IBM Corporation
1133 Westchester Avenue
White Plains, New York 10604
U.S.A.

31 May 2001

Mr William McDonough
Chairman, The Committee on Banking Supervision
The Bank for International Settlements
Centralbahnplatz 2
Basel 4002
Switzerland

Dear Mr McDonough

I am writing to share IBM's perspective on the proposed Basel Capital Accord published by the Committee on Banking Supervision. Our comments are directed to the Consultative Document on Operational Risk, as this is the subject on which our company has the greatest knowledge.

As you may know, IBM has designed, implemented and run the operational infrastructure of a number of financial institutions and markets. As much of what the BIS includes in its definition of Operational Risk is underpinned by technology, our comments may be of interest.

In developing our response, our objective has been to share our observations on technology-centric Operational Risk in financial institutions and markets. We have also set out to share our insight on how this risk might evolve in the future as these institutions innovate, e.g. as they continue to invest in e-business.

In our response, we have identified the challenges we see to implementing the BIS vision for Operational Risk, and have made suggestions on how these challenges might be addressed. Finally, we have identified a number of critical success factors that need to be in place to implement the BIS proposals.

IBM would like to thank the Committee for giving us the opportunity to respond. If you have an interest, we would be pleased to discuss these matters.

Kathleen A O'Neil
General Manager
Global Markets Infrastructure
Financial Services Sector
IBM Corporation

IBM Response to the Bank for International Settlements Consultative Document on Operational Risk

Executive summary

IBM would like to offer comments to the Basel Committee on Banking Supervision on its consultative document on Operational Risk. Much of what the BIS includes in its definition of Operational Risk is underpinned by technology. IBM has experience in designing, building, running, measuring and managing the risk in the operational infrastructures of a significant number of financial institutions and markets. We believe that the Committee might find our perspective of interest.

The Committee's vision of a progression from the standardized approach to the internal measurement and loss distribution approaches appears likely to create powerful management levers. These milestones should motivate the industry to develop a strong discipline for Operational Risk management.

At the same time, the implementation of the BIS vision will involve some significant challenges. For example, when the industry was developing the disciplines of market and credit risk management, a change in operational technology was often included in the risk mitigation approach. This dependency is likely to be even stronger with Operational Risk.

Similarly, the work required on settlement risk was found to be much greater than was first estimated. This was because so many settlement failures were found, on investigation, to be caused by operational and technology limitations. This work showed that it is key that institutions ensure that Operational Risk is sufficiently decomposed into its elements, and that the root causes of losses are identified with enough precision so that effective risk management can be undertaken.

IBM's objectives in responding to the consultative document are threefold. We will share our observations on technology-centric Operational Risk in financial institutions and markets and on how this risk will evolve as these entities innovate, e.g., as they move to e-business. We will also highlight challenges that the industry and its supervisors will face in implementing the BIS vision, and we will suggest approaches to address these challenges.

Challenges

There are a number of challenges to implementing the BIS vision, but the most fundamental is data. The data needs to be sourced, managed, scoped and interpreted. We will consider these in turn.

The first set of challenges concerns the sourcing of data. Many of the institutions' operational processes have been implemented based on an extensive technology infrastructure, and the implications of this need to be clearly understood. For example, network resilience, outsourcing and information security are just three areas where the technology is complex and the Operational Risk is critical. Much data exists on the technology, but it needs to be collected and interpreted in its business context. This will be fundamental to measuring the Operational Risk.

The second set of challenges lies in managing the data. The discipline of information technology strongly advocates the building of a data model, designed to ensure the data meets the institution's needs for consistency, confidentiality and speed of access. A well-designed data model helps the institution clearly understand and interpret the data. For example, it can help differentiate between cause and effect, assess the future using data about the past, and define the approach when evidence is scarce, such as in low frequency, high severity losses. Some companies have invested millions in developing databases, but have later had to discard them due to faulty design. As institutions increasingly transact over networks, these data models will be essential to structure the data required to manage both the operational risks and rewards of e-business.

The third set of challenges concerns the scope of data required. Data will be needed to estimate the impact and probability of the risks. It will also be needed to calibrate these measurements with those of other institutions that have comparable experience, for example on technology infrastructure. However, the calibration needs to recognize that institutions differ, for example, in their size, structure, geographic location and regulatory regime. A very effective way of addressing these challenges is to develop well-positioned scenario analyses of the risk exposure. These analyses comprehensively scope and define the categories of calibration data required.

Lastly, there are challenges to interpreting the data. Managing risk is complex and has complex inter-dependencies. As market and credit risk have shown, these challenges are effectively addressed with a statistical risk model that translates the complexity into a clear representation that enables management to focus on and prioritize remedial action. But although market and credit risk models are sufficiently generic to be replicated throughout the industry, institutions' operational processes and infrastructures are so diverse, that it is a major challenge to develop a generic Operational Risk model. However, for some areas of Operational Risk, where technology is central, it can be possible to develop generic risk models. One example is information security. This can significantly increase the cost effectiveness of managing such Operational Risk.

Having considered these four sets of challenges, we have netted them out as 13 specific challenges. Our response document discusses each one, and then suggests an approach to address it. From our analysis of these approaches, we have distilled four critical success factors, as explained in the Appendix, and detailed below.

Critical success factors

To implement the Committee's vision, a number of factors will be critical to success. First, the institutions need to design and build data models to manage the Operational Risk databases they develop and use. Second, they need to build and rely on generic risk models to increase their productivity in managing areas of risk that are replicated across the industry, such as certain aspects of the technology infrastructure. Third, they need to manage e-business innovation risk by focusing on the balance of risk versus reward. Lastly they need to implement a governance system that aggregates this information so that senior management can fully understand and manage the risk.

In summary, financial institutions have made relatively slow progress in measuring and managing Operational Risk. This reflects the complexity of the task. In a number of areas noted by the Committee, heavy reliance on qualitative parameters will be required. In contrast, the measurement and management of technology-centric operational risks, while certainly also complex, may prove to be more easily tackled as fewer qualitative parameters will be required. If the Committee has an interest, we would be pleased to discuss these matters.

Challenges to Implementing the BIS Vision, & Suggested Approaches to Address Them

The Committee advocates "the development of a sound process to identify in a consistent manner over time the events used to construct a loss database for the internal measurement approach". This will be a challenging task. We have identified 13 specific challenges to implementing the vision, and in the following sections we have described each one. In each case, we have also suggested a possible approach to address the challenge, and enable the measurement and management of Operational Risk.

Challenge 1 : Sourcing of Data

Comment on BIS paragraph 19, page 5 :

"The Committee urges the industry to work on the development of codified and centralised operational risk databases, using consistent definitions of loss types, risk categories and business lines. A number of separate processes are currently in train, and the Committee believes that both the supervisory and banking community would be well served by industry supported databases for pooling certain industry internal loss data".

1.1 The Internal Measurement Approach will require significant other data beyond an institution's actual losses. This is because many areas of Operational Risk are highly specialized, and will require specialist data that many institutions will be unlikely to have. The following are examples of such specialist areas:

Technology Infrastructure Data

1.2 Institutions are increasingly basing their operational systems on a technology infrastructure of significant complexity. They are often dependent on the robustness of this infrastructure to achieve their business objectives, such as the customer service and scalability required. As a result, institutions are exposed to Operational Risks of significant complexity.

1.3 In order to measure the risk in the technology infrastructure, the institution will need access to detailed data and information on the resilience of their networks. Further, they depend on the scale and criticality of the underlying processes, such as internal processing, payments and settlement: this includes most of the functions performed by central market utilities, such as clearing houses and settlement systems. The mitigation of these risks will often involve technologies such as self-diagnosing and self-healing systems, and loss data on these technologies is very likely to lie outside the institution. As the scale of the infrastructure increases, the diagnosis and repair of malfunctions become increasingly complex.

1.4 To manage these risks, financial institutions need to scope, analyze and interpret loss data in each technology area, and this is highly dependent on data about design of the infrastructure.

Information security data

1.5 There is an increasing trend to conduct business over networks, and even over the Internet. This means that information that institutions previously could confidently regard as secure and private now needs significant safeguards to assure its security and privacy. Loss data in this area is likely to be highly specialized, and institutions are likely to be dependent on expert suppliers to source it and soundly interpret it.

1.6 Moreover, the advantages that institutions see in conducting business over networks and the Internet are based on reaching an expanded customer set. This also raises the issue of dealing with trusted counterparties, or how to match on open systems the confidence that institutions have had in closed proprietary systems.

1.7 Extensive data is available on actual losses due to breaches in information security. At a minimum, the institution will require all available data on its own security breaches and its consequences. However, more data will be required. For example, the institution will require data on security breaches that could impact them, but have not done so yet. This requires data on the consequences of such security breaches that will reside with other institutions that have been impacted. They will also require data on the root causes of security breaches, such as new hacking methods. In most cases, the source of this data lies outside the institution.

Mergers and acquisitions data

1.8 In cases of mergers and acquisitions, the phases of negotiation, implementation and subsequent operation all involve significant Operational Risk. A particularly critical phase is the due diligence work that is done by the two institutions negotiating the merger. The completeness of this due diligence critically affects the cost benefit case that is proposed to the shareholders as part of the merger proposition. A comprehensive due diligence phase frequently requires highly expert people who adequately understand the operational consequences of the merger.

1.9 However, subsequent to the merger, the implementation phase can be just as critical. Most mergers commit to the shareholders a specific sum that will be saved through "synergy" -- for example, from combining operational infrastructures. The implementation and achievement of the synergy, and the delivery of the savings are in themselves significant Operational Risks that need to be managed.

1.10 The institution will at least need to assemble whatever data on M&A experience is available within the institution. However, in most cases, there will in addition be a much richer and more significant pool of data needed on comparable M&A experience in other institutions, particularly during the early phases.

Suggested approach to challenge 1 : sourcing of data

1.11 We have illustrated, from a technology infrastructure standpoint, the scale and extent to which Operational Risk can be specialized, and require specialist data. Comprehensive risk identification is required that decomposes the Operational Risk into its root cause components. The root causes need to be fully investigated, and the data needs to be identified that will be needed to measure the significance of the root causes. These are necessary conditions to putting in place effective mitigation plans to address the risk.

1.12 Additionally, in each process the Operational Risk needs to be broken down into its components , and the institution needs to identify the loss data that is required. Once that is the case, a self diagnosing infrastructure can be used to dynamically identify, and in some cases heal, significant shifts in the underlying risk.

Challenge 2 : Governance Structure

Comment on BIS paragraph 33, page 9 :

"The Committee proposes that the business lines will be the same as those used in the Standardised Approach. It is also proposed that operational risk in each business line then be divided into a number of non-overlapping and comprehensive loss types based on the industry's best current understanding of loss events."

2.1 Establishing loss types that are comprehensive yet non-overlapping can be a significant challenge. For example, some very large institutions have a matrix management organization, and this can frequently span a geographic structure.

2.2 This is an additional challenge to the effective collection of data. In order to support a governance structure, the loss scenarios developed need to be capable of aggregation and consolidation globally and across a business line. This will increase the challenge for those institutions in which regional geography structures have traditionally played a major role in organizational considerations, as well as for institutions organized on a matrix basis.

Suggested approach to challenge 2 : governance structure

2.3 The issue here is ownership of risk. In many business lines, explicit decisions need to be taken to fully apportion ownership of Operational Risk, so that there are no gaps and no overlaps. Once this has been done, the collection of data on loss events by business line will follow as a direct consequence.

Challenge 3 : Probability Data

Comment on BIS paragraph 35, page 9 :

"Probability of loss event (PE) represents the probability of occurrence of loss events, and loss given event (LGE) represents the proportion of transaction or exposure that would be expensed as loss, given that event."

3.1 In order to assess the probability of future loss events, a potentially wide range of data could be required. For example, to assess the probability of a power outage, this could include data on the power supplier's reliability, data on the financial institution's contingency plans for power supply, as well as data on the consequences of power loss within the financial institution.

3.2 Probability data has two aspects. Firstly, raw data: Is sufficient data available, and is there sufficient understanding of the interactions to model the loss distribution? Secondly, data modification: How does one modify the probability of an event or the associated event magnitude based on the risk management framework and the contingency plans that are in place?

3.3 First consider raw data. The underlying nature of both the probability of an event over time and the magnitude of that event over time can have significant impacts on the shape of loss distributions and the estimates of both expected and unexpected losses. This may require significant research in some areas of Operational Risk to develop a better understanding of the distributions and interactions.

3.4 Now consider data modification. The modification or adjustment of past data to account for new management systems, new operating contingencies or differences in process from the source of the data tends to be an inevitable and highly subjective activity.

3.5 The calculation of meaningful and objective estimates of operational losses based on limited prior data can be difficult if not impossible. However, through the use of sensitivity, "what if" or scenario modelling the importance of the different factors can be evaluated. The result can be used to determine which data is the most critical both in terms of developing an understanding of the underlying distributions and in the impact of modification to account for difference from the source data.

Suggested approach to challenge 3 : probability data

3.6 In summary, what is needed first is a full analysis of the mathematical steps required to estimate the probability. Then an inventory needs to be compiled of the data required to derive this estimate. Finally, if some of the data is difficult or expensive to obtain, it may be necessary to revisit the analysis to reach a cost-effective business compromise between the cost of the data and the effectiveness of the risk management.

Challenge 4 : Cause and Effect

Comment on BIS paragraph 37, page 10 :

"Current industry practice and data availability do not permit the empirical measurement of correlations across business lines and risk types. The Committee is therefore proposing a simple summation of the capital charges across business line / loss type cells."

4.1 While it is true that industry practice and data availability currently do not permit the measurement of correlations, this does not alter the fact that ignoring correlations might lead to seriously invalid conclusions.

4.2 A significant number of loss events involve a "cause and effect" chain of losses. Consider for example, the case of a power outage that leads to the settlement systems of two separate business lines being unable to operate. Suppose also that the institution had sufficient reserve power for only one of the business lines. This is a feasible scenario, yet one that results in a strong correlation between the Operational Risks in the two business lines.

4.3 A comprehensive analysis of this risk would need to include the losses that led to the power outage, the failure of the institution's business continuity plans, and the institution's operational contingency plans to deal with an inability to settle. The challenge here is that if the two business lines develop their risk scenarios independently, they might never recognize this critical risk interdependency.

4.4 We have observed cases where operationally caused losses have been categorized as credit or market losses. A cause and effect analysis would result in these risks being correctly apportioned to their correct owners. If this trend were widespread, it could suggest the Other Risks Technical Working Group's survey indicating the relative significance of the Operational Risk range could be on the low side.

Suggested approach to challenge 4 : cause and effect

4.5 These cause and effect relationships need to be established as part of the risk identification. If the cause and effect relationships cross the boundaries of business lines, these business lines then need to cooperate in the scenario development to identify all the interdependencies, and carry out a comprehensive risk analysis.

Challenge 5 : Past versus Future

Comment on BIS paragraph 39, page 10 :

"The historical loss observation may not always fully capture a bank's true risk profile, especially when the bank does not experience substantial loss events during the observation period."

5.1 In addition to the lack of events during the observation period, there are other significant factors. For example, in a bank implementing any kind of business change, the past and future risk profiles might be entirely different. In this situation, past losses are a poor or no basis on which to assess future risks.

Suggested approach to challenge 5 : past versus future

5.2 By definition, loss data is historical, yet many of the Operational Risks concern future change. Institutions will need significant interpretative expertise to assess the operational exposure in future change programs, while basing the analysis on the evidence of past losses. A significant part of this expertise may need to be contributed by other institutions in the industry with knowledge and/or experience of operating similar implementations.

5.3 This is another area where case studies can be very valuable. They can provide an institution with critical insight into technology infrastructures, by helping them learn from people with knowledge of other operational implementations. Case studies can also show development trends that can indicate the comparison between different stages of planning and development. For example, this approach could be used to substantiate a comparison between the successive stages of an e-business implementation.

Challenge 6 : Comparability Data

Comment on paragraph 39, page 11 :

"As previously noted, a regulatory specified gamma term, which is determined on an industry wide loss distribution, will be used across banks to transform a set of parameters, such as EI, PE and LGE, into a capital charge for each business line and risk type. However, the risk profile of a bank's loss distribution may not always be the same as that of the industry wide loss distribution."

6.1 In the technology infrastructure, in cases where industry norms are reliably documented, this difference between loss distributions frequently occurs.

Suggested approach to challenge 6 : comparability data

6.2 What is required is comparability data. In these cases, it is key to complement data on the institution's own losses with data on losses outside the institution. For example, this can help the institution learn from the consequences of failure from other institutions in a similar line of business.

6.3 However, this data on other institutions will usually need to be adjusted to make it comparable, e.g. when the other institution is of a different size is in a different geography or has a different business profile.

6.4 Comparison scenarios of this type will be needed to ensure this comparability data is included in the scope of data required.

6.5 A further challenge is that comparability data will tend to identify the institution concerned, and this conflicts with the desire for confidentiality. To achieve comparability and confidentiality, care will be needed to structure the data, and this needs a data model, as explained under Challenge 9 below.

Challenge 7 : Readiness for 2004

Comment on BIS paragraph 41, page 11 :

"In the proposed evolutionary framework of the approaches to determine capital charges for operational risk, individual banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices"

7.1 A major challenge to moving from the standardized approach to the internal measurement approach by 2004 will be the bank's ability to assemble enough data to qualify in the time available.

Suggested approach to challenge 7 : readiness for 2004

7.2 To assemble sufficient data in time to qualify, institutions will need to have gathered data that covers a reasonable time span. This means they will need to start collecting data very soon. As we have seen from the above section on data sourcing, although it is essential for the institution to collect data on its own losses, much of the total scope of data required in fact lies outside the institution.

7.3 A great deal of useful data already exists on operational losses, particularly in some of the technology areas involved. Significant progress can be made in the short term to collect and structure this data into a form that can help meet the requirements of the BIS proposal.

7.4 To fully scope and then collect the needed data will require a four-phased approach. First, the risk needs to be comprehensively identified. Second, the analysis approach necessary to measure the risk needs to be designed. Third, an inventory needs to be compiled of the data needed to support the analysis. Finally, as in challenge 3, there may well be data that is difficult or expensive to obtain. In this case, it will be necessary to recycle through these phases and make commercial decisions on a cost-effective plan to collect the data.

Challenge 8 : Data Responsibilities

Comment on BIS paragraph 43, page 12 :

"Banks must begin to systematically track relevant operational risk data by business line across the firm. It should be noted that the ability to monitor loss events and effectively gather loss data is a basic step for operational risk measurement and management and is a pre-requisite for movement to the more advanced regulatory approach."

8.1 In order to do this, banks will need to access data from a significant number of sources, with each of these sources taking responsibility for its validity. Quality risk data depends on participation from people with complementary but different responsibilities. To take an example from the airline industry, to collect data on metal fatigue, the industry did not ask the airlines to do it individually. Ultimately, the risk assessment will be built up from a broad range of data inputs. Consider an example from the field of airline safety. From a passenger's viewpoint, the safety of a specific flight is made up of a number of components, for example:

- Data that determines the safety of all aircraft, e.g. metal fatigue, and this needs to be supplied by aircraft manufacturers

- Data that determines the safety of all flights, e.g. reliability of air traffic control, and this needs to be provided by the air traffic controller

- Data that determines the safety of the specific flight, e.g. the training, experience and track record of the crew of the flight deck.

Suggested approach to challenge 8 : data responsibilities

8.2 The collection of the data also requires different areas of expertise. This can include those who can best collect the data (e.g. a counterparty, information provider, manufacturer, service provider, etc), and those who are best placed to check its validity and objectivity (e.g. a trade association). In each area, it is key that specialist experts be responsible for the data. There also needs to be organized teamwork to ensure the data aggregates to rigorously substantiate the conclusions.

Challenge 9 : Data Models

Comment on BIS paragraph 44, page 13 :

"Banks must have in place a sound process to identify in a consistent manner over time the events used to construct a loss database and to be able to identify which historical loss experiences are appropriate for the institution and are representative of their current and future business activities."

9.1 To be consistent over time, and to be representative, banks need a disciplined approach to managing their data. The discipline of data management recommends this be done through the development of a data model.

9.2 Institutions need a clear understanding of the exact meaning of each item of data, and also of the relationship between different data items. For example, consider a data item on security breaches. Suppose it indicated that over $100m had been lost as a result of an institution's 10 worst information security breaches in the US. To really understand this data, the institution needs to know some significant facts: for example, what definition was used for a security breach?

9.3 In the above example, the value of the data model is that it would provide all the explanatory facts required. It would include the precise definition of a security breach that was used. Many breaches go unnoticed, and so it would define how they were identified. It would also define more subtle facts: for example, whether the selection method first identified the 10 worst breaches, and then selected those in the US, or whether it was vice versa. This would give a different result.

9.4 By building a data model, the institution discovers the semantics of their enterprise's data, which exist whether or not they happen to be recorded in a formal data model. Data definitions, relationships and attributes are fundamental to all enterprises. However, their meaning may be poorly understood until they have been clearly documented.

Suggested approach to challenge 9 : data models

9.5 Significant work will need to be done to specify, design and implement data models for the operational loss data of each institution. A significant part of this work will require the knowledge of experts who understand data models, working together with those who understand the specialist data.

Challenge 10 : Outsourcing

Comment on BIS paragraph 48, page 15 :

"The Committee believes that banks engaged in outsourcing should aim to ensure that a "clean break" in their outsourcing activities is established, if there is to be reduction in operational risk capital, mainly through arranging robust legal agreements with outside service providers. Banks should also develop appropriate policies and controls to assess the quality and stability of outside service providers."

10.1 A "clean break" is undoubtedly a desirable goal in the working and contractual relationships between an institution and its outsourcing service provider. However, there are a number of challenges to implementing a clean break.

10.2 First, just as no business can afford to reduce all risks to zero, no outsourcing service provider can avoid all risks inherent in the process being outsourced. In many cases, the agreement does not provide funding to reduce the risk below its original level. As the Committee recommends, the institution needs to rigorously assess these residual risks.

10.3 However, the complication arises in assessing the residual risks the service provider is not funded to reduce. For example, there will always be a limit on the transaction volumes the service provider can handle. If the institution's transaction demand were to increase beyond this limit, the resulting scenario is one in which the institution and service provider would need to co-operate closely to manage the resulting operational exposure.

Suggested approach to challenge 10 : outsourcing

10.4 Outsourcing agreements need to start with a comprehensive risk assessment, so that all the residual risks are understood. The next step is for the institution and service provider to negotiate the apportionment of accountability for these risks, as part of the outsourcing agreement. This negotiation can be greatly facilitated by building a statistical risk model to represent the risks both of the institution and those of the service provider. This shared knowledge and understanding can be the basis on which a robust win-win agreement can be negotiated.

Challenge 11 : Mitigation Techniques

Comment on BIS paragraph 49, page 15 :

"In an effort to encourage better risk management practices, the Committee is keenly interested in efforts by institutions to better mitigate and manage operational risk. Such controls or programs have the potential to reduce the exposure, frequency, or severity of an event. Due to the crucial role these techniques can play in managing risk exposures, the Committee intends to work with the industry on risk mitigation concepts over the next several months."

11.1 A key success factor in implementing effective mitigation strategies is the business case that determines the benefit versus the cost. This will include consideration of the potential capital effect, compared to the cost of improving controls, system enhancements and data collection.

Suggested approach to challenge 11 : mitigation techniques

11.2 In cases of technology-related Operational Risk, where a reliable sizing of the risk exposure is possible, risk models can measure the potential or actual effects of mitigation.

Challenge 12 : Low Frequency High Severity Losses

Comment on BIS paragraph 44, page 14 :

"A process would need to be developed to identify and incorporate plausible historically large or significant events into assessments of operational risk exposure, which may fall outside the observation period"

12.1 These events constitute a significant challenge to collecting loss data. It is equivalent to collecting data on “the 100 year storm.” These are the high-impact, low-probability events for which there is, by definition, insufficient evidence to fully substantiate a conclusive decision. But due to the very limited range of loss experiences, these scenarios are difficult to analyze effectively.

12.2 In such cases, an individual institution is unlikely to have experienced a statistically significant number of such failures. To identify loss experiences representative of their business activities, these institutions will be dependent on loss data from outside their own institution.

12.3 Naturally, these are also areas where financial institutions make conscious decisions on how much they will spend to mitigate the risk.

Suggested approach to challenge 12 : low frequency high severity losses

12.4 To deal with these losses, it is necessary to collect global and industry-wide data from case studies on issues such as the above examples of information security, business continuity and network resilience. In addition, some of the required data is cross industry. For example, data from other industries such as insurance, manufacturing, distribution, telecommunications and travel can increase the supply of the rare data needed to substantiate these types of risk assessment.

Challenge 13 : Business Innovation

Comment on BIS paragraph 51, page 16 :

"An institution's ability to meet specific criteria will determine the specific capital framework for its operational risk calculation. To the extent they can demonstrate to supervisors increased sophistication and precision in their measurement, management and control of operational risk, institutions are expected to move into more advanced approaches. This will generally result in the reduction of the operational risk capital requirement."

13.1 While business innovations can often reduce risk, this may not always be the result. Most business innovations involve some uncertainty over both risk and reward. A good example would be the adoption of an e-business infrastructure to implement a new Internet-based business model. Institutions are now using technology to automate not only their supply chains, but their value chains as well. Early entrants have exploited e-business to improve customer service, increase productivity and cross national borders. More mature implementations are using it to implement far more powerful business models, such as instant auctions where the counterparties have nothing more in common than their connection to a Web site, and could be located anywhere in the world.

13.2 Business innovation benefits are not achieved without changing the underlying risks. Risks heightened by innovations such as e-business can include information security and privacy, fraud, the need to scale transaction volumes and the number of customers, and to deal with diverse regulatory and tax jurisdictions.

13.3 A major challenge we have observed is that many of these value propositions are in relatively uncharted waters. The loss data to underpin the analysis of these risks will not only be rare, it will also to a great extent be owned by institutions that have already experimented with the new propositions. Many of these will have discarded them, changed them significantly from their original intent, or scaled them for a different business environment.

Suggested approach to challenge 13 : business innovation

13.4 In business innovations such as e-business, risk management means dealing with the uncertainty about potential loss, and about potential benefit. To manage this situation, institutions need a method to net off upside versus downside uncertainty. This can be done with SWOT analyses (strengths, weaknesses, opportunities and threats).

13.5 Given that the risks in an e-business implementation can be quantified, then so can the SWOT analysis. A quantified SWOT analysis on an e-business venture can give senior management the focused, balanced and tangible view that they need. This will be critical to the risk reward decisions they need to take to design a successful e-business implementation.

Conclusion

Financial institutions have made relatively slow progress on measuring Operational Risks. This reflects the complexity of the task. For example, we have seen that there are challenges in sourcing data, collecting probability and comparability data, doing analyses on cause and effect, and finding sufficient data on low frequency high severity losses.

In a number of areas, the Committee has identified that heavy reliance on qualitative parameters will be required. This will be important, given the desire to be ready in 2004, to put in place quality mitigation techniques, and to establish an effective governance structure.

In contrast, the measurement of technology-centric Operational Risks, while certainly also complex, may prove to be more easily tackled. For example, replicable risk models have already been used for outsourcing, and quantified SWOT analyses have been used to manage the complex risk versus reward decisions that need to be taken in e-business. Further, the benefits of data models have been proven within the discipline of information technology.

The history of market and credit risk has demonstrated that measurement is a pre-condition of effective risk management. Within the bounds of technology-centric Operational Risk, that is an achievable goal. To implement the Committee's vision, four factors will be critical to success. Their effects are detailed in the appendix below. The four critical success factors are:

Manage Database Development

Data is the key to quantative management of Operational Risk. The sourcing, collection, analysis, storage and management of data will require significant investment to ensure effective risk management. Some companies have invested millions in developing databases, even for Operational Risk, but have later had to discard them due to faulty design. The design needs to accurately reflect the institutions' needs for data structure, ownership, confidentiality, consistency and speed of access. The most effective way to do this is to develop a data model. The design needs to be agreed before the start of database development, and this requires expert management.

Develop Generic Risk Models

As market and credit risk have shown, the challenges in risk management are most effectively addressed with a statistical risk model. This translates the complexity into a clear representation that enables management to focus on and prioritize the remedial action. Market and credit risk models are sufficiently generic to be replicated throughout the industry. But institutions' operational processes and infrastructures are so diverse, that it is a major challenge to develop a generic model for Operational Risk. However, it is possible to develop generic models for specific areas of Operational Risk. This is especially the case in areas of technology infrastructure such as information security and network resilience.

Manage Innovation Risk, e.g. e-business

Institutions are steadily increasing their investment in e-business. They are transferring not only their supply chains, but also their value chains from a physical to a network-based implementation. Technology can drive not only the downside but also the upside risk. Depending on the technology design, downside risks in one implementation can be upside risks in another. For example, security, privacy, scalability, re-branding, globalization and new business models such as e-marketplaces. Technology also introduces new ways to manage risk, bringing security safeguards such as public key infrastructure. It is critical to manage the risk versus the reward, and there are proven methods of doing this, such as quantified SWOT analyses.

Implement a Governance System

The purpose of a governance system is to provide senior management with the information that enables them to manage. Firstly, they need effective reporting: defining the risk, developing the plan to mitigate it, and monitoring how well the plan implementation is progressing. Secondly, when there is a problem, senior management need to be well enough briefed to effectively intervene. An effective data model, generic risk models and quantified SWOT analyses can enable institutions to implement a quantified governance system for technology-centric Operational Risk.

Final comment

Financial institutions have made relatively slow progress in measuring and managing Operational Risk. This reflects the complexity of the task. In a number of areas noted by the Committee, heavy reliance on qualitative parameters will be required. In contrast, the measurement and management of technology-centric Operational Risks, while certainly also complex, may prove to be more easily tackled, as fewer qualitative parameters may be required. If the Committee has an interest, we would be pleased to discuss these matters.

Appendix : Operational Risk Critical Success Factors, and the Challenges they Address

Critical success factors, and the challenges they address	Manage database development	Develop generic risk models	Manage business innovation, e.g. e-business	Implement a governance system
1. Sourcing of data	O	O		
2. Governance structure		O	O	O
3. Probability data	O	O		
4. Cause and effect	O	O		
5. Past versus future	O	O	O	O
6. Comparability data	O	O		
7. Readiness for 2004	O	O	O	O
8. Data responsibilities	O	O	O	O
9. Data models	O		O	O
10. Outsourcing			O	O
11. Mitigation techniques		O		O
12. Low frequency high severity losses	O			O
13. Business innovation		O	O	O