IT Governance & Risk Management: an integrated multi-stakeholder framework

Raymond Christopher Young[1], Ernest Jordan[2]

1) Macquarie University, Macquarie Graduate School of Management, (raymond.young@gsm.mq.edu.au)

2) Macquarie University, Macquarie Graduate School of Management, (ernie.jordan@gsm.mq.edu.au)

Abstract

IT increasingly underpins most forms of commercial, industrial and government activity. Organisational opportunities and risks related to IT sit better in the field of IT governance than IT project management alone. This is the more apparent when one considers that many decades of research into project management has failed to significantly improve the 80-90% failure rate of IT projects [1].

IT failure has lead to the failure of organizations and the recent spate of corporate collapses and the aftermath of Sept 11 has refocussed attention on corporate governance and security. For all these reasons, the need for a risk management framework in the context of IT governance is growing but to date there has been no solution. It is difficult because many key success factors are beyond the control of the IT function. Researchers and practitioners are recognising the risk management framework must follow an integrated multi-stakeholder approach [1] [2] [3].

This paper lays the groundwork to develop an integrated approach to risk management and IT governance. It does this by reviewing the development of all major traditions of risk management. It then presents the current crisis in the field because of the recognition of the limitations of statistical approaches to risk. Finally, by synthesising the best of all current practices, it proposes an IT goverance framework which is able to communicate risk from an operational level through all decision makers to Board level and beyond.

A case study of a project failure was analysed against this framework and weaknesses in current governance practices were revealed. The framework was shown to hold much promise for practice because it is likely the infrastructure already exists in current business practices to rapidly implement this framework, it leads logically to an escalation procedure for accountability and it effectively addresses the multi-stakeholder issues that confront the modern organization. A future research program has been detailed.

Introduction

The recent collapses of Enron in the US and HIH, One-Tel, Ansett, and Pasminco in Australia has highlighted the inadequacy of the current risk management regime in corporate governance. The groundswell of public opinion for change is the first of many likely triggers to expand the current governance regime to include matters relating to IT governance.

Cross Functional Perspectives

The recent collapses followed a number of high profile corporate collapses in the 80s and numerous reviews around the world all concluded that the Board of directors must bear the responsibility for adequate risk management [4] [5] [6] [7] [8].

Boards have been guided by substantial professional practice in the area of risk management from such perspectives as audit and control, financial management, insurance, OH&S, environmental assessments, operational continuity, crisis and emergency management, strategic management and from the professional practice of 'risk managers'. IT Governance and IT risk management is noticeable for its failure to contribute in any significant way.

IT: Risks & Opportunities

Inadequate IT governance exacerbates the problem by bringing high levels of risk to organizations. Clegg reports 80-90% of IT investments do not meet their performance objectives. Many authors [9][10][11] substantiate the size of the problem and point to the complete demise of companies because of inadequacies in IT governance. Their discussion however tends to focus on one aspect of IT governance: project risk management, and neglects the other two dimensions of IT governance: IT strategy and IT operations [12].

Investments in IT represent, for many businesses, their major sources of opportunities, costs and risks. The new information technologies increasingly underpin most forms of commercial, industrial and government activity [1]. IT investments are increasingly in areas requiring major organisational change for the full benefits to be realised [11]. Effective IT governance therefore reaches beyond the IT function and must be integrated into corporate governance as a whole and requires resolution of the tension between risk and innovation [13].

Developing an integrated IT risk management paradigm in the context of all risk management perspectives

Boards are very aware of IT risk [14] and project risk management has been the main approach to manage the risk but the success rate is still very low [1]. A more integrated approach is needed but progress is hindered because a fundamental issue has not been addressed: the many approaches to risk management have not been integrated into rigorous theories able to facilitate cross functional decision making.

This paper proposes to address this issue by reviewing the development of risk management in all major disciplines. It will highlight the current impasse because of the tensions between the traditional statistical quantitative approach and the context sensitive qualitative approaches. It will then propose a way forward based on a cross functional synthesis of the best practices. It will incorporate but not be limited by AS4360 [15] the world's first risk management standard, the Turnbull report [3] from the UK which sets the latest standard for higher standards of corporate governance, and the work of March and Shapira [16] clarifying actual management approaches to risk.

The contribution of this paper is to use IT Governance as the context to lay the groundwork for an integrative view of risk management and to propose an IT Governance framework based on this integrated view.

> *…No single interest group or profession can 'unlock' all the forces that currently 'conspire' to produce poor performance. In this view the poor performance of new IT systems is the result of a complex and interacting set of forces that will not be easy to change. A great deal of integrated effort is required. Indeed if it were easy, it would have been done already. [1]*

Literature Review

Risk Management

Risk management was recognised to be different to risk assessment in 1983 [2]. The literature in many sub-fields of risk management (e.g. chemicals, health, environment, engineering, insurance) is conceptualised within the dominant economic paradigm assuming decision makers make rational choices based on highest expected utility. For example, Molak's [17] introductory risk management textbook dedicates more than 50% to describing statistical methods to quantify risk for decision makers. Haimes [18] more advanced text adds multi-objective statistical methods to the standard suite of mathematical assessment tool and advances the field to emphasise the importance of multi-stakeholder techniques to identifying risks.

Most risk management writers recognise it to be a very young field. Molak [17] expresses concern when risk management experts are pitted against one another on controversial issues such as the environment and the nuclear debate to show the current inadequacy of the discipline. A 1996 US National Research Council [2] on this matter concluded that in the past we applied risk analysis "to relatively simple problems … but now that we are asking more complex questions, we are finding risk analysis is incapable of producing adequate answers" and that "the [current] view of risk characterization[1] is seriously deficient".

---

[1] Risk characterization is the process to translate risk assessment information into a form usable to a decision maker.

The National Research Council report is particularly relevant because they were trying to reconcile current paradigms with an environment with loosely formulated risk problems, multiple decision criteria and multiple decision makers; factors which are common to almost every business decision. Their recommendations for "a more robust construction" are particularly helpful in pointing out that perspective of all stakeholders must be incorporated.

> *"Adequate risk analysis and characterization thus depend on incorporating the perspectives and knowledge of the interested and affected parties from the earliest phases of the effort to understand the risks." [2]*

Beck [19] was one of the first post-modern philosophers to understand that risk is best understood in the question:

> *Where and how does one draw the line between still acceptable and no longer acceptable exposures? [19]*

Beck [19] does not dismiss the need for statistics and traditional scientific rational analysis, but makes the point that we have reached the limit of what risk analysis can do.

> *Scientific rationality without social rationality remains empty,*
> *but social rationality without scientific rationality remains blind. [19].*

Financial Risk Management

Risk management also has a substantial literature and practice in the financial arena. This sub-field appears not to have been influenced at all by the self-reflective findings reported above.

Led by the banking sector in Basle, financial risk managers continue to set the risk management standards to lead the corporate world. Having conquered market and credit risk, they are now pushing for operation risk measures to be implemented internationally by 2007, and there is talk of the four major Australian banks to be compliant by 2004.

Despite this confidence, recent corporate collapses have highlighted the inadequacy of the current risk management regime in corporate governance. The business world is faced with conflicting messages between the financial risk management regime of the banking sector and the likely legislative fallout from the latest round of corporate collapses.

Problems in the financial management literature

There are however suggestions that the confidence from the financial sector is misguided.

Reufli [20] reports "early empirical tests of the CAPM by Black, Jensen and Scholes (1972) and Fama and McBeth (1973) found a positive relationship between beta [a measure of risk] and average returns in the period 1926-68" but "more recent empirical studies (Reinganum 1981, Lakonishok and Shapiro 1986) … could not demonstrate [the same relationship] for the period 1963-90". Finally Fama [21] one of the major figures in the financial management literature, revisited his early work in a major study for the entire period 1926-90 and concluded "the SLB model does not describe the last 50 years of average stock returns".

"This is a strong statement made by two leading researchers in a leading journal in the field. Understandably, the response of financial economic researchers has been mixed" [20] but as early as 1987 Boyadian [22] reported the practice in investment banking has mainly been to marginalise risk calculations as a factor in decision making.

> *"financial data really only helps with an understanding of financial risks.*
> *The process by which a company makes money has economic, social, and human dimensions that are as important as the financial aspects [22]"*
>
> *"The empirical evidence strongly suggests that risk is bereft of reward."[22]*

The crisis in strategic management and IS literatures

Risk has been studied for many decades in strategic management literature [23] and openly recognises the implications of Fama's work. There has been the recognition that " researchers have not captured the concepts of risk employed by managers" [20] and that "findings in the financial economics and management science literatures have raised serious questions about strategic management's two most widely used measures of firm and business risk: beta (or its variants) from the Capital Assets Pricing Model and simple variance (or its variants)" [20] .

Ruefli has stated the strategic management literature is facing a crisis [20] because it has borrowed most of its risk concepts (CAPM, beta, risk return relationships) from the financial management literature and now has no credible way to discuss risk. He reports that strategic management researchers are actively exploring alternative measures of risk such as downside risk and surveys.

The implication to the IS literature is compounded because it has borrowed all its risk concepts from the strategic management and from the financial management literatures.

Promising Directions

Having established that there is something of a "crisis" in the field of risk management, it seems unwise to build an IT risk management and governance regime solely around the current risk management paradigms. Having said that, it needs to be remembered that the issue with IT projects is that many success factors lie outside the control of the IT function and any framework proposed must therefore integrate with the larger risk management frameworks.

Two additional literatures should be examined before proposing any framework, the corporate governance literature (because the Board of directors must bear the responsibility for adequate risk management) and the management literature (because the Board relies on management advice to carry out its responsibilities).

Corporate Governance Literature

The key events that have shaped the corporate governance literature are high profile corporate disasters. The focus is on maximising shareholder returns while minimising risk through adequate controls.

The introduction to this paper described the corporate collapses in the 1980s, the subsequent reviews and the worldwide acceptance of the Cadbury finding [6] that the Board of directors must bear the responsibility for adequate risk management. In 1998 Hampel [7] reviewed the effectiveness of the Cadbury practices and concluded that risk management should not overemphasise controls and be so prescriptive that it is perceived as a 'box ticking exercise'. The Turnbull Report [3] took Hampel's findings to develop recommendations that are now a requirement of listing on the London Stock Exchange.

Turnbull is being promoted in other countries for business reasons rather than compliance [14] but it does not provide the specifics to manage IT related risks. Recent failures suggest that the latest risk management regimes in corporate governance and even Turnbull may be inadequate. In particular they are showing the inadequacy of balance sheet measures as a risk management tool [24].

Enron and Turnbull have very big implications for the auditing profession with its focus on financial controls.

IT Governance

With this background we can consider the IT Governance Institute's [25] COBIT recommendations for IT governance. COBIT was prepared primarily by IT auditors to bridge the gap between the overall business control models like COSO and more focused IT control models like BS7799, AS/NZS 4444.2 [26], ISO 17799:2001 [27] and the NIST Security handbook [28] to "provide a foundation that is more closely linked to business objectives while focussing on IT". Their definition of IT Governance has an emphasis on control.

> *A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.*

The COBIT framework systematically groups the IT best practices that are believed to improve control of 34 IT objectives[2]. Major risks outside the control of IT directly such as failure of the organization due to IT projects or IT strategy are not addressed directly and in comparison to Turnbull: COBIT is more complicated, more prescriptive, less integrated into existing business processes and therefore more difficult to implement. It does however contribute a very valuable list of KPIs and KRIs (leading indicators of risk) and relates them to various IT processes.

---

[2] COBIT interprets IT Governance practice as a distinct subset of Enterprise governance and specifies a framework to report on whether 34 IT activities are meeting 34 defined IT objectives (such as alignment of IT with the business, IT resources being used responsibly and IT related risks being managed appropriately). The IT risks described within COBIT are security, reliability and compliance.

Management Decision Making Literature

The management literature on risk is quite diverse but two distinct streams can be recognised. Management decision sciences is the first stream and can be considered to be normative, following the statistical tradition of all the other risk management disciplines. Behavioural management decision-making stands in stark contrast and is focused on how managers handle risk in practice. This stream is most easily identified with Simon, March and Shapira.

Simon [29] was a contemporary of the early 20th century economists but he did not follow the dominant paradigm of economic rationalism. Rather he posited the notion of 'bounded rationality' and the 'satisficing principle' which recognised that human beings do not have the capacity to assess all the risks before making a decision and their practice is to search through a limited set of options until they find a good enough alternative. He was followed by March & Shapira [16] who demonstrated that not only do managers not follow the statistical tradition for measuring and managing risk; they actually reject it as a valid approach.

Shapira's [30] findings have big implications for any IT Governance framework.

> "In the world of executives, probability estimates are treated as unreliable and subject to post-decision control, and considerations of tradeoffs are framed by attention factors … Managers look for alternatives that can be managed to meet targets, rather than to merely assess or accept risks… [managers] believe in their ability to control the odds. This trend is facilitated by systems of organisational controls and incentives that dictate risk taking behaviour in significant ways.
>
> It is conventional in discussions of management to deplore the pattern of risk taking observed in management … In the short run, if we wish to encourage or inhibit risk taking on the part of managers, we probably need to shape our interventions to meet the ways in which managers think. For example, it may be easier to try to modify managerial attention patterns and conceits than to try to change their beliefs about the likelihood of events or to try to induce preferences[3] for high variance alternatives.
>
> Achieving change by developing a sound theory of decision-making should include the descriptive, normative and prescriptive aspects together (Bell, Raiffa, and Tversky, 1988), as well as consideration of the larger social context in which managers operate.
>
> It might be preferable to have managers imagine (sometimes falsely) that they can control their fates, rather than suffer the consequences of imagining (sometimes falsely) that they cannot. What is harder to determine … are the details of the ways in which such managerial impulses for discovering methods to improve the odds can be reconciled with standard, rational-calculation-based decisions to induce more sensible managerial risk taking."
>
> [30, pp128-132]

Summary of literature

We conclude our literature review by tying together the common themes and highlighting problematic issues.

1. The first major theme is that all relevant literatures (with the possible exceptions of financial & engineering risk management), recognise our current approaches to risk management are recognised not to be working effectively enough.
2. All literatures recognise an increasing role for judgement over analysis. With complex issues, the process to ensure multi-stakeholder perspectives is the key.
3. The biggest issue currently faced is how to define risk in terms acceptable to all stakeholders.
4. The dominant risk frameworks that need to be considered are: mainstream Risk Management [2], Turnbull [3], Standards (COBIT [25] , BS7799 [26][27], AS4360 [15], PMBOK, Basle) and March & Shapira [16][30]
5. The outstanding issue is how to reconcile the predominant managerial practices (which reject the normative approach.), with the predominant paradigms of understanding and managing risk (which are normative and based on probability)

---

[3] Shapira [30] quotes (Baker, Jensen and Murphy, 1988) to show that incentives are potentially one way of encouraging sensible risk taking, but that the current practice is not optimal. "Rewarding and penalizing employees is not done in a systematic way but, only if a critical level of success (or failure) is reached. These critical levels may not be defined *ex ante* in a clear manner".

A New Framework

The self reflective considerations in the risk management literature and the groundswell of feeling in the corporate governance area is leading us into some sort of convergence of the current practices and behavioural management decision making findings.

Simplicity: Framing attention on business objectives

Turnbull [3] and Shapira [30] are almost identical in advocating simplicity (focus on 10-15 significant risks). They also recommend focussing attention on agreed frames of reference (eg. business objectives, department goals) and defining risk as events that can lead to deviation from these reference points. NB. This implies that events that do not affect the department or business objectives are not considered risks.

Multi-stakeholder Perspective: risk is everyone's business, use a common risk language

Turnbull [3] and Stern [2] both emphasise multiple stakeholders. In Turnbull's terms "risk is everyone's job" and "there needs to be a common risk language". This is particularly relevant for IT project risk because the reason for poor performance often lies outside the stakeholders within the IT discipline alone [1].

A common IT risk management language

There are many risk management and IT security practices and the best of these practices have been codified into various Standards. These Standards all have something to offer and could form the basis for a common risk language once they were all integrated into a common framework.

The schematic diagram in Figure 1 tries to show the relationships between the various Standards in the context of a generic risk management framework (such as AS/NZS 4360:1999[4]).

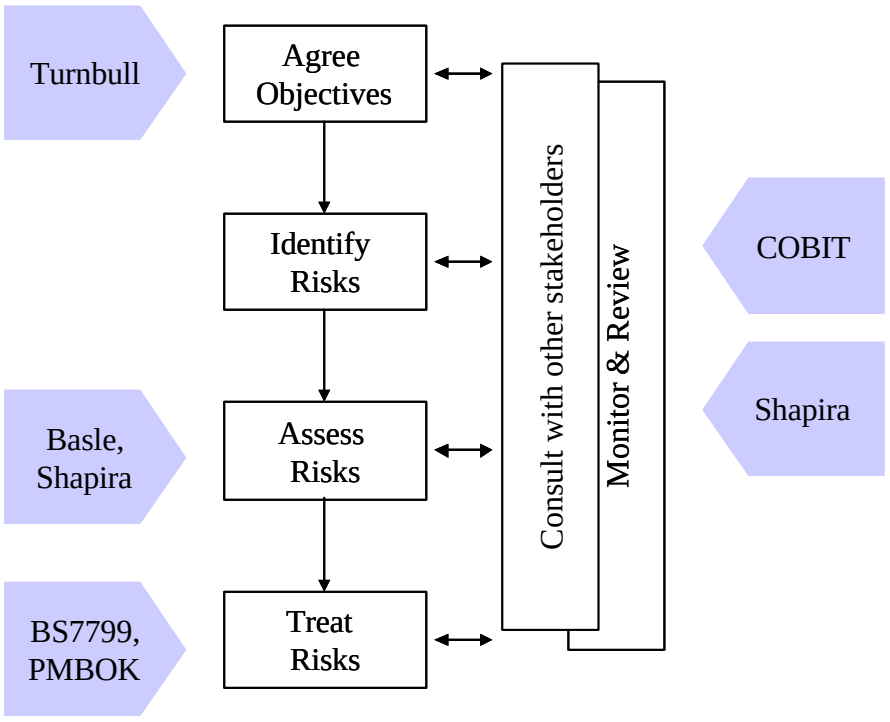


Figure 1: Relation of dominant risk standards to a generic risk management framework

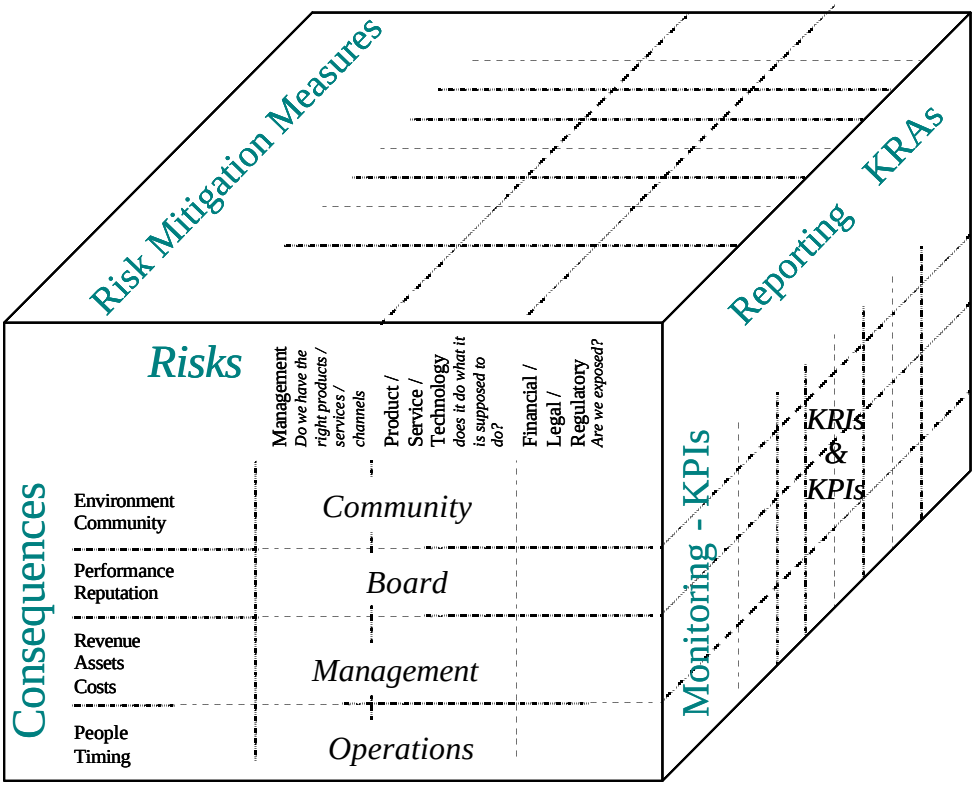
[4] The International Standards Organization has considered this standard for adoption as a world standard [31]

An Integrated Multi-Stakeholder Framework

Turnbull suggests that 'many fundamentals of good risk management and internal control are already in place' but gives no real guidance for identifying and implementing any missing layers (in IT for example). A more complete framework is needed because although Turnbull and most of the other dominant standards recommend a multi-stakeholder view of risk, none address all the issues and none have provided enough guidance on how a multi-stakeholder input should be implemented or what the common risk language could look like. The new framework needs to be integrated with other dominant frameworks rather than compete with them and complicate the matter further.

The framework shown in Figure 2 integrates all the promising recommendations and offers a context for IT Governance to be integrated into mainstream corporate governance practices and all other risk management practices. The strength of the framework is that it integrates all risk management approaches and reconciles the conflicting risk management paradigms. It does this because the multi-stakeholder perspective shifts the emphasis from analysis of risk to judgement of what is acceptable. It follows Shapira's iterative process of identifying and assessing risks and it can use statistical analysis to help decision-making without any over reliance on quantitative techniques.

> *The most important thing is to make risk assessment transparent. The thought process that goes into evaluating a particular hazard is more important than the application of some sophisticated mathematical technique or formula, which may often be based on an erroneous assumptions or models of the world. [17]*



This model addresses this and fully integrates IT Governance into the scope of Corporate Governance and is illustrated above and described below in the order it would be most logically implemented:

1. Multi-stakeholder view to identify & prioritise risks
2. Select & implement Risk mitigation measures
3. Report & monitor KRIs (key risk indicators) and KPIs (Key PerformanceIndicators)

Multi-stakeholder view of Risks and Consequences

The first dimension is based loosely on the generic models of risk management (Turnbull & AS4360) and shows how to implement a multi-stakeholder perspective to manage risk.

The starting point is to identify the key stakeholders and to list the important consequences for each stakeholder group. Consequences are the stakeholders (business or department) objectives. Generic objectives are described in the model and these should be updated over time when the organisational players become aware of the actual words different stakeholders use.

It is likely there will only be 2-3 stakeholder objectives for each stakeholder group. The consequences / objectives are grouped by stakeholder.

This multi-stakeholder view of Risks and Consequences is significant for a number of reasons:

- A small number of stakeholder objectives is used to 'frame' attention.
- Risks, which could be very numerous, are assessed according to whether they affect a stakeholders objectives to highlight 10-15 significant risks.
- The determination of the riskiness[5] may follow many different approaches. It could be done quantitatively, intuitively, through consultation or any other means the organization feels comfortable with. It is likely to be an iterative process starting from the first person to reporting a risk and the likely discussions to assess and reframe the risk until it is perceived to be acceptable.
- The multi-stakeholder approach is the key to effectively identify, assess, initiate treatment and maintain a focus on only the 'significant risks'.
- Accountability underpins the effectiveness of the framework, and all identified risks should be signed off.

As risks are identified by anyone in an organization, they will alert all the stakeholder groups they believe will be affected. This initial assessment will be made on the basis of whether the person 'reporting' the risk thinks a business objective in another stakeholder group will be affected or not. It will be the responsibility of a designated stakeholder within the notified stakeholder group to investigate whether the alert is correct or not. If the investigator is not sure, he/she should escalate within his/her group until the accountable person signs off on an appropriate action.

The result of this process will be that:

- Each stakeholder group will know what risks are likely to affect the things they care about, and they will know which of these risks deserve more or less attention.
- The relationship between each risk and the different stakeholder groups will be clearly identified.
- The appropriate allocation for responsibility for managing the risk is more likely to be vested with the highest relevant authority[6]

Although each stakeholder group will end to focus on the 10-15 risks with the biggest impact on their business objectives, the number of total risks may be very large. Categorisation will be unique for each organization and could follow the Basle system (Financial risks, Credit risks, Management risks), the more generic business classifications[7] shown in the schematic model or some other system that reflects the major stakeholders perception of how they operate.

---

[5] Risks are events that can affect the consequences / objectives [32].

[6] For example, if an IT project has the potential to significantly improve the profitability of the business, the board may want to sign off on the project and require the project manager to report to a senior manager who is responsible for realising the benefits or minimising any downside. This senior manager may authorise delays to the implementation of a project because he believes it will enhance the likelihood of achieving the desired benefit. A project manager alone is likely to manage on the basis of on time on budget without significant regard to the expected benefits.

[7] Boyadjian [22] makes a case for the category Strategic Business Risk – "If we want to know how a company will do in the future, we should be asking what it is the company must do and do well in the future"

Risk Mitigation Measure

There are many risk mitigation measures available. The BS7799, PMBOK, NIST standards lists some recommended IT risk mitigation measures. Risk in areas such as OH&S, the environment, legal liability, etc. all have their traditional treatments and the proposed model integrates all the tools into one framework. The total range of mitigation measures constitute a suite of tools the organization can implement as appropriate.

The strength of the model in this area is to show which risk(s) a particular risk mitigation measure is addressing. The issue is that most risk mitigation measures cost either time and/or money and it is unlikely organizations want to blindly follow all the measures in any one Standard merely for the sake of certification. The goal is to manage risks and if a multi-stakeholder approach was followed to determine the most critical risks, then the risk mitigation measures selected will address the most important risks. If the risks have been quantified or affect strategic goals, it may be possible to cost justify implementation of certain measures, and if not, the funding for particular measures may still be able to be allocated back to the stakeholder groups that benefit the most from the measure.

Reporting KRIs and Monitoring KPIs

The stakeholder objectives identified in the first step are probably already being measured by some KPI. They may even be defined in terms of the target level and minimum acceptable (survival) level. The integrated multi-stakeholder framework adds to an existing control environment Key Risk Indicators (KRIs).

KRIs are forward indicators of risk and should probably be based on some measure of the effectiveness of the risk mitigation measure. In contrast KPIs are lagging indicators of progress in meeting stakeholder objectives.

The KRIs may not[8] be in the same units as the KPI of a stakeholder. Some organizations may want to determine the correlation between KRIs and KPIs but other organizations will be satisfied to have an early warning system of potential problems. It is incumbent on the implementer of the risk mitigation measure to agree on a relevant KRI, and the COBIT guidelines may be used as a starting point.

The implementer of any risk mitigation measure should be responsible to provide KRI data to all stakeholders affected by the risk being managed.

Implementation of the IMS risk management framework

The next section tests the integrated multi-stakeholder (IMS) risk management framework to evaluate whether it can be applied to avoid risks more effectively than current practices. Before proceeding it is appropriate to recap the key steps for implementing IMS risk management:

1. Multi-stakeholder identification of Consequences & Risks
    a. Each stakeholder group identifies their objectives. It is better if this is formally clarified through the normal business planning process, but the objectives can be recognised tacitly. As risks are identified, the importance of various tacit objectives can be clarified through consultation.
    b. As risks are identified by individuals, affected stakeholder groups are notified.
    c. Affected stakeholder groups assess the risk iteratively to determine its significance.
    d. A key stakeholder is made responsible for initiating a risk management response
2. Selection and implementation of a risk management measure.
3. New KRIs, probably based on the risk management measure, are reported to the affected stakeholders. There is no change to the existing reporting of KPIs measuring stakeholder objectives, (although some may be added).

---

[8] A KRI may be number of attacks on the firewall but a KPI may be customer perception of trustworthiness as measured by market share.

Application of the IMS Risk Management Framework to a case of IT failure

Appendix 1 details an actual case of IT failure experienced by one of the authors. The key details of the case are summarised and compared to what would have happened if the IMS risk management framework had been followed. The key events are listed below in tabular form and the Integrated Multi-Stakeholder (IMS) Risk Management response is listed against each key event.

The case study was of a very common business situation, the integration of computer systems following a merger. The IT strategy following the merger was to support the business needs by being much more cost efficient internally and to produce crucial profitability information to manage in a very tight margin business. It was not recognised as a priority at the time but it was also strategic to build and maintain the functionality into the computer systems to meet customer needs in highly customised ways because that improved customer service and increased customer switching costs.

<table>
<tr><th>Date</th><th colspan="2">Key Event</th><th>IMS Risk Management Response</th></tr>
<tr><td rowspan="5">Jun 96</td><td colspan="2">XYZ merges with MF
transition from a high profit mainframe specialist maintenance business to highly cost competitive general maintenance business</td><td>Objectives recognised tacitly
market share, customer satisfaction
costs, revenue
on-time billing
cost per service call</td></tr>
<tr><td colspan="2">IT tactical strategy developed
to rationalise 11 systems down to 3 systems</td><td rowspan="2">Risk identified
Poor reputation of MF system developers

Risk Assessment
develop risk management plan</td></tr>
<tr><td>XYZ billing system</td><td>MF call system (?)</td></tr>
<tr><td>XYZ Proj. Mgr to merge billing systems</td><td>MF Proj. Mgr to merge call system</td><td>Risk treatment
formally appoint XYZ senior manager to sponsor project. Structure MF project manager to report to XYZ manager</td></tr>
<tr><td>Jul 96</td><td>Extensive liaison between XYZ and MF billing system IT staff</td><td rowspan="3">Almost no coordination between MF and XYZ call system IT staff</td><td rowspan="3">Risk identified
customer service, business strategy at risk

Risk assessment
XYZ staff resigned to MF call system being imposed against their will

Risk treatment
escalation to CEO, Board</td></tr>
<tr><td>Nov 96</td><td>Successful merging of billing systems</td></tr>
<tr><td rowspan="4">Jan 97</td><td>XYZ Proj Mgr promoted to CIO</td></tr>
<tr><td colspan="2">IT staff advise new CIO of technical problems</td><td>Risk identified
technical problem expressed in terms of impact to revenue</td></tr>
<tr><td colspan="2">CIO follows up with senior managers</td><td>Risk assessment
managers would not listen to CIO

Risk treatment
escalate to CEO, Board or assume direct responsibility</td></tr>
<tr><td colspan="2">Go / No Go meeting</td><td>Risk treatment
Senior XYZ managers would have signed off, CIO would have been at the meeting</td></tr>
<tr><td colspan="2">Disaster meeting</td><td>Risk identified and assessment
all relevant senior managers would have been at meeting., Technical problem would have been expressed in terms of impact to revenue, customer service and business strategy

Risk treatment
Probably would have decided to reverse the merger rather than fix the problems</td></tr>
<tr><td>Feb 97–
Apr 97</td><td colspan="2">Changes rectified

T&M revenue (30%) not collected</td><td rowspan="2">Conclusion
IMS Risk Management practices would have had 4 chances to intervene and is very likely to have either completely avoided any IT project failure or at the least minimised any adverse impact on critical business objectives.</td></tr>
<tr><td>Dec 97</td><td colspan="2">Missed all financial targets

Customer service reputation affected</td></tr>
</table>

Table 1 Application of the IMS risk management framework to the Risky Integration case

Eleven systems were being rationalised down to three systems. The choice of the three systems had been very political, but once the decision had been made the majority of the staff resigned themselves to the decision and got to work. The integration was planned in three stages and the first stage had been achieved without difficulty. The second stage was technically easier than the first and was being managed by an experienced project manager. There had been some warning signals of potential problems but to most they seemed to be matters relating to personal politics. No one really expected any major problems.

Unfortunately all the early warning signs were missed, a last minute chance to delay the project was not followed up with the attention it deserved and an ineffective go/no go meeting allowed the stage two to proceed and plunge the company into major financial distress. 30% of the revenue could not be billed and a number of major customers threatened to leave. All the financial targets were missed, none of the managers received their bonuses and 3 years later the company received a bottom 5 rating for customer service.

The distress of the situation could be remembered vividly by one of the authors and even now, five years later he still wondered what could have been done differently. When the case was analysed it was revealed IMS Risk Management practices would have thrown up four different chances to intervene and is very likely to have either completely avoided any IT project failure or at the least minimised any adverse impact on the critical business objectives. The results were particularly surprising because there was no need to implement any complex risk management procedure to realise the benefits, nor was there any need to use sophisticated mathematical tools to assess riskiness. The two key ingredients were:

- To communicate in terms of the language of the stakeholder, a language which was accessible to all staff (in this case the potential loss of 30% revenue and loss of functionality to major customers)
- To ensure a key stakeholder group is accountable for the results, and to escalate to MD and Board level if this is not occurring. This would normally be a big ask except that the consequences of this case were so severe that because the responsibility was not committed up front, everyone paid at the end. It required only the effort to communicate in terms of the key objectives of a stakeholder.

Discussion

The application of the IMS risk management framework in this case has confirmed some key concepts expressed by Clegg [1].

- The main language of risk is based on resolving conflicting values
- Better project management is not the solution
- Technology is driving change, but it is bringing unmanaged risk, because we are not controlling it properly.

The main language of risk is based on resolving conflicting values. (It is not mathematics)

"One of the strongest and clearest messages that emerges … concerns the levels of fragmentation within organizations . Company functions and specialisms were described as highly differentiated and separate, often with their own set of professional interests, agendas and specialist languages. This view of fragmented organizational life and its associated territorial and political battles helps to explain why co-ordinated effort proves very difficult to manage. This fragmentation is … especially germane to the domain of new technology … however … IT can be regarded as a special case of a more general phenomenon" [1]

The multi-stakeholder approach is ideal to resolve co-ordination issues and the case showed it was not difficult to connect a technical issue to an objective of another stakeholder. Once they can speak in the same terms, the will to resolve the problem arises if the issue is perceived to be significant.

IT Project Management

Project managers were criticised for their lack of attention to the human and organizational aspects of the systems that they are responsible for developing and introducing. In their defence however, it was recognised that people working in these roles are usually not expected to address these issues, are not rewarded for doing so, are not educated or trained in them, nor supported adequately in any endeavours that they make in these areas. [1]

The case showed that the resolution of the issue required a key stakeholder to be accountable, and for the key stakeholder to manage the project manager. The project in the case was experiencing a great deal of passive resistance and negativity. It is very unlikely a project manager could significantly influence this and it is difficult to see how even the best project management methodology would have made any difference in this respect.

… project management methods and tools are in widespread use; in part this reflects the common concern that projects run over time and over budget. Unfortunately these same techniques are widely criticized. … For example, some reported that these methods simply do not work, that they omit too much, and that they are too technically oriented. [1]

Currently technology is driving change, but it is bringing unmanaged risk, because we are not controlling it properly.

Regarding the impact of new technology on the way in which work is organized and upon individual job designs, the majority view was that this is hugely important but largely ignored in practice. Again this was seen as a topic that is significantly under-estimated. Where it is addressed this is because the job design implications of technical change are discovered, usually relatively late in the development process. These findings demonstrate that IT remains technology-led … IT is not seen in an integrated way as raising sets of related business and organizational issues. [1]

The business process issues were not addressed at all by the experience project manager in the case. Her approach was to implement the system and to fix the problems afterwards. In hindsight, this was completely irresponsible but the business mangers allowed her to do it. The best quote from a manager in the case is "if we had known the consequences, we wouldn't have been so cavalier about it", yet this same manager was clearly the one who had the most to lose by implementing badly. He simply did not connect the IT issues with his business objectives.

Conclusion

This paper has laid the groundwork to develop an integrated approach to IT governance and risk management. It has reviewing the development of all major traditions of risk management. It has presented the current crisis in the field because of the recognition of the limitations of statistical approaches to risk. Finally, by synthesising the best of all current practices, it proposed an integrated multi stakeholder risk management framework which is able to communicate IT risk from an operational level through all decision makers to Board level and beyond.

A case study of a project failure was analysed against this framework and weaknesses in current governance practices were revealed. The framework holds much promise for practice because it is likely the infrastructure already exists in current business practices to rapidly implement this framework, it leads logically to an escalation procedure for accountability, it effectively addresses the multi-stakeholder issues that confront the modern organization and reconciles the conflict in risk management paradigms.

Further research should be conducted against more case studies of IT failure to refine the tool and then testing in an action research environment. The testing should try to look for situations where competing risk management regimes may be vying for managerial attention and should investigate issues with embedding the framework into organizations.

References

[1] Clegg, C., C. Axtell, et al. (1997). "Information technology: a study of performance and the role of human and organizational factors." Ergonomics **40**(9): 851-871.

[2] Stern, P. C. and H. V. Fineberg, Eds. (1996). Understanding Risk: informing decisions in a democratic society. Washington, D.C., National Academy Press.**40**(9): 851-871.

[3] Turnbull, N. (1999). Internal Control: Guidance for Directors on the Combined Code. London, The Institute of Chartered Accountants in England & Wales.

[4] COSO: Committee of Sponsoring Organisations of the Treadway Commission (1994). Internal control - integrated framework. New Jersey, American Institute of Certified Accountants.

[5] The Business Roundtable (1997). Statement on Corporate Governance, The Business Roundtable.

[6] Cadbury (1992). The Financial Aspects of Corporate Governance. London, Gee Publishing.

[7] Hampel, R. (1988). Committee on Corporate Governance. London, Gee Publishing.

[8] Bosch, H. O. (1995). Corporate Practices and Conduct. Melbourne, FT Pitman.

[9] Applegate, L. M., F. W. McFarlan, et al. (1999). Corporate Information Systems Management. Boston, Irwin McGraw-Hill.

[10] Turban, E., E. McLean, et al. (2002). Information Technology for Management. New York, John Wiley & Sons.

[11] Remenyi, D. (1999). Stop IT project failure through risk management. Oxford, Butterworth Heinemann.

[12] Sambamurthy, V and R.W. Zmud (1999) Arrangements for information technology governance: A theory of multiple contingencies. MIS Quarterly 23(2) 261-290rr

[13] Vitale, M. (2001). The Dot.Com Legacy: Governing IT on Internet Time. Australasian Conference on Information Systems, Coffs Harbour, Southern Cross University.

[14] Young, R. C. and E. Jordan (2002). Lifting the Game: Board views on e-commerce risk. Paper to be presented at IFIP TG8.6 The adoption and diffusion of IT in an environment of critical change, Sydney.

[15] Standards Australia (1999). AS/NZS4360:1999 Risk Management. Sydney, Standards Association of Australia.

[16] March, J. G. and Z. Shapira (1987). "Managerial perspectives on risk and risk taking." Management Science **33**(11): 1404.

[17] Molak, V., Ed. (1997). Fundamentals of Risk Analysis and Risk Management. Boca Raton, Lewis Publishers.

[18] Haimes, Y. Y. (1998). Risk Modelling, Assessment, and Management. New York, Wiley.

[19] Beck, U. (1992). Risk Society: towards a new modernity. London, Sage.

[20] Ruefli, T. W., J. M. Collins, et al. (1999). "Risk Measures in Strategic Management Research: Auld Lang Syne?" Strategic Management Journal **20**: 167-194.

[21] Fama, E. F. and K. R. French (1992). "The cross-section of expected stock returns." Journal of Finance **67**(2): 427-465.

[22] Boyadjian, H. J. and J. F. Warren (1987). Risks: reading corporate signals. Chichester, John Wiley & Sons.

[23] Bettis, R. A. and H. Thomas, Eds. (1990). Risk Strategy and Management. Greenwich, Connecticut, JAI Press Inc.

[24] Whitely, P. (2002). Powercut. Global HR March: 24-29

[25] COBIT (2000). Framework. Rolling Meadows, IT Governance Institute.

[26] Standards Australia (2000). AS/NZS4444:2000 Information Security Management: specification for information security management systems. Sydney, Standards Association of Australia.

[27] Standards Australia (2001). AS/NZS / ISO 17799:2001 information technology-code of practice for informational security management. Sydney, Standards Association of Australia.

[28] National Institute of Standards and Technology (1995). An Introduction to Computer Security: the NIST handbook: NIST special publication 800-12. Washington, DC, U.S. Department of Commerce.

[29] Simon, H. A. (1945, 1947, 1957,1976). Administrative Behaviour. New York, The Free Press.

[30] Shapira, Z. (1995). Risk Taking: a managerial perspective. New York, Sage.

[31] Price Waterhouse Coopers (1999). Enhancing Shareholder Wealth by Better Managing Business Risk, IFAC Study 9. New York, International Federation Of Accountants - Financial and Management Accounting Committee.

[32] ISO (2000). Working Draft for ISO Guide - Risk Management Terminology. Japan, ISO/TMB Working Group on Risk Management Terminology.

Appendix 1: Risky Integration Case

Difficulties consolidating IT systems following a merger of two computer services companies

Prologue

In 1996, XYZ merged with Mainframe Australia Ltd to form the third largest computer services company in Australia. In order to realise the benefits of the merger, the IT systems were rationalised. The decision to select FSMS over ASIS as the call system was political rather than technical and many difficulties were encountered in the merger. The following case study describes the context of the key events. Names may have been changed to protect identities.

Chris Little was excited. He had just been promoted to a CIO role and it reflected the confidence senior management had in him. He had successfully overseen the creation of an IT infrastructure for a newly merged computer services company and he was convinced a new data warehousing initiative was the next step to use information to drive higher levels of profitability.

Chris had not been taking the lead with the call system conversion. As far as he knew it was on track and although it was a key operational system he felt he had bigger fish to fry. He was feeling so good that he decided that he would take his long overdue holiday and come back to get started on what he felt was the more strategic data warehouse project.

Prior to leaving for his holiday, two 'techies' made him aware of a technical problem relating to the merging of the two call systems.

> "This merger is never going to work!"
> "Oh?"
>
> "They're decommissioning the ASIS call system but FSMS doesn't have a flag for T&M and they don't report calls the way we do"
>
> "Have you discussed this with Cindy (the project manager)?"
> "Yes"
>
> "what about John (the support services [IT & Logistics] manager)?"
> "We told him first"
>
> "and Dan (the operations manager)?"
> "Yeah he knows"
>
> "OK, I'll have a word with them. Thanks for letting me know"

In the same way that Steve Stout had been the owner of the successfully merged billing systems, Dan and John were the owners of the to be merged call systems. Unlike Steve however, neither Dan and especially not John had fully agreed with the choice of the new system. They had resigned themselves to the decision. In addition to this, John was no doubt extremely unhappy to be losing control of the IT function that had previously reported him. With his promotion, Chris as the new CIO would gain control of the IT function, but he had not yet assumed the responsibilities of the role and did not know the significance of 'T&M'.

> "Cindy, what's the deal with the T&M flag?"
> "Oh they're overreacting. We'll be able to invoice. They're annoyed their system is being pulled"
>
> "John, what's the issue with this merger?"
> "…leave it to Cindy. We've explained it to her, she's got it under control"
>
> "Dan, if anything goes wrong with the merger, it's going to hurt you the most. I won't be starting till next week, so can you make sure all the players sign off at the 'go/no-go' meeting this Friday. Especially this T&M thing. If there's anything fishy, I'm happy to delay it till we're 100% ready"
> "yeah, me too"

Difficulties with the Call System consolidation

Despite the assurances, the system merger proceeded with disastrous results. A major functionality: T&M invoicing, could not be processed in the new system. Because of the changed reporting system, some customers also lost the ability to monitor the progress of their calls.

The state managers were alarmed and a conference call of the senior management team was convened. The issue was escalated to the MD of Mainframe Australia.

Later that day a crisis meeting of the technical staff was held. Chris (who had just returned from vacation) wanted to reverse the conversion and revert back to the two separate systems. He did this with the blessing of Ed Lin the marketing manager, but Mick Bard, Ed's representative at the crisis meeting, did not support this option. Cindy believed that the problems could be rectified within a month but at that stage, no one was sure what all the problems were. Dan felt that if the problems could all be fixed within a month, the pain of fixing the problem would not be as great as the pain of reversing the conversions. Mick agreed.

Everyone knew the decision had to be made that day because further delay would have made it impossible to reverse the conversion.

The decision

Chris responded to the pressure by insisting that the specific problems be itemised before committing to any option.

Within hours, it was reported that 27 key fields had never been considered in the conversion and the business processes such as T&M invoicing had not been discussed. Estimates of the time it would take to fix 21 of the crucial fields were between one to six weeks. None of the technical staff at the crisis meeting supported a decision to reverse the conversion, because they felt it could be fixed. The two business managers in the crisis meeting, Mike Bard from marketing and Dan Scarlet the operations manager also strongly supported the decision to go ahead.

Mike's boss told Chris he preferred to reverse the decision but it was apparent he had not told Mike. Chris personally wanted to focus on the data warehouse initiative but if he were to be the lone voice wanting to reverse the conversion he could make a lot of enemies for no reason i.e. to go back to the old system was to signal that it had not been done right and people's careers would be affected. The atmosphere of the meeting was very intense. Careers were on the line…

Dan was the logical owner of the system. If he wanted to go ahead Chris would do the 'right thing' and help fix the problems. He committed the organization to go ahead.

The business environment and IT Strategy

Computer maintenance services had traditionally been a very high margin business for mainframe computer manufacturers. Once a customer bought a proprietary mainframe computer, they had no choice but to rely on the manufacturer for parts and maintenance.

Technological change however, was changing the market rapidly. The rapid improvement in the capabilities of mid-range computers and PCs made it possible for customers to run their mission critical IT applications on lower cost platforms. The market for mainframe computers was shrinking and it was no longer the centre of IT infrastructures. The mainframe was now only one component of a complex IT environment where hardware was sourced from many suppliers. The need for fast service for mission critical platforms remained, but highly cost competitive low margin PC maintenance service providers were squeezing the fat profits.

The merged company took full advantage of the new IT environment by sourcing 2nd hand parts from the US and breaking IBM's monopoly on mainframe computer parts. They sourced inventory and trained staff to service most brands of mainframe, mid-range and PC computers and they marketed themselves as a multi-vendor computer maintenance services provider.

Cultural differences

The merger however, reflected the contradictions in the market. The merged company had gross margins of around 6% compared to the old Mainframe Australia business of around 20-30%. Mainframe Australia's culture reflected the high service high margin proprietary mainframe market. XYZ in contrast was very cost sensitive and they often deliberately chose to provide lower levels of customer service for lower profitability customers eg. They reduced inventory to reduce costs but they had to balance this against higher staff costs because engineers may have to travel to customer sites many times before fixing a computer problem. Note: the key performance measure in the industry is downtime.

XYZ management's style were more appropriate in the new business environment but the overall corporate goal was to keep their high margin mainframe customers for as long as possible before migrating them off mainframes to more cost effective and lower margin mid-range and PC platforms. Information was critical to managing in this business although few in the management team apart from the MD, CIO and financial controller realised this need (eg. profitability by customer information). Together they prepared the strategic IT plan for the future of the new company.

Extracts from company newsletters capture some of the excitement at this time:

The merger of XYZ with Mainframe Australia Limited has given us enormous potential to be the major force in the IT services business. With over 500 employees we are the 3rd largest in the industry behind only DEC and IBM.

XYZ, however, has a major competitive advantage. No other competitor has our A-Z capability to support mainframe, mid-range and desktop products.

25 June 1996

The appointment of Doug Hollow as our new MD is the highlight of a month of solid effort.

30 Jul 1996

Contracts conversion from OVERSEER and CFINCS is progressing well and on schedule for the 1 October billing from ASIS.

New invoice formats have been created in ASIS so that our customers will see almost the same format as before. We are also preparing a large mail out to our customers to advise them why their maintenance invoices will now be on XYZ letterhead 30 Jul 1996

Contracts extracted from CFINCS and OVERSEER have been validated and parallel invoicing runs between our systems for the last two months have been reconciled. ASIS training is almost complete and the new maintenance contract procedure is being resolved. ***We will 'go live' with contracts in ASIS on 1 October****.*

We've pointed to our disparate systems as a source of inefficiency and as a cultural barrier. With the impending systems consolidation only weeks away, we will take an irreversible step forward to become something greater than the sum of our past mergers. 25 Sep 1996

We have met our first milestone in rationalising systems! All maintenance contracts have been moved to ASIS and the first invoicing run on XYZ letterhead has been successful.

The current status of our IT systems is as follows:

- *Financial systems*
  ASIS, DEBTORS, PREMIER, MASTERPIECE, ASSETS
- *Contracts / Billing*
  ASIS, ~~SPARCS~~, ~~CFINCS~~, ~~OVERSEER~~
- *Call Management*
  ASIS, FSMS, FSMS-WW
- *Logistics*
  ASIS, SOLS, RAMS

One might summarise the status of our IT systems as: '3 down, 8 to go'.

12 Nov 1996

On Friday 25 October, the first "one page KPI reports" were sent to managers across the country. They will continue to be sent on a weekly basis.

12 Nov 1996

"we're not integrating any more" … "we've gone beyond that"

12 Jan 1997

Key Events

ASIS -> FSMS Call Conversion 20/1/97

ASIS -> SOLS Logistics Conversion 26/1/97

Data Warehouse implemented & report writer roll-out 26/1/97

Electronic distribution of KPI's Feb 97

The last newsletter dated 12 January 1997 proudly declared that "we're not integrating anymore … we've gone beyond that". The confidence within the company was reflected in both the draft IT strategic plan below (fig 3) and the planned consolidation of the strategic 'Call System' on the 20 Jan 1997.

Merger of IT Systems

The consolidation of four separate Contracts & Billing systems to one allowed the newly merged company to do two things: (1) to lower it's own cost structure and follow one standardised business process (The three decommissioned systems were all legacy systems running on a mainframe platform and they were expensive to maintain). (2) It also, more importantly, paved the way to calculate profitability by customer because it was difficult to get customer information from four disparate systems.

A second major systems integration of the call systems was crucial to the business for operational reasons. The major cost in the business were staff. The staff costs were largely driven by the business process which in turn was underpinned by the IT system. It was necessary to have one call system before the business process could be effectively fine tuned for efficiency.

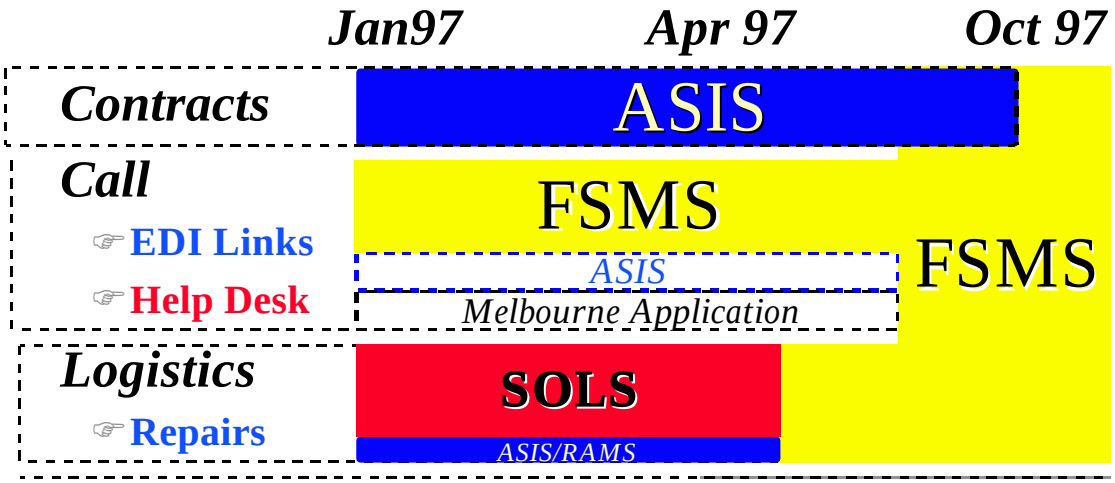


Figure 3: Draft IT strategic plan showing rationalisation of the operational systems firstly to 3 (ASIS, FSMS, SOLS) and then to 1 (FSMS).

Technical issues affecting the consolidation of the call systems

ASIS was the fully integrated services system used by XYZ prior to the merger. It had been fully developed in house using AREV, a little known programming language, but it worked and had the advantage of being able to run on a low cost IT platform. After the merger XYZ management presented a case for consolidating all systems to ASIS because of the lower cost and advantages of a fully integrated system. However, several considerations made this option unattractive:

- ASIS was largely undocumented and all the knowledge lay in the head of one talented but somewhat fickle programmer known to have occasional 'Prima Donna' fits of uncooperativeness.
- AREV, the development language, was being superseded and would no longer be supported in the near future.
- Negotiations were proceeding with a software development company to overcome both these issues. The development company could provide staff that could learn ASIS and support AREV. Despite this, the issue remained that AREV was a dying language and programmers would be difficult to source.
- AREV had its roots on a PC platform and there were doubts as to whether it would be fully scalable to handle the demands of the newly formed $100M pa company. Independent tests had shown that it would work, but the IT staff in the parent company were unconvinced. One very telling sign was that whenever the lights flickered because of power surges, the developer looked nervous and would often rush to the server to check everything was ok. He said that once the network had been upgraded, this problem would be overcome.
- FSMS an alternative system, although not fully developed, was being sponsored by the international parent company to be the services system of choice for all subsidiaries. It was based on Ingres: a well known development language and there was no question that it had the potential to handle the increased demands of the merged company.
- There were however some doubts regarding the quality of FSMS. The development group had a poor reputation and the specifications on which it was based were sometimes based on best practice from over six years ago. The was a rumour that the local parent maintained its profitability on the basis of software development revenue and that it was milking its international parent for all it could get.

- The financial case for FSMS was extremely strong. Approximately $6M had already been spent in development of FSMS. It was fully funded for future development and the international parent would pay all for enhancements. Another division of Mainframe Australia was doing the development work and the development work contributed significant revenue for the local company. Any decision not to use FSMS would have major political ramifications.

Organization Structure

XYZ was set up to have a separate market identity from its parent company. In practice, it had direct reporting links to its parent, but because of profitable results, it was making significant progress in establishing its independence.

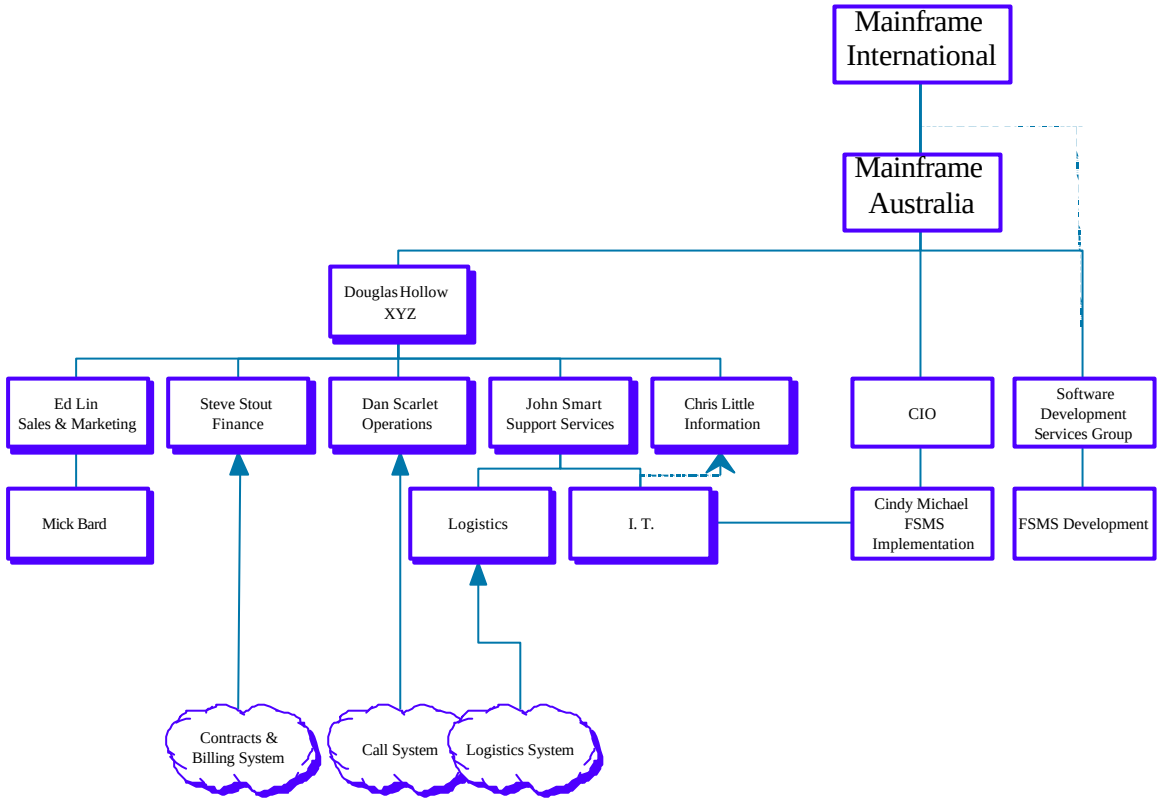


Figure 4 Organisational chart showing FSMS ownership

The original ownership of the IT Systems is shown in Table 2 below.

IT System	XYZ	MAINFRAME AUSTRALIA
Contracts & Billing	ASIS	~~SPARCS~~, ~~CFINCS~~, ~~OVERSEER~~
Call	~~ASIS~~	FSMS, FSMS –WW
Logistics	~~ASIS~~	SOLS, RAMS

Table 2 Consolidation of IT applications (strikeouts show decommissioned systems)

The organization chart shows the fragmented ownership of FSMS as well as the impending change in reporting structure in the IT function. Some implications of this are described below.

Some reasons for the difficulties

Dick Stone, one of the key staff working on the decommissioned ASIS call system commented later: "I'm not sure anyone from the FSMS team ever talked to us… we were glossed over" He added "the attitude was that FSMS had been selected, and by definition was the best thing for the company. The edict was 'thou shalt have FSMS'. They believed FSMS was generic and therefore it would work. Problems could be dealt with later. They didn't realise how inflexible the T&M procedure really was."

According to Dick, the XYZ staff felt that FSMS wouldn't work (the way XYZ was used to working) and they knew Mainframe wouldn't change FSMS. Everyone had different reasons why it might not work e.g. too slow, didn't do something, didn't know how data would get in, etc. and along with this negative atmosphere was a conservatism inconsistent with the pace of rapid change. "I am a naturally conservative person. I tend not to say 'it will work' until it's actually done and working. I had a lot of misgivings because I didn't feel that anyone had been through it thoroughly and checked this and ticked that"

Dick felt that Dan's attitude was 'we have too, we don't have a choice' and that John's attitude (after losing control of the IT function) was that he didn't care any more. He was suspicious and thought they may be looking for scapegoat. He is said to me "get a lawyer... be very careful who you talk to and what you say"

He felt that the earlier contracts systems (CFINCS, OVERSEER & SPARCS to ASIS) conversion was successful because the people worked so closely together. "With FSMS, there were always two people between (the people who knew how it worked). Even the development team didn't know what the operations team were doing." His overall feeling was that the people issues had never been adequately addressed i.e. Why should we do this?

The result

The next few months were spent rectifying the problem. As each problem was solved one by one, Chris seethed inside because they were easily identified and he asked himself "why wasn't this discussed and resolved before we cut over?" He tried apologising formally to the customers but Mick Bard in marketing refused to authorise any document acknowledging responsibility because it might open XYZ to liability claims.

By the 17th March, two months later T&M revenue was starting to be collected again but there were still a number of major tasks to be completed. The company had lost 30% of it's revenue during this period. No one had realised it would be this significant. Dan Scarlet commented "if we had realised the implications, we wouldn't have been so calvalier about it". Every IT system consolidation had been delayed 2-4 months.

All the financial targets were missed that year. None of the senior managers received their bonuses. Three years later XYZ, in an independent survey of customer service, had a 'bottom 5' rating.

Post Script

The ASIS support staff were completely frustrated with the process and stopped cooperating. The key developer decided that if he was not going to be listened to, he would increase his hourly rate from $60/hr to $200/hr and leave as soon as he got another job. The other developer opted to leave the AREV support company that XYZ contracted to overcome support difficulties. He offered to work for $120/hr and continued at this rate for the next 4 years. XYZ had no choice but to pay and it also had to pay out the software development company to prevent legal action for taking one of their staff. The news spread and some technical support staff for the legacy logistics system did the same thing.

Development stopped on the FSMS system after another six months of political negotiations. It was important that the international sponsor not be seen to be at fault and the cancelling of the project had to wait until he had another successful project to justify diverting his attention. FSMS was dropped in favour of a packaged solution. The implementation of the packaged solution was successful only after its second attempt. Cindy, the project manager of the failed call conversion managed both the failed and the successful packaged solution implementation.

The logistics system consolidation has been deferred indefinitely and the logistics function has been outsourced.

Key Performance Measures started to be produced from the data warehouse initiative 90 days after the call system difficulties were resolved.