

BROKING SYSTEMS:
A REVIEW OF THE MARKET



October 2004

Mazars' Insurance Broker Industry Survey carried out in January 2004 in conjunction with BIBA, found that the broking market, both in London and regionally, was continuing to go through a period of aggressive price competition. In addition, the market was primed for increased consolidation activity as a result of the introduction of the FSA as regulator to the general insurance industry from early 2005. New accounting requirements and technology improvements were also found to be influencing the level of expenditure on new IT systems.

In order to find out more about the impact of these requirements, Mazars carried out a review of selected brokers in the Lloyd's and regional markets focusing on the implementation of systems for FSA regulation and general IT governance. The review produced a number of significant findings that in turn could provide information to the wider insurance broker market.

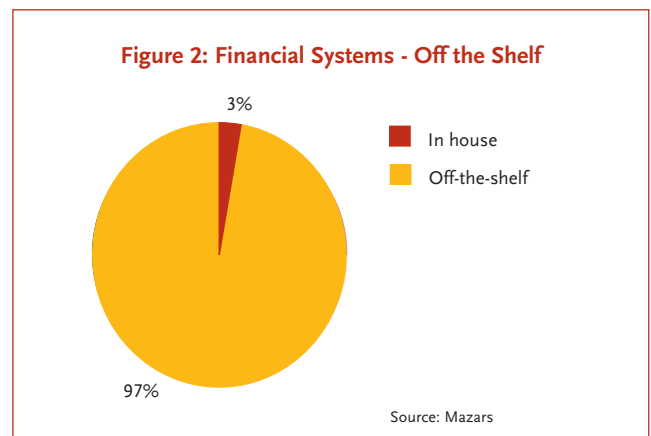
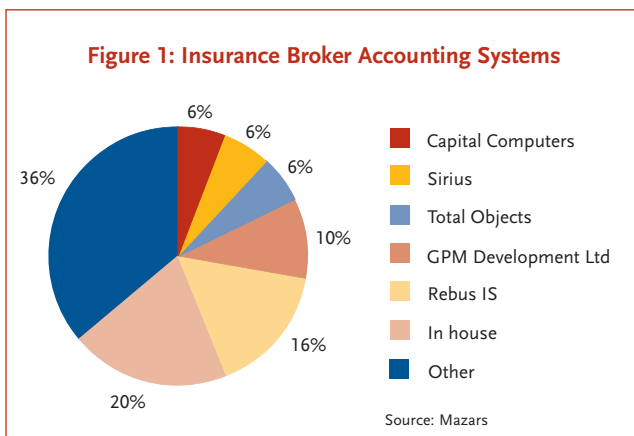
Key Findings of the Analysis

Systems Fragmentation

As a result of FSA regulation, new accounting standards (FRS5 application note G), internationalisation, new technology, the varied types of business transacted and the level of competition between organisations, there are few standards and cost-efficient ways to manage and underwrite insurance using technology as a platform. This is especially the case for broker-to-broker and reinsurance business. Direct personal lines insurance has, in many areas, been revolutionised by the internet.

Figure 1 below indicates the extent of systems fragmentation. 36% of the suppliers have a relationship with only one intermediary for the provision of insurance broker accounting (IBA) support systems.

Owing to the level of investment required and the diverse business requirements that an IBA system might support, there are very few effective integrated solutions currently on the market. Only 10% of those reviewed have an integrated solution. The accounting for brokerage, however, once calculated, is more straightforward and could be handled by a cheaper, off-the-shelf solution. 97% of organisations reviewed opted for an off-the-shelf accounting solution such as Sage, Sun or Pegasus (see figure 2).



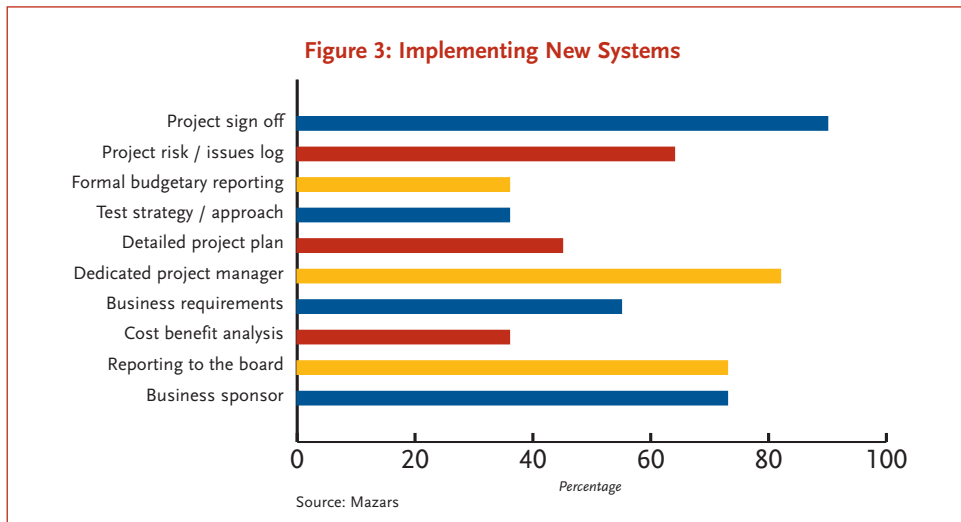
Conclusion

The above analysis raises significant issues when management considers the documentation of internal policies for business continuity, succession planning and disaster recovery, specifically where there is a high level of customisation and dependency on external vendors and a small number of internal staff. Management need to ensure that appropriate measures are taken to insure against vendor insolvency, ensure key man insurance is purchased and ensure strong documentation is in place to monitor the development and maintenance of systems. Where organisations are acquiring businesses, serious consideration needs to be given to carrying out the right level of due diligence on systems that are not off-the-shelf, as systems processes and controls need to be fully understood. Data and systems integration can be very costly if there are compatibility issues to overcome.

New Systems Management and Control

Of the organisations reviewed, 37% were implementing a significant upgrade, had introduced one recently or were in the process of planning a change. The normal life cycle for key systems is between 3 and 5 years. Change tends to be driven by improvements in the use of technology, where the existing systems fail to meet changes in business needs or where staff leave and are replaced by people who wish to replace the current systems.

With this continual change in systems, especially if they are customised, increased control is required. This should be on several levels - financial control in the form of the right cost-benefit analysis and maintenance of the spend on a project; operational control based on having the right skills and experience to specify requirements; and management control by ensuring that final acceptance by the business is in place. It is surprising, then, that only 55% of the reviewed brokers have formally documented and detailed business requirements for choosing system vendors and developing a detailed project plan (see figure 3). This would explain, in part, why only 45% have a project plan to manage the implementation process. Furthermore, only 36% conducted a cost benefit analysis prior to the change. This means that management may be making decisions based on instinct rather than looking directly at how the system changes could be used to generate competitive advantage and cost savings. Several of the organisations reviewed have been working directly with new vendors in the market, spending significant amounts of money and management time and changing their requirements constantly. Such an approach appears to benefit the vendor only, and management time may be diverted away from the broker's business.



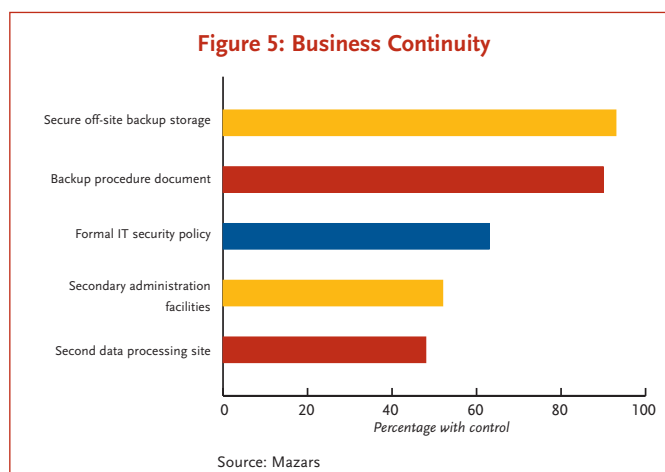
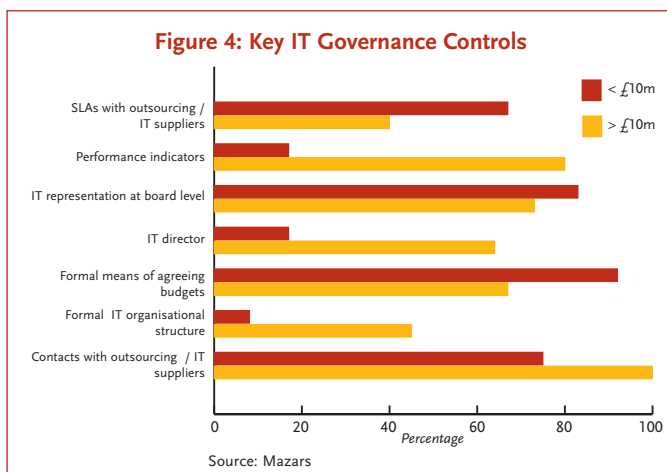
Conclusion

The above raises significant issues when management considers the need for new systems, the cost of implementation and the acceptance of the new system into the business. This area is becoming more important as new regulation, internationalisation (currencies), and accounting rules (FRS5 – Recognition of income) are forcing organisations to review whether their existing systems can continue to deliver. Insurance intermediaries are increasingly working in an IT-based environment where the demands of customers (including the markets), the need for profit protection and new competition are forcing companies to rethink their strategies. There are a few key activities that will improve the change process:

- clearly define and document what the business does now and is expected to be doing in the future;
- carry out a cost-benefit analysis, focusing on how a new system would complement the business, either by reducing cost or by assisting in the acquisition of new business;
- free up dedicated, skilled resource or buy in key people to implement the system efficiently, installing a communication process that will pro-actively get things done and not become a burden;
- ensure that there is a well-controlled procedure for testing and retesting the software before acceptance, final sign-off and payment of supplier invoices; and
- implement a governance structure to manage the contractual relationship and continuing development of the system.

IT Governance and Systems Security

Structuring and monitoring a practical approach for measuring the risk of IT is becoming increasingly important. The analysis below illustrates the comparison between intermediaries with greater or less than £10m brokerage (1) (see figure 4). What is interesting is that as many as one quarter of smaller companies do not have a formal contract of service with their main IT suppliers. This absence of management control must lead to increased risk of loss (financial and operational) in implementing a disaster recovery process. The analysis also shows that many larger intermediaries are employing good management practice when monitoring on-going systems performance (80%). However, less than half are obtaining Service Level Agreements with key IT providers / outsourcers (40%) and a significant number are neither implementing formal budgetary control (33%) nor have board-level IT representation (27%) – two important controls which, if ignored, increase business risk.



(1) This split has been observed as a point when companies systems and internal IT resources begin to become more complex in nature and security becomes an increased priority.

Conclusion

It is important to install security checks in the systems operated for insurance business, not only because it is good management practice but also to ensure that external regulatory demands are satisfied. It is surprising that only 63% of companies reviewed had a formal security policy (see figure 5) and of these only 15% are following a recognised industry standard for information control covered by BS7799 and ISO 17799. These are standards that have been developed in conjunction with the government to assist management to implement strong frameworks for monitoring and controlling information. This method of protecting company data is vital for compliance with FSA requirements and should be high on management's agenda. Failure to do so may lead to a competitive disadvantage, loss of business and/or the risk that employees may not act in the best interests of the business. As part of any strong IT governance and security process, the management need to consider the following steps, which will help ensure that IT management becomes an integral part of the overall risk and strategic management approach:

- understand, document and agree the critical business processes and associated risks, including systems;
- understand what technology is being used now and its purpose, including how it assists in the effective control and mitigation of critical business risks;
- decide upon a suitable management structure to support the IT function, ensuring that the right security, people and reporting framework are installed;
- involve IT resources in the strategic development of the company at an early stage; and
- develop an appropriate project management approach that will ensure that initial benefits determined for the introduction of a new system are realised and that management are not distracted from the business.

For more information, please contact Alistair Bennett on
Tel: 020 7220 3443 or alistair.bennett@mazars.co.uk