a “live” environment.
5. System development methodology – inappropriate application leading to divergent approaches.
6. Number of stakeholders – failure to satisfy the system requirements of the disparate groups.
7. Immovable end date.
8. Limited access to users – lack of analysis in business areas.
Consultancy support – several suppliers of consultancy with separate aims and objectives.

Local business requirements – failure to reconcile separate design needs.

System changeover – lack of contingency planning.

Availability of qualified staff.

This list is not exhaustive but does go some of the way towards showing how risky the development of an information system can be when customers are directly involved. The writer has tried to show the need for organisations to be wary about the issues that can have a detrimental effect on the system development process. It is often a very complex process with many opportunities for things to go wrong. Historically, organisations were often able to confine the repercussions of their system failures within organisational boundaries. The increasing development of inter-organisational systems will make the process more visible. Organisations are becoming tightly coupled through the use of information and communication technologies. There are also increasing possibilities for integrated systems. These new systems could provide substantial benefits for organisations. However, there is a need to identify, at an early stage, the critical nature of certain system developments. It may be very difficult to isolate the consequences of a system failure and this puts extra pressure on those staff involved in the system development to ensure that things go according to plan. If things go wrong who will be affected? What will be the knock-on effect of a system failure? Will it affect our working relationships with customers and suppliers? New business opportunities brought about by improvements in information and communication technologies should not be jeopardised by failing to identify the potential risks within the IS development process.

References


Hicks, J.O. (1980), Management Information Systems – A User Perspective, West, St Paul, MN.


