# CHAPTER 3

# SYSTEMS DEVELOPMENT LIFE CYCLE RISKS - A PERSPECTIVE

## 3.1 INTRODUCTION

The waterfall model, as discussed in chapter 2, is applicable to the South African Post Office projects, but the South African Post Office needs to address the shortcomings of risk management. This chapter addresses risks in general as applied to the systems development life cycle and provides a basis for chapter 4 which deals with the application of risk management in the South African Post Office.

## 3.2 THE PROCESS OF MANAGEMENT

No discussion about risk management is justified without explaining what is meant with "management". Daft (1994) explained that management decisions fall into one of two categories, namely programmed and nonprogrammed.

*Programmed* decisions involve situations that have occurred often enough to enable decision rules to be developed and applied in the future. Programmed decisions are made in response to the organisational problems. Programmed decisions concern that type of skills required. Once managers formulate decision rules, subordinates and others can make the decision, freeing managers for other tasks.

*Nonprogrammed* decisions are made in response to situations that are unique, are broadly defined and largely unstructured, and have important consequences for the organisation. Nonprogrammed decisions often involve strategic planning, because uncertainty is great and decisions are complex. Nonprogrammed decisions would include decisions to build the new system and develop a new service into a new environment. The decision rules or techniques for solving this problem do not exist.

## 3.3 CERTAINTY, RISK, UNCERTAINTY AND AMBIGUITY

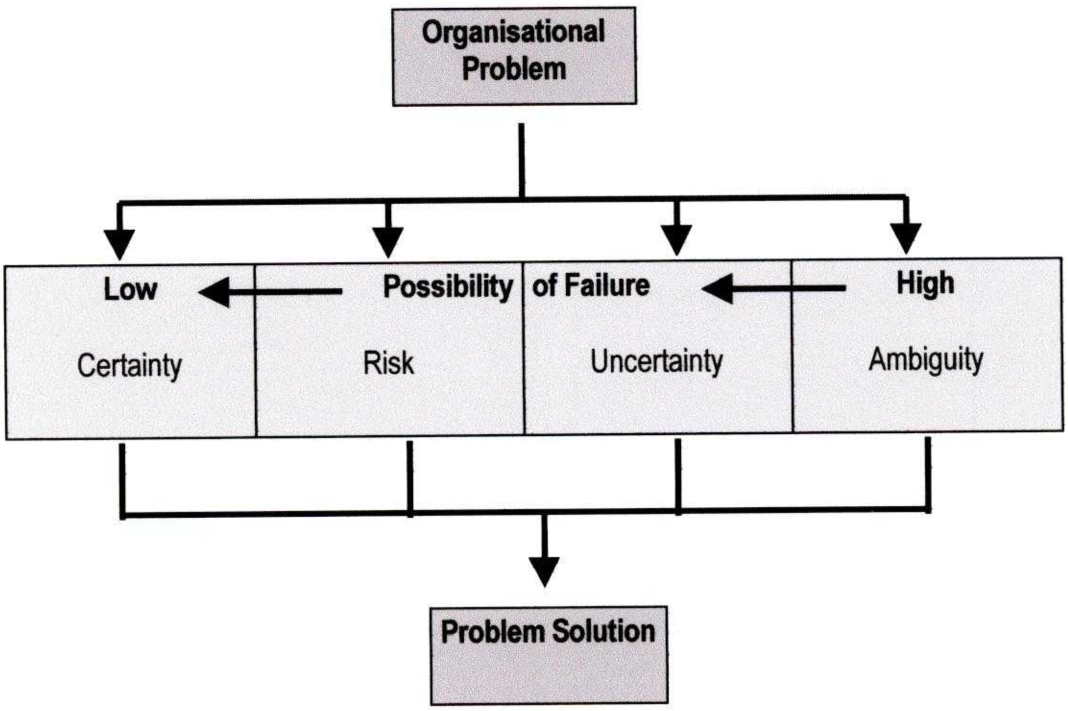
In the perfect world, managers would have all the information necessary for making decisions. In reality, however, some things are unknowable. Every decision situation can be organised on a scale according to availability of information and the possibility of failure.

*Certainty.* Certainty means that all the information the decision maker needs is fully available, managers have information on operational conditions, official costs, and each course of action and possible outcome. However, few decisions are certain in the real world. Most contain risk or uncertainty.

*Risk.* Risk means a decision has clear-cut objectives and information is available, but the future outcomes associated with each alternative are subject to chance. Statistical analysis might be used to calculate the probabilities of success or failure. The measure of risk captures the possibility that future events will render the alternative unsuccessful.

*Uncertainty.* Uncertainty means that managers know which objectives they wish to achieve, but information about alternatives and future events is incomplete. Managers do not have enough information to be clear about alternatives or to estimate their risk. Factors that may affect a decision, such as price, production costs, volume, or future interest rates, are difficult to analyse and predict. Managers may have to come up with a creative approach to alternatives and use personal judgements to determine which alternative is best.

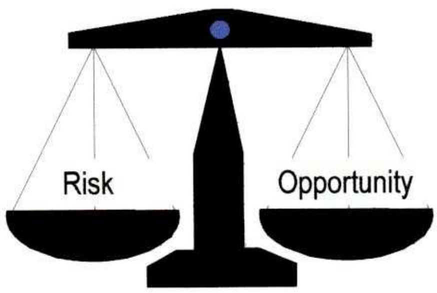
*Ambiguity*. Ambiguity is by far the most difficult decision situation. Ambiguity means that the objectives to be achieved or of the problem to be solved are unclear, alternatives are difficult to define, and information about outcomes is not available.



## 3.4 RISK DEFINED

Risk is a combination of the probability of a negative event and its consequences (Chapman:1997). Anything that is not well understood, anything that is not well documented, and anything that can change creates a risk to the project. A golden rule is: "Things that haven't been tested" are always at risk.

Risk is part of any activity and can never be eliminated, nor can all risks ever be known. Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunities.




Even if we're not familiar with the formal definition, most of us have an innate sense of risk. We are aware of the potential dangers that permeate even simple daily activities, from getting injured when crossing the street to having an accident with the family car on your way to work.

Anyone thinking of the term risk might ask himself: Can it be managed? or, Isn't risk rather unpredictable? To both these questions the answer is yes and no. Let me clarify by first explaining the nature of risks and then why it can be managed.

**Nature of risks**

Chapman(1997:7) states: “A source of risk is any factor that can affect project performance, and risk arises when this effect is both uncertain and significant in its impact on project performance.” Setting tight cost and time targets makes a project more cost or time risky. Conversely, setting slack time or quality requirements implies low time or quality risk. Whatever the underlying performance objectives, the focus on project success and uncertainty about achieving it leads to risk being defined in terms of a “threat to success”.

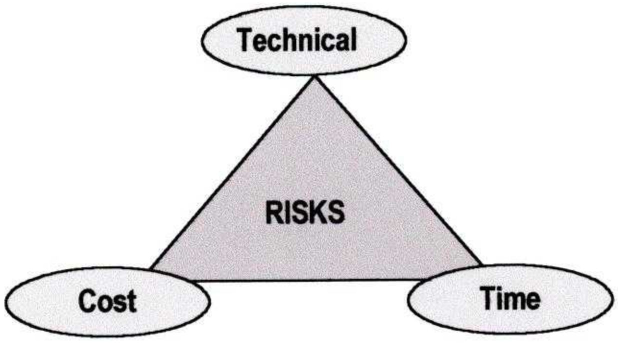
**Manageability of risks**

Risks are a major influence on the success or failure of a project. They must be managed by applying a conscientious effort to their reduction or elimination. Not all risks need to be eliminated entirely; often it is sufficient to reduce the project’s exposure to a level that is acceptable to the project. Risk management costs time and effort, but the rewards can be significant. Without risk management, the danger of failure is magnified. Projects generally involve large, expensive, unique or high-risk undertakings, which have to be completed by a certain date, for a certain amount of money, within some expected level of performance.

## 3.5 MANAGING RISKS IN THE LIFE CYCLE

### 3.5.1 A PERSPECTIVE

In the evolution of project management, the traditional schedule, cost and technical (quality/scope) aspects of a project have been considered as the main objectives of project managers - Better known as the "Iron triangle".




If one of the components is not achieved, the project manager cannot claim a successful project

How well the project is managed depends largely on the effective implementation of a programme in which the relationship between the schedule, cost and technical parameters is optimised. As pressures to complete more effectively and efficiently for business opportunities increase, companies have been striving to refine and redefine their project management practices to comply with customers' contractual requirements and thus increase their customers' satisfaction. Customers no longer accept unanticipated, surprised risks in their projects' executions. More and more project managers learn the hard way that successful implementation of project management requires not only other traditionally accepted management approaches, but also a formal, effective risk management approach that provides a basis for mitigating impacts associated with the project and its suppliers' structure.

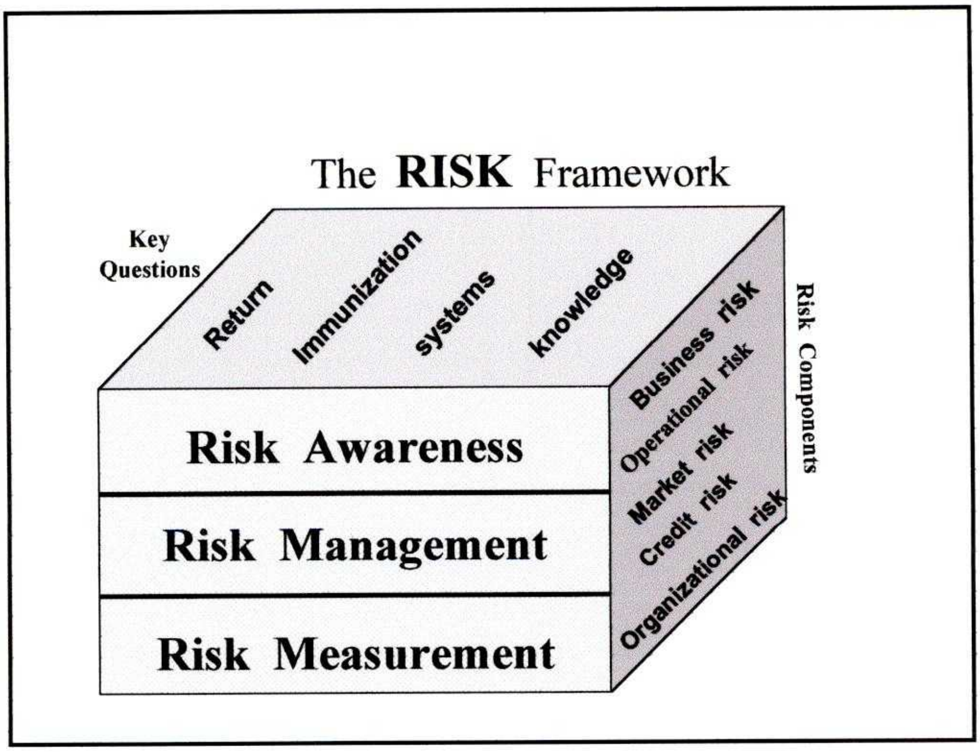
Because of the high competitiveness and state-of-the-art technology advances caused by changing market conditions, companies need to adopt and implement new and effective project management techniques that will allow them to survive and profit in tomorrow's project-driven environment as well as fulfil potential business globalisation strategy requirements in the coming years. Risk management is a technique that identifies a concern that threatens the success of a project and focuses the project management attention on this concern. This proactive approach gives project managers time to identify possible alternatives, develop action plans and select those that are most consistent with the project's alternatives. Since risk has always been an integral part of a project and associated with uncertainties, risk management is a systematic approach to evaluate the uncertainty, isolate the critical ones, and formulate cost-effective methods for minimising those uncertainties.

Cash (1992) explains, "In discussing risk, we are assuming that the manager has brought appropriate methods and approaches to bear on the project – mismanagement is obviously another element of risk. Implementing risk control is what remains after application of proper tools. Also, we are not implying that risk is bad. These words denote entirely different concepts, and the link between the two is simply that higher-risk projects must have potential for greater benefits. The typical project feasibility study covers exhaustively such topics as financial benefits, qualitative benefits, implementation costs, target milestones and completion dates and necessary staffing levels. In precise, crisp terms, the developers of these estimates provide voluminous supporting documentation. Only rarely, however, do they deal frankly with the risks of slippage in time, cost overrun, technical shortfall or outright failure. Rather, they deny the existence of such possibilities by ignoring them. They assume the appropriate human skills, controls, and so on are in place to ensure success."

Rodney Turner (1993:236) defines risk management as follows: "Risk management is the process by which its impact is reduced." Risk management in essence is a discipline, which objectives are to identify, address, and eliminate risk items before they become threats to the project by either abandoning the project or necessitating rework. In addition, risk management provides an improved way of addressing and organising the systems development life cycle. Risk-driven approaches also show how and where to incorporate new technologies such as rapid prototyping, fourth-generation languages and commercial software products into the systems development life cycle, and help managers determine how much of a given activity is enough.

James Lam (Chief Risk Officer of Fidelity Investments) uses a RISK framework to clarify risk and its involvement. The same framework can be used in information technology projects.

**"R" is for return:** Are we achieving an appropriate return for the risks we take?
**"I" is for immunisation:** Do we have the controls and limits in place to manage risks?
**"S" is for systems:** Do we have the systems to measure and report risk?
**"K" is for knowledge:** Do we have the right people, skills, culture and incentives for effective risk management?




Source: Fidelity Investments

An Arthur Andersen survey of CEOs, presidents and board members at more than 150 global companies, reveals the need to look more carefully at information technology risks based on the following:

- One in three senior executives does not have any information technology risk management process in place; only half of those who do, are confident the process is strong enough.
- Two out of three executives say their companies do not understand information technology-related risks well enough.
- Only 13 per cent of executives believe information technology strategy is well integrated with business strategy.
- Technology professionals are responsible for the daily management of information technology - related risk at 51 per cent of companies

Source: "Managing Business Risks in the Information Age" a study by Arthur Anderson and the Economic Intelligence Unit Ltd (EIU), 1998.

The desire to build information systems across functional boundaries is also not new. "A disadvantage of being preoccupied with organisation charts is that it becomes difficult to cut across departmental lines in developing the kind of system which ties together different departments and divisions," observed a manager at General Electric in 1960.

Firms that do develop new applications must do so in a new way. Organisations commonly tailor application packages to fit existing business practice, with the result that most business applications are functionally oriented - marketing systems solve marketing problems, sales systems solve sales problems, manufacturing systems solve manufacturing problems. Davenport (1993) argued that such "stove piped" systems cannot support a process view of the organisation; they imprison data within functions, so that new product designs cannot be released to engineering, sales data cannot be transferred to manufacturing, and customers for one product who might be customers for another product cannot be identified.

Having identified potential opportunities and constraints, their relevance to the process under analysis must be determined. Opportunities must be researched to determine how the technological or human innovation might be employed in the process. Constraints, on the other hand, are usually better examined through discussion than research. Which of the constraining factors should be accepted as constraints, and which should the organisation try to overcome? Analysis at this point is still quick and at a high level, but it provides a better understanding of which enablers will become part of the process vision and also how they will be employed in the process.

### 3.5.2 RISK FACTORS

Throughout the literature study of the waterfall model, risks were categorised in two classes – those of internal factors and of external factors. The following list of factors was compiled which could either act as quality of process measurement or as risk indicator.

#### 3.5.2.1 Internal factors

The internal factors are those that have their origin within the project itself. Internal factors to a large extent are controllable. Internal risk factors can also be named critical success factors. Critical success factors are those factors that have a direct bearing on the outcome of the project and can cause the termination or failure of a development project. The following list contains typical factors to consider in the systems development life cycle. The factors are grouped according to the relevant phase of the life cycle.

**Project planning and initiation**

- The scope, objectives and boundaries of the project should be clearly understood
- Approach best suited for the type of project
- Determination of management approval and their commitment levels
- The service request (requirements) detailed, relevant and complete
- Determination of business case risks
- Training requirements of team members.
- Work breakdown structure – schedules for every phase

- Team structure for every phase
- Communication channels
- Stakeholder's commitment
- Deliverables list
- Assumptions and rationale for estimates, schedules and contingencies
- Financial plans
- Communication plans
- Risk and contingency
- Conflict management plans
- Loss management plans

**System requirements analysis**

- Methods used to determine requirements.
- Investigation team skills
- The use of market sector specialists
- Modelling of requirements
- Requirements confirmation by user management
- The number of design alternatives for evaluation
- User understanding and commitment
- Cost and benefit analysis
- A thorough route map
- Realistic and coordinated plans for delivery of system

### Product evaluation and recommendation

- Evaluation of vendor proposals and their relations
- Costs and benefit summation
- Evaluation criteria, for example functional requirements, technical requirements, business requirements
- Formal request for proposal procedures
- Adequate training plans for skills transfer
- Change management procedures
- Realistic implementation and milestones
- Users must agree to deliverables
- Change control procedures
- Functional alternatives restrictions

### Technical system design

- Design standards should be appropriate to environment
- Design properly coordinated with user procedure
- Technical design team skills (specialist flexibility)
- Change control procedures
- Hardware requirements documented and mapped
- Details of technical design
- Maintainability of finished product
- Enhance ability after delivery
- Programming standard appropriate
- Configuration management procedures
- Communication between users, operations, support staff
- Testing approach (phases or once)

**System and acceptance testing**

- Objectives detailed
- Test data (relevance and volume for stress test)
- Resources availability
- Plans for parallel running - if required
- System ability to run without assistance from technical people
- Day-to-day problem-solving and monitoring
- Error-handling procedures
- Input–output controls and analysis
- Test plan documentation and actions

### 3.5.2.2 External factors

There are a few factors encompassing the systems development life cycle, bearing an outcome of activities. A term generally used is influencers. A brief discussion follows to clarify the reason why these influences can affect the outcome.

**Organisational culture**

Information technology departments do not give the necessary attention to organisational structures and processes, as they should do. Information technology departments too often ignore the impact of new technology on the way work is organised and on job design. Through the years, technologists became accustomed to the idea of "user-friendliness". The part of user-friendliness has been recognised for its importance due to system user dependence. Any system implemented relies on the user inputs for its effectiveness.

## Preliminary study

A study conducted in the United Kingdom in 1996 (Report to the Economic and Social Research Council: 1996) revealed that investigation teams rarely dig deeper than the surface or face value of systems. Their findings also proved that "most organisations are not good at evaluating the performance, impact and effectiveness of their investments". In the report it was also stated that organisations do not perform a careful, systematic evaluation of the operational performance of investments against their objectives. The main reason given was due to politics. Managers perceived that it is not in their best interest to perform such an evaluation. Problems in this area are compounded by the fact that prespecified objectives are often political statements to persuade senior managers to make the investment, rather than a commitment to expected levels of performance.

## Performance of Information Technology

According to the study done in the United Kingdom (Report to the Economic and Social Research Council), 80 to 90 per cent of new investments in systems fail to meet their objectives. Some of the researchers stated that no systems in their experience had met the objectives. Evaluation of performance is considered the most difficult part of information technology projects. The same group of researchers reported that between 20 to 30 per cent of projects were successful in delivering on time and within budget. The main reasons given are that plans are altered too often for the sake of technology, poor management (generally and project), poor articulation of user requirements, inadequate attention to business needs and goals and a failure to involve users appropriately.

**Purpose of systems**

Cash (1992) discusses the problems related to information systems' success and identifies management policies and procedures that help to ensure the potentially high-risk projects. These risks focus on strategic vulnerabilities as opposed to the more defined implementation issues. Cash (1992) categorises the types of system as follows:

- Systems that change the basis of competition to a company's' disadvantage
- Systems that lower entry barriers
- Systems that bring on litigation or regulation
- Systems that increase customer power to the detriment of the innovator
- Investments that turn out to be indefensible and fail to produce lasting advantages
- Systems that pose an immediate threat to large established competitors
- Inadequate understanding of buying dynamics across market segments
- Cultural lag and perceived transfer of power

## 3.6 MOST COMMON SOFTWARE RISKS

Jones (1994) provided extensive data in his book on the reasons why Information technology projects fail. He also gives reasons to why, as well as possible resolutions. The table below is his summary.

**Management Information Systems Risks**

| Risk factor | % of projects at risk |
|---|---|
| Creeping user requirements | 80 |
| Excessive schedule pressure | 65 |
| Low quality | 60 |
| Cost overruns | 55 |
| Inadequate configuration control | 50 |

**System software risks**

| Risk factor | % of projects at risk |
|---|---|
| Long schedules | 70 |
| Inadequate cost estimates | 65 |
| Excessive paperwork | 60 |
| Error-prone modules | 50 |
| Cancelled projects | 35 |

**Contract or outsourced software risks**

| Risk factor | % of projects at risk |
|---|---|
| High maintenance costs | 60 |
| Friction between contractor and client personnel | 50 |
| Creeping user requirements | 45 |
| Unanticipated acceptance criteria | 30 |
| Legal ownership of software and deliverables | 20 |

# CHAPTER 4

# RISK MANAGEMENT IN THE SYSTEMS DEVELOPMENT LIFE CYCLE IN THE SOUTH AFRICAN POST OFFICE

## 4.1 INTRODUCTION

With any development of an information system, one has to ask oneself the question of what value the information has. Information has many attributes, such as verifiably, accessibility, clarity, precision and cost. Four factors that are especially important for management is quality, timeliness, completeness, and relevance.

*Quality.* Information that accurately portrays reality is said to have quality. The data are accurate and reliable. Once a system is known to have errors, managers will no longer use it, and its value for decision-making will disappear.

*Timeliness.* Information that is available soon after events occurred has timeliness. The most immediate benefit of computerised management is a quick response time.

*Completeness.* Information completeness refers to the problem of quantification of data. Too much data lead to information overload. Managers often devise exception to the boards that contained only a few pages of deviations from target rather than hundreds of pages of raw data.

*Relevance.* Information relevance means that the information must pertain to the problems, decisions and tasks for which a manager is responsible.

The real challenge is to establish a system with these characteristics. Establishing such a system involves risks. The next chapter deals with a real situation whereby the South African Post Office established a system successfully, but failed the project "iron triangle" of costs, time and technical constraints. Throughout he project the operations subproject was on course, but the systems development failed to deliver on time.

This chapter will discuss the risks in sequence to the waterfall process for ease of reading.

## 4.2 BACKGROUND TO THE SYSTEM

The concept of tracking containers and individual items is nothing new in any logistics company, but for the South African Post Office, it was new in that operations had to make the paradigm shift from a manual system to a technology-based system.

Previously, items and containers were recorded manually, producing a number of manual reports, which had the risk of getting lost on the journey. This also resulted in external customers being frustrated with the "old and backward company". Thus the decision was made to implement the system.

## 4.3 SYSTEM FEASIBILITY

Before any project can start, we need to establish if it is possible and the right thing to do. There is a number of issues to consider at this stage, namely; business issues, technical issues and timing.

From the *business perspective*, the analysis revealed a number of advantages of introducing such a system. The system was to replace the repetitive manual tasks and to optimise an expensive process. No risk assessment was performed regarding the long-term financial viability. Benefits outweighed any possible risks. The argument used was that we wanted to become a world-class organisation, so we had to use world-class technology. The South African Post Office will have the capacity to offer new services to customers locally and internationally while having the flexibility of product characteristics form market to market.

From the *technical perspective*, the system could add to the value chain in that future systems could be integrated, using the data available. The system, which the South African Post Office acquired from New Zealand, was already two years old. The South African Post Office could have implemented the system as an "off-the-shelf" system, but decided to modify the software to the local protocols. The reasons given were that the platforms were old, unstable and had an outdated network protocol, which made it impossible to implement as is. One of the strongest motivators were that the old system would not cope with the volumes, since the South African volumes were ten times that of New Zealand.

The feasibility report presented to the then management board contained only the following headings:

- Objectives
- Scope
- Possible courses of action
- Pros and cons
- Recommendations

No risk assessment was performed. The investigating team did not consider the following risks:

- Acceptance by the unions
- Resources and skills available
- User capabilities, requirements and interfaces
- Organisational implications
- Features of the system
- Hardware and software
- Communication protocols

With this as the foundation, management should have realised that the chances of the system not being implemented were high. The management board gave the permission to buy and adapt the system.

## 4.4 SOFTWARE PLANS AND REQUIREMENTS

The consulting firm from Canada, Systemhouse, managed the software development, while a local team managed the remaining part of the project.

Deliverables produced were as follows:

- Operations environment analysis (volumes and products)
- Software requirements
- Performance requirements
- Interface requirements
- Resource requirements
- Acceptance test requirements
- Maintainability requirements

The following deliverables were not produced:

- Functional requirements
- User requirements
- Verification requirements
- Quality requirements
- Safety requirements
- Reliability requirements

The above is a clear indication of no risk management. The following deliverables were delivered after the project were 25 per cent completed which in actual fact should have been delivered during the feasibility phase:

- Functional requirements
- User requirements
- Reliability requirements

This in itself poses a major risk in that the South African Post Office would have paid penalties if the system did not deliver in the actual requirements and the contract was cancelled.

If one takes into consideration that the same team implemented the exact system in New Zealand, the documentation of the New Zealand system should have been available at the outset. This would have enabled the team to make the necessary changes for South Africa.

## 4.5 PRODUCT DESIGN

The South African Post Office was aware of the following capabilities of the New Zealand version:

- Accuracy
- Efficiency
- Compatibility
- Flexibility
- Expandability
- Maintainability

What the team did not consider was the fact that these and other capabilities would change if the proposed changes were made. The technical team proposed the following changes:

- Host machine (from Ahmdahl to HP)
- Oracle 6 to 7 (versions)
- SQL Forms 3 to 4 (versions)
- Operational Computer (hardware) composition
- Unix O/S 4.1.2. to System 5
- Microcomputer setup with Dos 5, Btrieve 5.1, Microsoft C, Reflection

The users on the project made changes to some of the functionalities and thereby changed parts of the application so that it resulted into a complete rewrite of certain modules. All the screens had to change to accommodate the word "South Africa". This together with the technical changes lead to a situation where the project schedules had to be changed. The above is a clear indication that the preliminary investigation was inadequate. The technical team was strongly opposed to the Ahmdahl (host), but the local management overruled their proposal due to so-called "savings". This resulted in a dispute at a later stage when it appeared that the Ahmdahl was incompatible with the software and network protocols.

The core members of the operations team had to visit New Zealand to determine the true functionality of the system. The functional requirements were changed, after the team returned from their visit. This combined with the technical changes, resulting in a four-month delay of the project.

Documentation on the following was also not provided:

- System flow charts
- Chart standards
- Chart hierarchy
- System controls
- Security and privacy
- Hardware protection
- Software protection
- Input data controls

Proper risk management could have foreseen the problems experienced by means of an in-depth technical investigation during the feasibility phase. What was imminent during the interviews was that there was enough money built into the project plan to provide for the changes. The project plan, however, did not provide for slack time. Up to this stage in the process, the project experienced 90 per cent of the risks encountered, mainly because the

South African Post Office management by now realised what was involved in an information technology project. It was the first project of its nature having an influence across functional boundaries.

## 4.6 CODING, UNIT TESTING AND INTEGRATION

This part of the project was without any major events. Activities that took place were as follows:

- Modification performed
- Acceptance plan and strategy
- Test cases were prepared
- Code integrity checks
- Testing of modules for errors
- Testing of complete system as a unit
- Stress tests
- Integration testing

By now the project had its fair share of uncertainties and risks. The only remaining aspect was the acceptance test, where the South African Post Office had no experienced personnel. This was resolved in that the technical team provided their time and skills to the operational people to perform the testing. There was only one aspect of the system that could not be resolved, and that was the application of the scanning equipment. This proved to be a major stumbling block until one day before the official training of the users took place. Again, the risk of hardware compatibility with the modified software was not foreseen. If proper risk assessments were conducted, this would have been identified as one of the major risks, which had to be resolved before the project started.

## 4.7 IMPLEMENTATION (TRANSITION)

During this phase, the development software was transferred to the production machine (HP T500). The following actions took place:

- Final tests
- Network connections were tested
- Source code were installed
- Maintenance procedures were put in place
- Training and transfer of skills took place
- Users were trained
- System was signed off

## 4.8 OPERATIONS

The South African Post Office initially decided to run the system parallel to the manual system for two months, but after one month in operation, the users voted to switch to production. The "settling down" month was used for all role players to familiarise themselves with the system and to find any shortcomings. Training of the users proved again to be a risk, since more than 90 per cent of the users never touched a computer. Therefore, users had to be educated in order to reduce their resistance to change.

## 4.9 CONCLUSION

This chapter dealt with actual events as they took place. The project team had no formal risk management plan in place, nor had the local team members experience in projects of this magnitude. If one considers that there are 28 major production sites with 8 000 users, you might consider the project team to be lucky. However, other projects in the South African Post Office are not in that same position. No major technology project was successful since the Track and Trace implementation.

During the interviews, it appeared that on the current projects, no consideration is given to risks and their consequences. Concurrent engineering principles are not employed and the team members solely rely on the waterfall process. However, the South African Post Office recently invested in a methodology process called Summit-D, which are marketed by PricewaterhouseCoopers.

In the next chapter (chapter 5), the topic of project risk management in the systems development life cycle will be addressed. The author is of the opinion that with the introduction of risk management, information technology projects will be more successful. Proper risk control will enhance the ability of management to determine in advance if a project stands the chance of being a failure.

# CHAPTER 5

# RISK MANAGEMENT IN THE SYSTEMS DEVELOPMENT LIFE CYCLE - PROPOSED MODEL FOR IMPLEMENTATION

## 5.1 INTRODUCTION

In this chapter we will deal with the aspects of managing risks through proper risk plans. No longer can the South African Post Office rely on the instincts of people to make unfounded assessments on projects. Furthermore, team members have to realise that they as individuals are contributing to the level of risks. By means of proper plans, the management board will be able to take calculated risks.

The question of any manager is "where do we start", "what are the steps", "how can risks be identified". This chapter will build a model from the basic concepts (as discussed in chapter 3) up to the finishing of a project.

## 5.2 PROJECT FAILURES

No discussion of any risk plan can start without investigating the history of failed projects. This is done in order to equip oneself with the knowledge not to repeat the same mistakes. The conclusion to be drawn from reviewing the main research studies (Wilcox: 1997) (See Addendum B) on risk, is that major projects commonly experience overruns, are often over budget, do not perform in the way expected, involve severe strain on participating institutions, or are cancelled prior to their completion after the expenditure of considerable sums of money. Studies suggest that these problems relate essentially to issues of size, complexity, long time-span, uncertainty, governance and management peculiar to larger-scale projects. A generic list of risks is to be found in Addendum C provided by Tera Quest.

## 5.3 RISK MINIMIZATION

Before any manager determines a risk plan, he/she has to know what to do when risk factors have been identified. This section is an overview of risk minimization.

An easy way to reduce risk is to have less ambitious goals. After evaluating risks, one can choose a path of risk avoidance or risk mitigation and management. If project managers understand the risks during the various phases, they can decide which risks are acceptable and take actions to mitigate or forestall those risks. If the initial risk assessment determines that the risks are excessive, one has to consider restructuring the project to within acceptable levels. Risks that do not offer potential gain should be avoided.

Cash (1992) provide various strategies available for resolving a specific risk, which are listed below:

- *Avoidance:* Make decisions to avoid placing the team in risky situations. The following is typical responses to eliminate uncertainty or risks:
    - Clarifying requirements
    - Defining objectives
    - Obtaining information
    - Improving communication
    - Acquiring expertise by training or recruitment
    - Targeting cause or source of risk by removing it
    - Changing the scope of the project to exclude risks
    - Using proven technology methodology
    - Redesigning to eliminate risk

- *Protection:* Take actions that protect you from the consequences of a risk.

- *Research:* Eliminate the uncertainty associated with a risk by learning more about it.

- *Reduction:* Take actions that reduce either the probability or the consequences of a large risk to the point where it becomes a small risk.

- *Transfer:* Shift the risk somewhere else, for example, by getting the customer to take responsibility. Many project managers opt for this kind of strategy, but one has to remember that if you do not have direct control over a task, you cannot determine the outcome. Shifting the risk to someone else might also cause other unforeseen risks. An illustration is to subcontract at a fixed price. The risks are then borne by the subcontractor. The project manager should also keep in mind that to transfer the risk to someone else is to transfer the responsibility as well.

- *Acceptance:* It often makes sense to simply accept a risk with a relatively low exposure. If the risk becomes reality, you can deal with the consequences. Residual risks remain after avoidance and/or transfer. This must be proactively managed, even if they cannot be influenced in the same way as other risks. The most common way of acceptance is by means of contingency planning. This will include time, money and resources. Other means to accept responsibility for the risks are:

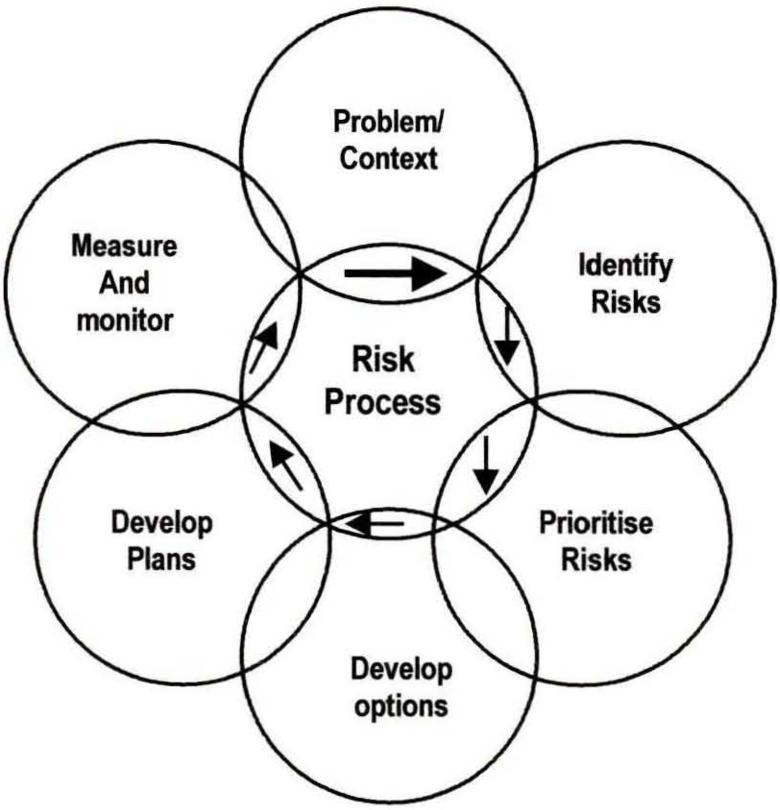
  - Development of a risk-aware culture in the organisation and on projects
  - Incorporation of risk management into routine project processes with regular reviews, reports and updates
  - Taking account of identified risk and agreed responses in project strategy, including appropriate activities in the project plan and budget.

## 5.4 RISK MANAGEMENT – THE METHOD

This section will deal with the risks in the systems development life cycle as applicable to the waterfall process.

The steps involved are:

1. Identify risks
2. Prioritize risks from high to low
3. Develop risk management action plans,
4. Measure and monitor action plans (risk)




### 5.4.1 IDENTIFY RISKS (What can go wrong and what are the causes?)

Consider the potential sources of risk and the options available for identifying risks and identify specific risk items that could compromise the project's success.

Remember that Murphy was an optimist. It's too easy for project managers to construct their models hoping that the things that could go wrong won't for their project. But that is not a level-headed way of looking at risk. If you're going to dodge the risk factors, you might as well channel your energy into completing the project and hope that divine intervention will guide your team to success. But if you want to manage your risks fairly, there are some steps that can help.

First, name your risks. One of the best ways to do this is to hold team sessions – inspections, if you will – to identify possible risks. Once you have a list of candidate risks, you should evaluate each risk and assign it a weight representing its likelihood. Following that, you must determine what will happen to the project if each risk becomes an actuality.

Given that it's impossible to reduce the likelihood of all risks to zero, you must identify the most significant risks in terms of severity, likelihood, and potential consequences.

**The change constant**

The biggest risk management mistake is not failing to identify risks. It's failing to continually revise the risk management plan. A software development project's environment is constantly changing, as a result of competitive pressures, organisational strategy and personnel changes and technical challenges. Too frequently, a risk management plan, like a system architecture design, is prepared at the beginning of the project and then shelved. To be valuable, risk management needs to be revisited as frequently as schedule and technical issues. Quantify the extent of each risk by measuring the risk exposure.

### 5.4.2 PRIORITIZE RISKS (Which risk can be responsible for the

**biggest upset?)**

Prioritize the identified risks in descending order of numerical risk exposure, to bring to the forefront those risks with a combination of relatively high impact and relatively high probability of occurrence.

- Document the results, using a Risk Management Log
- Develop Risk Management Action Plans
- Think through the options available for risk resolution.

One of the biggest risk analysis mistakes is confusing ordinal rankings with actual measurements. That is, if you assign a high, medium, or low ranking to a risk variable, it's inappropriate to construct a mathematical model of probability based on those rankings. A rank of "medium" cannot be interpreted as statistically significant. If, however, you assert that, a function point count greater than 100 will trigger a large project risk, you are using a measurement. Maybe a function point count of 100 translates into a medium-level risk, but you can't say a medium risk that your project will be cancelled is equivalent to the medium risk that your project will be too big. All you can say is that the risk is greater than low and less than high.

Another common mistake is confusing risk with uncertainty. Both may find a place in your spreadsheet, but you usually calculate risk. Uncertainty, by definition, negates any effort to assign a certain value to an uncertain variable.

### 5.4.3 DEVELOP RISK MANAGEMENT ACTION PLANS (What must be done?)

Develop a Risk Management Action Plan for each high-risk item. Ensure that each such plan is concise, action-oriented, easy to understand and easy to monitor. For each, plan how and at what cost. Make sure that the Risk Management Action Plans include specific contingency plans for high risk items.

**Integrate into the detailed work breakdown structure**

Ensure that the work required to implement the risk management action plans is integrated into the overall project work plans and that the costs of implementing the contingency plans are taken into consideration in the project budget. For example, if one of the risk management action plans calls for a prototyping or proof-of-concept activity, include the prototype or proof-of-concept (and the work required to develop and review it) in the detailed project work breakdown structure.

### 5.4.4 MEASURE AND MONITOR ACTION PLANS (RISKS)

Monitor the status of each risk and its Risk Management Action Plan and prepare a Project Weekly Risk. Report as part of the ongoing process of managing project performance. Involve the customer in increasing the visibility of risks and removing high-risk items. Focus on risks to which you can apply some form of risk elimination or containment strategy, as distinct from those over which you have no control.

Differentiate between generic risks (all of the things that can possibly go wrong on any project) and project-specific risks. Generic risks are dealt with through the standard project

Transfer of title and transfer of risk must be consistent for prime and subcontracts.

**Recourse for delays**

The prime contractor must have recourse for delays caused by the customer or by subcontractors.

**Dispute mechanisms**

There must be clear instructions for handling disagreements including problem escalation procedures.

**Update provisions**

There must be provisions for changes to the contracts and subcontracts, including keeping the agreements current.

### 5.4.5.2 RISK MINIMIZATION MEASURES FOR PREPARING WORK PLANS

**Goal-oriented plans**

There must be well-defined rather than broad objectives, a defined budget, reasonable schedule pressure, incremental change with well-defined intermediate states (measurable milestones), appropriate phasing recognizing the strategic aspects of the project schedule, and manage-to-budget techniques for each chunk.

**Work breakdown structure method**

Planning must be based on a comprehensive Work Breakdown Structure (WBS) which provides a clear and unambiguous definition of scope in terms of expected products or deliverables and work effort. The WBS must be used to identify, authorize, perform, accept, and manage all significant project activities.

**Clearly assigned responsibility**

Each component of the WBS must be assigned to a single point of responsibility.

**Team-based, leveraging previous experience**

Planning must be a group process to think through all elements of the project, clarify the scope of work, take into consideration previous experience on similar projects, and reuse or leverage existing materials to the maximum.

**Realistic**

The process, staffing commitments, schedules, and budgets for each subproject must be realistic.

**Traceable**

All subprojects must be broken down into detailed, traceable activities and tasks based on the WBS.

**Balanced estimates**

Estimates must be based on good estimating techniques, accurate estimating metrics and heuristics, and knowledgeable estimators, and must be accompanied by comprehensive detailed documentation of all assumptions.

**Risk management**

Planning must incorporate proactive identification of potential project risks and the development of plans to contain them.

**Contingency planning**

There must be contingency plans with fallback strategies for high-risk aspects.

### 5.4.5.3 RISK MINIMIZATION MEASURES FOR ORGANISED PROJECT START-UP

**Clearly assigned responsibilities**

There must be a clear definition of responsibility at all levels: who has overall responsibility for delivery of the project and who has responsibility for acceptance of the project on behalf of the customer, as well as who has responsibility for delivering and accepting each element of the work breakdown structure.

**Optimal structures**

The organization structure must be flat and non-hierarchical to the extent possible and must maximize the ability of team members to contribute to project success.

**Qualified team**

The team must comprise qualified personnel, including qualified subcontractors and partners, with the right person staffed to the right job.

**Integrated team**

There must be effective integration of the efforts of all contributors, including our staff, customer staff.

**Excellent infrastructure**

There must be an excellent infrastructure built well in advance (for example, System Development Environment, automated project management tools).

**Integrated facilities planning**

There must be effective synchronization of project planning with staffing, facilities, and other infrastructure planning. Poor planning can result in hundreds of person-days in lost productivity on a large team.

**Orientation**

There must be a strong orientation and training programme.

**Attention to cultural concerns**

Attention must be paid to cultural differences to identify and quickly resolve problems associated with different backgrounds.

**Controlled environment**

There must be appropriate planning and control systems providing an effective information flow.

#### 5.4.5.4 RISK MINIMISATION MEASURES - MANAGING THE CUSTOMER RELATIONSHIP

There must be a clear and unambiguous understanding of the goals and objectives of the endeavour. The vision must be clear, articulated, and agreed upon.

**Shared understanding**

There must be an understanding on both sides of the broader goals and aspirations of each organization (the bigger picture), so that the project can be placed in the proper context.

**Personal relationships**

Successful partnerships are based on people working with people who are on honest and have integrity.

**Positive attitudes**

Everyone must be committed to making the project a success. No one can be thinking in terms of being right at the expense of being successful.

**Realistic expectations**

Everyone must be balancing fundamental principles and ideals with reasonable expectations for the real world.

**Realistic commitments**

The project team must commit only to work, which it can deliver successfully.

**Frequent contact**

There must be frequent contact and discussions with customer management and with the customer's staff.

**Open communication**

Communications must be honest and open, based on fact, not hearsay, so that there are no surprises.

**Effective risk and issue management**

There must be clear demonstration to the customer of effective risk and issue identification and problem solving.

**Evidence of mutual satisfaction**

Interim work products and deliverables must be evaluated with the customer to ensure that work remains aligned with the customer's required direction, and that there is evidence of mutual satisfaction.

#### 5.4.5.5 RISK MINIMISATION MEASURES FOR MANAGING PERFORMANCE

**Commitment**

The management style must encourage respect for the individual and generate personal focus and clear intent to achieve customer satisfaction.

**Enthusiasm**

There must be a personal and collective display of excitement and interest.

**Visibility**

There must be visibility of responsibility and commitments, visibility of status based upon early and objective measurement of progress, full visibility and documentation of variances, issues, and changes, issue management, risk management, and financial management.

**Teamwork**

There must be evidence of positive morale and teamwork and evidence of stakeholder and end-user participation and understanding.

**Integrated systems**

The project management tools must be effectively integrated to schedule, track and account for all project work, including that of customers and subcontractors who are part of the project team. This requires that there must also be effective integration of the customers' and subcontractors' management systems with the project management tools.

**Cost/schedule management**

Cost and schedule must be managed proactively based on fact. The systems must provide the capability to predict final performance as accurately and early as possible. The systems must also generate early warning indicators that automatically trigger the application of additional face-to-face management experience to enable timeous, corrective action.

**Measurement**

There must be effective measurement techniques to identify the levels of quality and productivity being achieved and to provide a baseline for continuous improvement.

**Communications**

There must be effective team communication including all members, not just senior levels. Attention must be paid to ensuring effective communication processes (for example, use of LANs, WANs, effective use of meeting time).

**Decision-making**

Decision-making must be participative so that the right person makes the right decision information, rather than a person in the hierarchy. Everyone must be able to influence decision-making and understand the results.

**Problem-solving**

Everyone must be committed to understanding the issues and opportunities in problem situations and developing effective plans to achieve or resolve them.

**Rewards and recognition**

There must be recognition and rewards for quality service, creativity, innovation, and success.

**Continuous improvement**

The environment must encourage creative dissonance and continual striving for improvement within the time/cost constraints.

#### 5.4.5.6 RISK MINIMISATION MEASURES FOR MANAGING QUALITY

**Customer focus**

There must be an absolute focus on customer requirements and business objectives.

**Defined quality requirements**

Customer expectations for quality must be examined and quality specifications must be defined with our customers.

**Rigorous and optimized processes**

There must be defined processes which, when followed, lead to the desired end goals. The processes must be streamlined, fast and agile and must produce work products that are consistent and rigorous.

**Standards and procedures**

The project must use appropriate standards and procedures, which are re-used extensively across projects.

**Maximum empowerment**

Each team member must be responsible for building in quality, by applying approved policies, procedures, and work instructions in accordance with the Quality System.

**Quality control**

Independent verification and validation mechanisms must be in place to verify that the work products produced by the processes meet the agreed-upon quality specifications defined with the customer (the producer's view), and are suitable to meet the customer's business objectives (the customer's view). There must be built-in checks to identify errors that may have occurred and to ensure effective corrective action for nonconforming items.

**Quality assurance**

There must be a quality assurance function to provide confidence to internal management and to customers that the intended quality is being achieved and will be sustained.

**Measurement**

The approach to quality must be based on rigorous measurement and optimization of the cost of quality. Prevention and appraisal costs must be controlled and optimized to minimize resultant poor quality cost.

**Continuous improvement**

Defective processes must be corrected to make sure that similar problems do not recur. The approach must result in the continuous improvement of the quality of our staff and work products through training, positive management, and continuous monitoring of the needs of our market.

### 5.4.5.7 CLIENT/SERVER RISK MINIMIZATION MEASURES

Risk minimization measures are key practices that have been integrated into the Knowledge Base methodologies to minimize quality, cost, and schedule risks, as part of a comprehensive risk management approach.

**Client/server**

The following outlines the key areas to examine in each stage of the Client/Server methodology, to minimize risk:

1. Concept definition
2. Functional definition
3. Structural design
4. Development
5. Implementation

## 1. Concept definition risk minimization measures

The following outlines the key areas to examine, in the Concept Definition stage, to minimize risk.

**Proof of concept**

Use proof of concept testing early to prove the proposed technology architecture of the system. Ensure that selected products actually work together and that new products are compatible with existing products. Test the communications network and distribution strategy for data and process placement to ensure that the solution meets requirements and provides maximum performance.

**Implementation strategy**

If the system is to be deployed in releases, is distributed, or is to be deployed at many sites, invest time and effort to ensure that issues are identified and addressed and a detailed cost/benefit analysis is completed.

Deployment in releases increases the complexity of the project and adds overhead; make sure you have built additional project management effort into the work plan.

Overlapping stages (for example, design and development) adds another layer of complexity. Plan carefully and fully assess the impact of a scheduling delay or issue in one stage on the other stage.

**Plan for maintenance**

Start thinking early about maintaining the system and develop a plan for the System Management Environment. By defining requirements early, it will ensure that they are included in the design and development of the application.

**Prepare for the next stage**

Take the time to prepare for the next stage; ensure that the System Development Environment (SDE) is ready for the analysis and prototyping activities, analysis and SDE standards and procedures are defined, a baseline requirements trace ability matrix is complete and approved by the Acceptor. This matrix is used throughout the remaining stages to ensure that requirements are met.

## 2. Function definition risk minimization measures

The following outlines the key areas to examine, in the Function Definition stage, to minimize risk.

**Confirming requirements**

One of the most expensive and time-consuming errors to correct is the result of a missed or misunderstood requirement. Develop horizontal prototypes and vertical prototypes and use these to confirm the system requirements with the end-users in workshop settings.

Begin the Acceptance Test Plan and test scenarios in parallel and use the test scenarios during the prototype review workshops. Working through a test scenario with the prototype can ensure that a requirement is really understood by the project team and may also point out missed requirements (for example, missed data item, or awkward navigation for the business process).

**Before prototyping starts**

Before prototyping begins, decide whether the prototype will evolve into the production system or will be used and then thrown away.

If the prototype will evolve into the production system, it is imperative that the System Development Environment is in place and the design and development standards and procedures are defined before prototyping begins.

**Data conversion effort**

Do not underestimate the effort required to complete the data conversion activities, including preparation (or cleansing) of the data for conversion.

Conduct a thorough analysis of the existing data structures to ensure that procedures are defined to accurately load the data into the new data structure or to make the data available to the new system by interpreting the data in its existing architecture.

To confirm the integrity of the data and determine the effort required to cleanse it, audit the data in critical files to be converted. For example, in an accounts receivable system, audit the customer, sales history, and payment history data.

**Planning for deployment**

Start deployment and site preparation activities early to avoid schedule impacts caused by long lead times for equipment and facility upgrades.

### 3. Structural design risk minimization measures

The following outlines the key areas to examine, in the Structural Design stage, to minimize risk.

**Save time through re-use**

Structure the system to utilize common program units, wherever possible. Build these program units early so they are available to the team. Especially ensure that common architectural components such as data access and messaging utilities, are built early and placed in the re-use library. Prepare re-use procedures and train the project team on how to take advantage of re-use.

**Monitor system performance**

Continually test performance to confirm the technical solution and ensure that requirements are met.

## 4. Developing risk minimization measures

The following outlines the key areas to examine, in the development stage, to minimize risk.

**Organizing development**

Itemize the program units and order their development appropriately to help with the creation of test data for unit testing. For example, in a library system, develop the catalogue maintenance program units first; these maintenance programs can then be used to maintain catalogue entries to test the check-in and check-out program units, developed next.

Likewise, try to order the development of programs to consider integration testing. For example, develop program units that rely on one another to complete a larger task in a group, to allow integration testing to begin as early as possible.

**Integration testing**

Invest time and effort in a thorough integration test to avoid scheduling and effort impacts during system test. In other words, to avoid rework, make sure you are ready for system testing before you begin.

Integration testing is especially important if the system test and acceptance test have been combined into one test where the project team and the end-users conduct the test together.

**Test performance**

Continue to test system performance throughout development. During system testing, conduct volume and stress tests.

**5. Implementing risk minimization measures**

The following outlines the key areas to examine, in the Deployment stage, to minimize risk.

**Installation testing**

Complete a thorough hardware and application installation test before cutting over to the new system at each site. Putting a new system in place is stressful for the end-users and needs to run smoothly.

**Confirm conversion**

Confirm the accuracy of the data conversion and loading, especially of critical data, before cutting over to the new system.

## 5.5 RISK MANAGEMENT ADVANTAGES

There will be a cultural shift from “fire-fighting” and “crisis management” to proactive decision-making that avoids problems before they arise. Anticipating what might go wrong will become a part of everyday business, and the management of risks will be as integral to program management as problem or configuration management.

## 5.6 CONSEQUENCES OR NEGATIVES OF RISK MANAGEMENT

Management will not have insight into what could go wrong – consequently more resources will be spent correcting problems that could have been avoided sooner, catastrophic problems (surprises) may occur without complete information or adequate knowledge of future consequences, the overall probability of successful completion of the program is reduced, and your program will always be in a crisis. A question asked by many business people is: If risk management is implemented, does that guarantee success? The answer is "No". There are many aspects to achieving program success. Risk management is not a silver bullet. However, it can improve decision making, help avoid surprises, and improve your changes of succeeding.

## 5.7 CONCLUSION

Throughout this chapter we argued that managing risks are vital. The author is of the opinion that project managers will be able to plan more effectively by analysing a project before they proceed. A typical role-player activity list is provided (See Addendum D) and an example of a risk check list (See Addendum E) to complete the discussion. If project managers take risk management in the systems development life cycle seriously, it will reduce the rate at which information technology projects fail.