Impact Leadership through Sharing

Checklist and explanatory notes

Information as an Asset

The Board Agenda

The Hawley Committee

A consultative document for chairmen, chief executives and boards of directors developed on behalf of the KPMG IMPACT programme by a committee under the chairmanship of Dr Robert Hawley, chief executive of Nuclear Electric plc.

Information as an Asset

Contents

Foreword..3

1 Introduction 4

2 The Board Agenda..5

3 Checklist and Explanatory Notes...6

Appendices...14

For further copies of the Checklist and explanatory notes of the Consultative report or to give views and feedback, please contact:

Dr Nigel Horne or Colin Palmer, KPMG IMPACT, 8 Salisbury Square, London, EC4Y 8BB

Tel: 0171 311 1000 Fax: 0171 311 8697

Foreword

A number of my business colleagues and acquaintances from a range of organisations have, for some time, been expressing concerns about the information they hold in their organisations. In particular, we have often discussed these questions:

- *Do we have information that is a strategic asset to our organisation?* The answer seemed to be: yes, we have quite a lot of such assets.

- *Are we content that we understand these assets in the same way we understand our other strategic assets and are we harnessing them and protecting them as we should?* The answer seemed to be: no, we are not.

Regular newspaper headlines and war stories - major disasters, losses, fraudulent action and competitive advantage stolen - stirred us into action.

A group of us came together under the auspices of the KPMG IMPACT programme to see if we could put together a succinct set of guidelines for boards of directors in 'Information as an Asset'.

I hope we have succeeded. We carried out interviews with a wide range of chairmen, chief executives and executive and non-executive directors in the public and private sectors. We analysed published literature where we could find it, and we spend significant time putting together our views.

The Board Agenda, which follows the introduction explaining the rationale for our work, is on one side and is intended as a brief for chairmen of the board to consider and test the health of policy and practices in their organisation.

The 'Checklist and explanatory notes' that follow are for those who wish to consider the subject more fully and who need to respond to the questions the board will raise.

There is also a separate publication, the Consultative report, which sets out our work programme and the results of our research. It provides some practical approaches to classifying, harnessing and protecting information assets.

We are now circulating the Board Agenda and the Checklist and explanatory notes widely to chairmen and chief executives of public and private sector organisations and to interested institutions. We are encouraging comments and testing of our ideas: we want people to try the Board Agenda and Checklist in their organisations and to feedback their views and experiences. We do not pretend to have all the answers and we want to consult and improve on what we've done so far. In 12 month's time we will review what has been learned. Please help us and yourself by taking part.

I am note grateful for the members of the committee for the quality of their thinking and for the support from the KPMG IMPACT team. They made the hob of chairman a real pleasure. If you would like to know more, write to me at the KPMG IMPACT office (the address is on page 1) or speak to Nigel Horne or Colin Palmer on the phone number listed. I wish you well with enhancing the value of your information assets.

Dr Robert Hawley

1 Introduction

The board of directors of any organisation is responsible for the conduct of that organisation in every way - financially, operationally, legally and ethically. Specifically, it has responsibility for its assets and their use.

Boards fulfil their responsibilities by ensuring that their requirements for the conduct of the business are clearly specified to management and by ensuring management comply with their wishes.

Many responsibilities of a board of directors concern the activities and processes of the organisation - e.g. investment for a new product, selling in a new market, building a new plant. But some of the most important responsibilities are defined functionally by subject - e.g. financial affairs, human resources. One such subject is information - not information systems but the information itself.

Organisations operate by producing, transmitting and digesting information. The right information at the right place at the right time is essential for effective conduct of business. Equally, the misuse, copying, theft, loss and abuse of information can be the cause of scandals and business failures.

Information is required in every activity and every function and the proper control of information and care in its use have always been subjects of concern. In particular, too much information is often as bad as too little and information is often best disseminated and used on a 'necessary and sufficient for purpose' basis at each organisational level.

Modern computers and communications can store information, process it and make it accessible in ways never before achieved. This can be of great additional benefit to business but it can also enhance opportunities for misuse, theft, loss and abuse and in particular, indiscriminate dissemination of information.

In some organisation it is accepted that some types of information are assets - for example, intellectual property such as patents and copyright.

The Hawley Committee proposes that all significant information in an organisation, regardless of its purpose, should be properly identified, even if not in an accounting sense, for consideration as an asset of the business. The board of directors should address its responsibilities for information assets in the same way as other assets - e.g. property, plant. This implies a new approach to how information should be treated and requires a board to make clear to management what actions it wishes to be taken and who is responsible for action and compliance.

Most boards have extensive experience in the subjects and functions they address. Relatively few boards have experience in the acquisition, processing, storage and transmitting of information and fewer still in the responsibilities which arise when information is considered as an asset.

The Hawley Committee has set out to stimulate board to address their responsibilities in treating information as an asset by providing and agenda and supporting documents which can be used for periodic discussion by the board and for reports of compliance by management.

2 The Board Agenda

The Hawley Committee proposes that all significant information in an organisation, regardless of its purpose, should be properly identified, even if not in an accounting sense, for consideration as an asset of the business.

The board of directors should address its responsibilities for information assets in the same way as for other assets - e.g., property, plant.

This implies a new approach to how information should be treated and requires a board to make clear to management what actions it wishes to be taken and who is responsible for action and compliance.

The board should satisfy itself that its own business is conducted so that:

1. The information it uses is necessary and sufficient for its purpose.
2. It is aware of and properly advised on the information aspects of all the subjects on its agenda.
3. Its use of information, collectively and individually, complies with applicable laws, regulations and recognised ethical standards.
4. The board should determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed, including:
5. The identification of information assets and the classification into those of value and importance that merit special attention and those that do not.
6. The quality and quantity of information for effective operation, ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent.
7. The proper use of information in accordance with applicable legal, regulatory, operational and ethical standards, and the roles and responsibilities for the creation, safekeeping, access, change and destruction of information.
8. The capability, suitability and training of people to safeguard and enhance information assets.
9. The protection of information from theft, loss, unauthorised access, abuse and misuse, including information which is the property of others.
10. The harnessing of information assets and their proper use for the maximum benefit of the organisation including legally protecting, licensing, re-using, combining, re-presenting, publishing and destroying.
11. The strategy for information systems, including those using computers and electronic communications, and the implementation of that strategy with particular reference to the costs, benefits and risks arising.

3 Checklist and Explanatory Notes

The Hawley Committee proposes that all significant information in an organisation, regardless of its purpose, should be properly identified, even if not in an accounting sense, for consideration as an asset of the business.

The board of directors should address its responsibility for information assets in the same was as for other assets - e.g., property, plant.

This implies a new approach to actions it wishes to be taken and who is responsible for action and compliance.

The board should satisfy itself that its own business is conducted so that:

1. The information it uses is necessary and sufficient for its purpose

Callout: Review board information

The board should review what information it needs, remembering that this is likely to change over time, both to ensure that it remains adequate for its purpose and to remove unnecessary information.

2 It is aware of and properly advised on the information aspects of all the subjects on its agenda.

Callout: Get advice for the board

In most subjects - e.g., marketing, finance and personnel - it is accepted that appropriate expertise and experience is required at the board table and it is probable that suitably qualified people wi11 be present.

Experience of the consequences of treating information as an asset and expertise in information systems is not yet common and, for example, reliability and risk issues can easily be overlooked. Proper advice for the board, possibly independent of that used by the organisation, should be sought until such time as such experience is more widespread.

3 Its own use of information, collectively and individually, complies with applicable laws, regulations and recognised ethical standards

Callout: Comply with regulations

Regulations, including legislation, covering information and its use are becoming more common as concern grows for information misuse and for rights to privacy and confidentiality. The number of rules and regulations with which a board needs to comply is considerable, ranging from Stock Exchange rules, through financial services regulations to the Data Protection Act.

The board also needs to review the implications of the EU 1aws covering the use of information such as the proposed Directive on data protection and privacy.

Similarly, the increasing emphasis on demonstrably ethical behaviour needs to be taken into account. The law is incomplete and sometimes idiosyncratic regarding information - e.g., having different conditions dependent on the medium used to store it - so the matter is not straightforward. Board members should be briefed on the rules and regulations and updated from time to time.

The board should determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed, including:

Callout: Set content of policy

The organisation's policy will include how and when the board wishes to discuss its information assets, who will be responsible for reporting to the board and in what form, as well as specific points on the subjects below, probably including how the organisation compares with similar organisations elsewhere. Where applicable, the policy will also include which powers on information assets are delegated and which are reserved to corporate 1eve1. The appropriate method for ensuring compliance will include the internal audit function where it exists but is also likely to include line management and the use of specialists in the business, in information and in information systems.

4 The identification of information assets and the classification into those of value and importance that merit special attention and those that do not

Callout: Classify importance and value

The organisation should analyse information and classify it according to importance and value to the organisation, to its customers, to collaborators and suppliers, to individuals and to the national interest. Where information is intended for limited circulation or to be used only for a particular purpose, there must be an appropriate identification, procedures for use, and rules for safekeeping.

This is the basic first step in information management and control. It is as much about deciding what information is not important and, even, can be eliminated, as it is about identifying information which needs special treatment. In most cases the number of categories of information will be low, probably three or 1ess. There are a number of possible methodologies available to classify information, some of which are referenced in the Hawley Committee report.

The organisation should review (probably as part of a regular review of plans and budgets) how changes - for example, in business strategy, regulation, economic factors, technology, business practices, publicly available information and people may affect its assessment of its information assets.

The value of information is not static in a changing world. Changes might present opportunities for the organisation to be more effective or represent a threat because they might enable other organisations to perform its business more effectively.

This review should be part of an overall review of strategy and direction because the subject of information cannot be covered fully on its own. The objective is to make sure that the availability and use of information in different ways is fully considered, possibly including the use of modelling techniques The sort of opportunity being sought could be, for example, in telephone banking, booking systems in airline operations, direct ordering by customers, or home shopping. Such opportunities can, in turn, change the value of information in an organisation.

5 The quality and quantity of information for effective operation, ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent.

Callout: Review quality and quantity

The organisation should review the information required at each stage of each process in its business to ensure that necessary and sufficient information is available as required for effective operation - and no more. This must include summary information for decision support at the various levels of the organisation.

Modern computer systems have the virtue of making information more available, but this can be a vice if they provide too much information which can slow down processes, add cost and increase the possibility of accidental or deliberate misuse.

Callout: Review timeliness

The organisation should review the timeliness of information at each stage of each process to ensure that it can be used most effectively. Information frequently loses its value over time, sometimes over very short periods. Making information available more quickly can have dramatic effects on an organisation's performance. Equally, updating information unnecessarily can be wasteful and costly.

Callout: Managing change consistently

The organisation should ensure that accuracy and consistency of information is maintained. There should be proper procedures for managing changes, with the same care used in including and communicating the consequences of change as is used in the creation of information.

This is about accuracy and consistency when changes are made. Even in the engineering industry where the full effects of each change have to be included for products and systems to work, configuration control systems are frequently inadequate. This can result in products having the same identification even when they are different or vice versa. The same principle applies in other organisations and can be very dangerous in business, but is most frequently seen to be inadequate in simple things like mailing lists which are not updated even when everyone knows of a change, or inadequate differentiation of versions of a document as it goes through progressive redrafting. This can produce bad management decisions through the use of bad information.

6 The proper use of information in accordance with applicable legal, regulatory, operational and ethical standards, and the roles and responsibilities for the creation, safekeeping, access, change and destruction of information.

Callout: Comply with regulations

The organisation should review the legal and regulatory position which applies as it is constantly updated by international, national, industry and other bodies, and take full account of the board's policy on information assets, including those relating to ethical standards. This is likely to result in a list of applicable rules and regulations with clear knowledge of who is responsible for keeping the list and who is responsible for ensuring compliance with each item on the list. A further outcome is likely to be a number of straightforward procedures and rules - for example, on safekeeping and copying - which should apply to the various categories of information identified in strategic review. Such rules not only raise the awareness of the workforce but also simplify training and measurement of compliance.

Callout: Define information roles

The organisation should define roles and responsibilities with regard to information. There should be a clear distinction drawn between the owner of information (who is responsible for its creation and accuracy); the custodian of information (who is responsible for its physical safekeeping); those with right of access (who can view but not change information); those with the right to copy (who can reproduce information for other purposes); and those with the right to destroy (who can eliminate all trace of the existence of information).

It is self-evident that two people changing different copies of the same information independently will destroy its value because it will never be clear which is right. Yet it is surprising how many organisations allow this to happen. This can be avoided by clear identification of the owner's rights and safeguards. The librarian or the information systems manager may own physical assets which hold information but, generally, they do not own the information itself nor have rights to it. The management and controls must ensure safekeeping.

Copying implies use rather than simply access and may need to be controlled. Similarly the fact that information has ever existed is of value in itself and the decision to eliminate all trace is an important one for audit and other purposes.

Callout: Check the rights of others

The rights of third parties can restrict the value of information to an organisation. This is not just concerned with ownership by others, rights to use or have used, and so on, but also includes the case where information refers to third parties and/or to their affairs. In this case, data protection laws, privacy laws and laws related to confidential information have to be taken into account.

7 The capability, reliability and training of people to safeguard and enhance information assets.

Callout: Get proper advice

Recognising the relative immaturity of the concept of information as an asset and of information systems, the organisation should ensure that properly selected and qualified people are available to provide advice, to carry out its business and to report regularly regarding information assets Frequently such subjects are regarded as "technical" and ignored. Yet information is the lifeblood of organisations and the policies and procedures laid down by the board must be implemented.

Callout: Check reliability of people

The organisation should implement reasonable personnel procedures to avoid the use of people, as employees or third parties, who might exploit knowledge or information to their own, or other people's, advantage or be vulnerable to persuasion to do so by threat or abuse.

There have been many cases where sensitive information has been obtained by personal threats or blackmail. In many cases, organisations are rigorous in screening their own staff but less rigorous with other people's - as in at least one case where contract staff were used extensively during a large system development.

Callout: Avoid conflicts of interest

The organisation should manage its affairs such that the knowledge or information available to departments and individuals does not create conflicts of interest in their responsibilities, tasks or relationships.

This is to avoid both temptation and the accidental disclosure of information. For example, "Chinese walls" must be supported by physical separation of people where necessary in their normal places of work.

8 The protection of information from theft, loss, unauthorised access, abuse and misuse, including information which is the property of others.

Callout: control access

The organisation should make all reasonable steps to ensure that its information is protected from unauthorised access.

This includes people's own knowledge and information and access to documents as well as access to computers. Clearly the end result must be a compromise. Information which is guarded to the extremes of security is unlikely to be available in a timely manner to those who need it and people's heads cannot, in the last resort, be made the property of the organisation.

The organisation should take all reasonable steps to protect important information from physical destruction due to disaster and terrorism, including selecting appropriate sites for storage and access.

Frequently some obvious steps are taken, such as duplicate computers, remote duplicate storage etc. Bet equally frequently important characteristics of physical centres are ignored such as a network control centre for a financial institution being next to a busy street, vulnerable to terrorism. Often very simple things, such as ensuring a remote copy of the names and addresses of employees, are forgotten.

Callout: Test recovery procedures

The organisation should ensure that appropriate duplication and recovery procedures are established and regularly tested for information which is important to the organisation on order to protect itself from the loss of information and its consequences.

Terrorist bombs and other disasters have provided an important lesson that recovery procedures must be tested. It is not just about knowing what to do but also about knowing when to let other people, trained and practised, do it. In at least one recent case, directors of firms gave conflicting instructions which delayed or even jeopardised recovery.

Callout: Be tidy

The organisation should implement procedures for good housekeeping in the storage, transport and use of information which will minimise the possibility of loss, inaccuracy and misuse.

This concerns simple things like a 'clear desk' policy so that unwanted eyes do not see, or labelling of floppy disks so that it is obvious if there are unauthorised disks which may have viruses or be used to copy information. A recent example concerned a search consultant whose complete contact lists for clients and potential recruits were copied and removed. They were his business.

Callout: Use for intended purpose

The organisation should implement appropriate procedures to ensure that information, particularly that owned and originated by third parties, or which can affect the national interest, is used for its intended purpose and for no other purpose. There must be an appropriate authorisation procedure for information to be copied or used other than for its intended purpose.

This is to avoid the possibility of such situations as insider trading, abuse of personal information, address lists and so on. A recent case arose in the financial services sector, where information on the rating of credit worthiness of customers became public knowledge.

Callout: Check ownership

The organisation should implement procedures for checking the ownership of information to ensure that the use of intellectual property owned by third parties complies with the law and with their and other relevant interests.

There have been many cases of the misuse of information owned by third parties, some of which have resulted in large fines, some of which have caused great operational difficulties or cost.

9 The harnessing of information assets and their proper use for the maximum benefit of the organisation, including legally protecting, licensing, re-using, combining, re-presenting, publishing and destroying.

Callout: Stimulate innovation

The organisation should encourage innovative ideas in the derivation and use of information both belonging to the organisation and from outside sources.

Practically all organisations today depend on having and using better information in a timely manner. Ways of giving an organisation advantage is not obvious and the use of special events or outside advice as a catalyst can be useful. Use of different information can make defects in performance and new opportunities obvious when previously they were hidden. The organisation should build information models to test that it is making best use of information and compare itself, using benchmark techniques and other means, with other organisations.

Callout: Review form and function

The organisation should review how additional information, a change in the medium used to store information, combining information, sequencing it in different ways, additional manipulation, different or alternative use, summarising and re-presentation of information, restricting circulation and destruction of information, can increase the effectiveness of its organisation.

Simple examples here include holding customer information in the financial sector by name instead of account number (so that a full range of financial services used can be seen), use of membership lists to sell services, use of retail history from tills for order forecasting and targeted marketing campaigns. The results of such a review frequently involve new requirements for computer based information systems.

Callout: Protect property rights

The organisation should use the 1aw, including copyright, patents, confidentiality, employment terms and data protection, to protect its information from copying, use and abuse by third parties. It should undertake regular reviews of the legal protection of its intellectual property so that proper judgments are made on initiating, continuing, extending or cancelling protection.

Many organisations simply do not realise the value of the information they have. This is not just a matter of being able to license or sell intellectual property directly. Frequently recognising and protecting information can raise valuable opportunities in business negotiations generally. Yet patents, protection of copyright etc. can be expensive. Judgements are frequently made at a level where the full implication of actions cannot be understood. Decisions on how to use inventions, designs, brands, mailing lists, and so on to best advantage are strategic and should be reported to the board at least annually.

Callout: Review use by third parties

The organisation should review exploitation of its Intellectual Property by third parties in order to ensure that maximum benefit is being obtained.

Frequently more benefit can be obtained for stakeholders by licensing intellectual property than by exploiting it directly. A well-known example is in consumer electronics, where an invention to reduce "hiss" by using noise reduction technology for audio equipment is licensed for a tiny royalty on each piece of equipment.

Callout: Review value of information standards

The organisation should review how sharing its information assets in order to create standards could benefit its organisation.

The best examples are the use of bar coding and electronic trading in retail and the sharing of "open systems" information in the computer business.

10 The strategy for information systems, including those using computers and electronic communications, and the implementation of that strategy with particular reference to the costs, benefits and risks arising.

Callout: Base information strategy on business strategy

The organisation should ensure that its use of information systems, including those which are computer based, is consistent with its business strategy and that its investment in such systems is commensurate with the benefits anticipated and possible risks.

This is a necessary output of business planning in the organisation as a whole, treating information systems pari passu with other potential investments. However, treating information as an asset represents a different and potentially beneficial starting point in a review of information systems.

Callout: Take account of change

The organisation should review its use of information technology and other systems to take account of constantly changing market and technical conditions.

Advances in technology and change in market conditions provide new opportunities as well as threats. The speed of change means that an organisation's strategy for the use of computers and communications must be updated regularly, probably at least every two years, for this reason if for no other.

Callout: Take account of risks

The organisation should ensure that the risks involved in implementing information systems are commensurate with the expected benefits.

Information systems, particularly those involving information technology, are frequently very costly to implement and subject to delay and, even, total failure. The risks can be reduced by clarity of thought in defining precisely what is to be done, in testing assumptions and in focusing on the benefits which are expected.

Callout: Realise benefits

The organisation should ensure that the benefits which should be achieved from its use of information, computers and communications systems are being realised and that its information assets are being harnessed and protected.

The realisation of benefits from information systems is as much about the competencies of the users of the systems as it is about the providers of the systems. Measurement and diagnostic tools should be used to measure competencies throughout the organisation.

Callout: Use benchmarks

The organisation should compare its use of information systems with other organisations, both in similar circumstances and other-wise, nationally and internationally, and justify both differences and similarities in approach, benefits and costs.

There is now a range of benchmark and diagnostic tools, in addition to the use of bespoke consultancy, to measure most aspects of the use of information systems. The importance of the exercise is not the fact that differences and similarities exist, it lies in justifying to the organisation and to the board what, if anything, should be done. No organisation can afford to be complacent about its performance.

Callout: Review capabilities and sourcing

The organisation should review costs, effectiveness and skills required in acquiring, storing, accessing and use of its information, including its use of information technology, and consider whether there are more effective ways of performing those functions.

Aspects of information systems can often be better done by other people, so as to concentrate an organisation on what it is really good at doing.

Information as an Asset

Appendices

1 Members of the Hawley Committee.....14

2 Participants in the IMPACT research.....14

3 Background to the IMPACT programme....16

Appendix 1 - Membership of the Hawley Committee

Norman Barber, Chairman, Aerospace and Defence Group, Smiths Industries plc

Andrew Campbell, Director, Ashridge Strategic Management Centre

Dick Evans, General Manager (IS), Pearl Assurance plc

Mick Firth, Executive Director, The Co-operative Bank plc

Chris French, Director of CICS, NM Rothschild and Sons Ltd

Bob Hawley, Chief Executive, Nuclear Electric plc

Nigel Horne, IMPACT

Philip Langsdale, IT Director, ASDA Stores Ltd

John Leightfield, President, British Computer Society

Steve Matheson, Deputy Chairman, Inland Revenue

Colin Palmer, IMPACT

Bill Robins, Ministry of Defence

Michael Steen, Partner, KPMG

Michael Tuke, Group Services Director, Woolwich Building Society

Mike Winch, Group IT Director, Safeway Stores plc

Appendix 2 - Participants in the IMPACT research

Professor John Ashworth, Director, London School of Economics and Political Science

Caroline Banszky, Director, NM Rothschild and Sons Ltd

Ted Burden, Chief Executive, ISSC

Sir Adrian Cadbury

Sir Bryan Carsberg, Director General, Office of Fair Trading

Margaret Clayton, Assistant Under Secretary of State (Personnel, Organisation Management), Home Office

Don Dewin, Operations Director, BAe Dynamics

Syd Gillibrand, Vice-Chairman, British Aerospace

Kenneth Harvey, Chairman and Chief Executive, NORWEB

Richard Henchley, Company Secretary, Blue Circle Industries

Colin Hope, Chairman and Chief Executive, T&N

Keith Humphreys, Chairman and Chief Executive, Rhone-Poulenc UK

David Jackson, Company Secretary, Powergen

Bill Jeffreys, Assistant Under Secretary of State (Immigration and Nationality Dept), Home Office

Michael Jenkins, Chairman, London Commodities Exchange

Ken Jordan, Director, Department of Unemployment

Gordon Mackie, Director and General Manager, British Aerospace Regional Aircraft

Neville Moss, Company Secretary, Eastern Electricity

Sir Geoffrey Mulcahy, Executive Chairman, Kingfisher

David Mutton, Corporate Services Director, SW Electricity

Sid Norris, Assistant Under Secretary of State, Home Office

David O'Brien, Chief Executive, National and Provincial Building Society

Rod Olsen, Director of Finance, Cable and Wireless

Dick Paine, Director of Corporate Development, SW Electricity

Terry Platts, Principal Establishment Officer, Home Office

Sir Michael Richardson, Chairman, Smith New Court

Alan Rudge, Managing Director, BT Development & Procurement

Bob Scott, Deputy Chief Executive, General Accident

Colin Short, Group Finance Director, ICI

Colin Smith, Chief Executive, Safeway

Ian Smith, Director of Strategic Planning, NHS

Nick Stuart, Deputy Secretary, Department of Employment

Mike Townsend, Finance Director, Rolls-Royce

Tim Walker, Group Finance Director, Vaux Group

Reginald Watts, Deputy Chairman, Citigate Corporate

John Weston, Chairman and Managing Director, British Aerospace Defence

Peter Williams, Chairman, Amdahl Europe

Ray Wilson, Operations Director, British Aerospace Airbus

Appendix 3 - Background to the IMPACT programme

What is IMPACT?

The KPMG IMPACT club has a membership of 30 major organisations. Its purpose is the sharing of practical experience and knowledge about information management. It is not another multi-client research programme simply publishing reports, nor is it dedicated consultancy. It is designed to deliver some of the benefits of both, requiring time and effort from the senior staff of its members. It is aimed at enabling organisations to harness information and information systems for successful radical change.

How does IMPACT work?

IMPACT activities are driven by the needs of its members; IMPACT works on the simple approach of Define-Measure-Diagnose-Correct-Measure. Tools and techniques have been developed over the five year life of IMPACT to measure different aspects of the subject. The measurements are often based on original research, whose conclusions are pilot tested in member organisations; diagnostics are built with a view to providing practical guidance on how a situation can be improved. There is now a library of proven techniques and of case data to assist IMPACT club members.

IMPACT has developed a distinctive character to its work. Overall direction of the club is under the guidance of an Advisory Board of senior business people. IMPACT is staffed by experienced business and IS professionals who have spent their working lives doing rather than advising. IMPACT draws on the world's best ideas with its Distinguished Seminar programme. It has close links with a number of business schools assisting in the research. It draws its best practices from a1l over the world. The club allows members to compare and contrast their own situation with those of others and provides stimulating ideas and understanding of what is happening worldwide. IMPACT has a wealth of experience which it puts at the disposal of its members.

Current areas of work include:

- Measurement of change
- Information assets
- Strategic partnerships
- Measuring IS effectiveness

IMPACT Leadership through Sharing

Information as an Asset

Do we have information that is a strategic asset to our organisation?

Are we content that we understand these assets in the same way we understand our other strategic assets, and are we harnessing them and protecting them as we should?

Against a background of newspaper headlines of major disasters and frauds, a group of business people came together under the auspices of the KPMG IMPACT programme to consider these questions.

The Hawley Committee, as the group became known, has published its findings as a Consultative report. This Checklist and explanatory notes summarises the research and aims to encourage comment on the committee's conclusions.