Testimony of
Steven G. Elliott
Senior Vice Chairman
Mellon Financial Corporation

Before the
Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
U.S. House of Representative

June 22, 2004

It is a pleasure to testify today before this Subcommittee on the potential impact of Basel II on Mellon Financial Corporation and, more broadly, on the ability of U.S. banks to serve their customers and investors. It was an honor also to appear last June before this panel on this topic. I am grateful for the Congress' continuing interest in the Basel Accord. Your focus on this sometimes overwhelmingly technical rule has ensured attention by regulators at home and abroad on what the changes to the international risk-based capital rules mean on the most important level: the ability of individual and corporate customers to get what they need at a price they like from a vibrant U.S. financial services industry.

Mellon Financial Corporation is one of the world's leading providers of financial services, with extensive product capabilities that it has offered to its customers for more than 130 years. Headquartered in Pittsburgh, Mellon provides its services to institutions, corporations and high net worth individuals, providing institutional asset management, mutual funds, private wealth management, asset servicing, human resources and investor solutions, and treasury services. Mellon has approximately $3.6 trillion in assets under management, administration or custody, including more than $675 billion under management.

As a specialized financial institution, Mellon has a special concern with a particular aspect of the Basel II proposal: the new regulatory capital charge for operational risk. We think much in the proposed new international capital standards and in the way regulators here plan to implement them are quite good. Indeed, the current risk-based capital standards need a wholesale rewrite. However, the overall need for new capital standards should not distract from the critical importance of getting the details right. The operational risk charge could well have a dramatic and adverse competitive impact on specialized banks. Trillion-dollar diversified banks can offer a broader range of services to their customers. However, that is often done at a cost – the inability to focus clearly on individual clients who want a high degree of expertise in areas like asset management and payment processing.

Mellon is grateful to you, Chairman Bachus and the leadership of this Subcommittee, along with that of the Financial Services Committee under Chairman Oxley and Ranking Member Frank, for your continuing attention to the many problems with the operational risk charge, particularly its potential adverse competitive impact. You have rightly pressed the Federal Reserve to analyze the Accord's competitive impact. We understand that the Board is currently studying the operational risk-based capital charge's competitive impact. Mellon is of course happy to cooperate in any way that would help in bringing about the right result. The Board has also completed a study on the rule's impact on mergers and acquisitions – a key question to ensure that the nation's banking system doesn't become too consolidated. I would argue that there is a direct correlation between capital and business activity. If it wasn't, it's hard to understand why all of the

U.S. and international banking agencies have devoted so many years of hard work to the Basel II rewrite. This is far from a technical exercise, but rather one with profound implications.

Today, I would like to emphasize:

- the need for the Basel rules – and especially the U.S. version – to rely on effective prudential regulation and enforcement to address operational risk. An arbitrary regulatory capital charge for operational risk like the one now proposed will have adverse market consequences that will ultimately undermine customer service;

- the risks posed by the operational risk capital charge, even in the "advanced" version proposed in the U.S. We continue to believe that ongoing improvements to operational risk management will be undermined by the proposed capital charge, creating perverse incentives for increased operational risk, not the decrease regulators desire and on which Congress should insist; and

- the importance of other changes to the U.S. version of Basel II to ensure that our banks remain competitive and focused on key market needs. This means a review of the complex credit risk standards for specialized banks. A hard look at the proposed retention of the leverage standard and the criteria for determining who is a "well-capitalized" bank is also vital, since these standards govern only U. S. banks and could have adverse competitive impact if retained.

As I shall discuss in more detail, Mellon respects the desire by the regulatory agencies in Basel and the U.S. to advance operational risk management. That's why the Financial Guardian Group, to which Mellon belongs, has answered the U.S. regulators' request for a detailed and enforceable safety-and-soundness standard with a comprehensive proposal. I have attached that proposal to this statement for your consideration. The U.S. regulators have also asked us if a safety-and-soundness approach (called Pillar 2 in the Basel II framework) could be paired with improved disclosure (Pillar 3) to back up regulatory enforcement with market discipline. We took that request very seriously and provided a detailed proposal which I have also attached to my statement. The Federal Reserve Board thanked us for our submission, but does not appear to be pursuing it as an option.

Is a capital charge for operational risk a detail that can be worked out later as regulators finalize the capital rewrite? I don't think so since it would be fairly costly. Application of the OR charge would obligate us to review our business model and incorporate a regulatory capital charge that bears little reflection to the real risks that we run.

What is operational risk?

Before I go too far into the complicated details of Basel II and the proposed capital charge for operational risk, I think I should first explain operational risk. It's an important risk, and one to which Mellon's senior management dedicates much attention and considerable resources. Operational risk – OR, for short – is the risk of systems or human failures, as well as the impact from natural or manmade disasters like hurricanes or terrorist attacks. The bank regulators have decided to include in their OR definition "legal risk". This type of risk includes the risk resulting from tort liability, securities suitability standards, and the laws against loan and employment discrimination-among many others. These same legal standards, however, do not apply in many other countries or legal systems. One must question why US regulators would agree to a capital charge for US banks arising from laws and regulations unique to our country that are designed to achieve our own social objectives- especially given the requirement for reserves against material legal risk. Furthermore, these are laws that have no known bearing on any bank's failure. In cases where a bank may be subject to legal risk, securities law requires full disclosure of material matters, thus the operational risk proposal would have no new impact on market discipline. Moreover, litigation loss history provides limited insights into future losses, creating significant challenges to modeling. Since legal losses are typically closely linked to individual events and circumstances, the use of external data is particularly inappropriate for legal risk.

The bank regulators have decided to exclude "reputational risk" – that is, violations of customer expectations, regulatory requirements or social expectations that damage investor or customer confidence. I'm not at all certain that the regulatory OR definition – legal risk in, reputational risk out – is the correct one, but I know that it is extremely difficult to quantify much that the regulators call operational risk. Without reliable, tested and industry-standard models for defining and quantifying operational risk, a capital charge to offset a risk that cannot be clearly quantified doesn't make sense.

How Do Banks Now Handle OR

Operational risk is covered in two ways. First, through critical risk management efforts that include investments in operational risk infrastructure, systems, processes and people (compliance, audit, legal, risk management) as well as contingency planning, disaster preparedness, back-up facilities and redundancies (the latter would help deal with a 9/11-type risk). Second, OR is ordinarily covered by revenues, reserves, insurance and risk mitigation. These latter techniques are particularly helpful for managing "expected loss" (EL). This is, for example, the risk that we know that a computer will make mistakes a certain percentage of the time or the likelihood that an employee will misplace an order or misread a trade. We know how to anticipate and guard against these risks, and we have a range of tested systems in place to address them. The list of bank problems circulated in the regulators' discussion of OR that tries to rationalize the capital charge includes not a single incident of expected loss risk. The Basel Committee earlier this year rightly decided to take expected credit loss out of that aspect of Basel II, focusing the rule instead only on unexpected loss (UL) because of a comparable problem with the role of expected credit loss on bank failures. However, the proposed new capital charge

for OR – even in its most "advanced" form – still covers both EL and UL. Since EL is well handled now and UL – the risk of a 9/11 attack, for example – is immeasurable, the capital charge is deeply flawed.

Additional Problems with a Regulatory Capital Charge

In my testimony before this panel on June 19, 2003, I went into considerable detail on the problems with the operational risk-based capital (ORBC) proposal. Nothing in the advance notice of proposed rulemaking published by the U. S. agencies thereafter addressed any of these fundamental flaws, although we appreciate that numerous questions about them were posed. Since then, the Basel Committee has made some changes to the final version of the rules, which are expected later this week in final form. However, these changes we anticipate will fail to reflect the fundamental problems in the ORBC proposal – problems that can only be fixed by eliminating the proposed capital charge from "Pillar 1" regulatory capital standards and substituting strong supervisory standards and enhanced disclosures. Mellon is not alone in its opposition to a Pillar 1 capital charge, although specialized banks will be adversely affected by it. Even banks that may broadly support the concept of a regulatory capital charge – which we don't – have problems with how an ORBC requirement will work in practice. Other institutions that, like Mellon, strongly oppose a Pillar 1 charge, based on their public comments, include Wells Fargo, MBNA, Washington Mutual, Merrill Lynch, Lehman Brothers and Goldman Sachs.

Numerous commenters – including several Federal Reserve Banks and the Federal Reserve Bank of New York's Foreign Exchange Committee have also noted serious problems with a quantitative approach to operational risk. Indeed, the Federal Reserve Bank of Chicago filed a comment with the Basel Committee making clear the numerous problems with an operational risk capital charge.[1]

The Federal Reserve Bank of Richmond also filed a comment noting that operational risk can be "[a] difficult risk to quantify and can be very subjective."[2] The Federal Reserve Bank of San Francisco has noted, "[a] key component of risk management is measuring the size and scope of the firm's risk exposures. As yet, however, there is no clearly established, single way to measure operational risk on a firm-wide basis."[3]

I would like to summarize key problems with the current version of the ORBC proposal beyond the basic one that capital can't be assessed for risks no one can define or measure in a uniform, industry-wide way. They include:

- An ORBC charge creates perverse incentives to effective OR management. The "advanced measurement approach" (AMA) proposed by U.S. regulators

---

[1] *Federal Reserve Bank of Chicago Response to BIS Capital Proposal*; Federal Reserve Bank of Chicago; May, 2001.
[2] *"The New Basel Accord" Second Consultative Package, January 2001*; Federal Reserve Bank of Richmond; May 30, 2001.
[3] *FRBSF Economic Letter,* Federal Reserve Bank of San Francisco, January 25, 2002.

is designed to fix the acknowledged flaws in the more simple ORBC options included in the original Basel II proposal, but it still doesn't resolve this serious problem. For example, insurance isn't fully recognized, even though the "loss data collection" exercise conducted by Basel last year showed that insurance reimbursed banks for the vast majority of expected and unexpected operational losses.

- There will likely be major disparities in the way regulators in different countries will impose the ORBC charge because there is no accepted definition or way of measuring OR. The Basel Committee has tried to address this through a "hybrid" approach to deciding which regulator sets the capital charge for which subsidiary of an internationally-active bank, but this compromise leaves many important issues unresolved. Since host-country regulators can fundamentally set whatever ORBC charge they want, they could well set ORBC in a way that advantages their own banks at the cost of those seeking to enter their markets. This can particularly disadvantage U.S. banks because of the much stricter and thorough US regulatory environment.

- These potential competitive problems are exacerbated by the much more encompassing supervisory and enforcement roles of U.S. bank regulators than the approach adopted in many other nations. Japanese banks, for example, were deemed by the Japanese regulator to comply with their regulatory capital standards for over a decade despite objective analysis which showed that serious credit risk problems meant that those banks did not comply. In the EU, bank regulators rely on auditors, not their own examiners, to determine if banks meet capital standards. The auditors, in essence, wear two hats – working for their bank clients that pay them and the regulators that rely on their reviews, clearly not a good situation under Sarbanes-Oxley and bound to raise questions in this post-Enron environment. Thus, non-U.S. banks can stay open for business and compete vigorously against U.S. banks even if comparable conditions for a U.S. bank would likely lead to severe sanctions under Prompt Corrective Action procedures.

- Reliance on untested, ill-understood models to set ORBC creates "models risk." That is, all banks will set capital in the same way even if their risks vary dramatically – what experts call "endogenization" and what I call the herd mentality. Reliance on diverse models tested by bank supervisors on a case-by-case basis ensures that different circumstances are appropriately reflected. Improved disclosure would ensure accurate market understanding of these differences and impose discipline on them where needed.

- ORBC established through arbitrary regulatory capital standards will adversely affect specialized banks competitively because the many non-banks against which they compete in key business lines remain outside the Basel capital standards. This remains true despite the "consolidated supervised entity" capital rule recently adopted by the Securities and Exchange

> Commission because the Basel capital standards will apply only at the parent company level for some large non-banks, with many remaining outside this framework and, thus, free from regulatory ORBC. Further, the SEC's capital charge for covered investment banks is substantially different than the charge imposed on U.S. banks and the capital charge is offset in part by a huge drop in regulatory capital for broker-dealers.[4]

Credit Risk Concerns

In general, Mellon supports the proposed rewrite of the credit risk-based capital (CRBC) standards. We unequivocally support their goals – better correlation of regulatory capital with economic capital (that is, the amount of capital market forces demand to protect against risks). Differences between regulatory and economic capital can have profound market impact — companies that have to hold undue amounts of regulatory capital because of rules that don't apply to their competitors must meet investor profit expectations because their basic "return on equity" equation is skewed against them and in favor of competitors with a smaller capital base. Conversely, banks that don't hold enough economic capital for high-risk positions and still comply with their rules can take business away from firms subject to market discipline. This, of course, puts both these banks and the FDIC at undue risk.

However, a balance must be struck between getting regulatory capital precisely right and the complexity and burden associated with doing so. Basel II is a very costly proposition**.** An April PriceWaterhouseCoopers study, commissioned by the European Commission, estimates Basel implementation costs for large banks to range between $98-$181 million. Thus, wherever possible, regulators should balance the proposal with simplifying assumptions appropriate for industry segments or particular circumstances. We note that the final version of Basel II takes such an approach for revolving credit exposures – one of the most difficult and complex sections in the proposal – and we urge that type of simplification also be applied to other aspects of the rule.

In particular, we believe that regulators should ensure that specialized banks with minimal credit risk positions do not need to take on all the modeling and related cost burdens appropriate to diversified banks with large credit risk. A more simple approach to CRBC is appropriate for specialized banks whose main activities are providing asset management, custody, payments processing and other "agency" type services.

Mellon and other institutions are currently working with the U.S. regulators on ways to address this concern. We appreciate their interest in a suitable CRBC framework for specialized banks, but we would urge Congress to ensure that the final U.S. rules do not impose an unnecessary regulatory burden.

---

[4] *Alternative Net Capital Requirements for Broker-Dealers That Are Part of Consolidated Supervised Entities*, Securities and Exchange Commission, Final Rule, June 8, 2004.

Broader Revisions to the U. S. Capital Proposal

The advance notice of proposed rulemaking issued last year states that OR was implicit in the Basel I Accord, which included a "buffer" to account for OR and other non-credit risks. With an AMA approach, the ANPR says no such "buffer" is required because no implicit risks remain in the regulatory capital charge. Of course, interest-rate risk, liquidity risk and many other types of risk remain without a specific regulatory capital charge. We would refer to the "supervision-by-risk" framework rightly used by all of the agencies, and would note the many specified risks for which no Pillar 1 capital charge is proposed.[5] Many of these risks – interest-rate risk, of course, but also liquidity and foreign-exchange risk – are quantified daily, in sharp contrast to operational risk, but only OR is included as a new charge in the ANPR.

The agencies in fact appear to recognize that a "buffer" remains important because of the proposed retention of the unique U.S. leverage capital standards, as well as the use of 10% as the risk-based capital criterion for eligibility as a "well-capitalized" financial holding company or insured depository. These standards are anachronistic and should be abolished, especially if a Pillar 1 ORBC charge is retained. With these standards in place and a new ORBC charge mandated, the overall cost of the Basel rules rises so high as to create undue economic cost and unnecessary competitive damage. Given that U.S. banks – in sharp contrast to EU banks – compete every day against firms outside the bank capital rules in key lines of business, these costs are particularly inappropriate and excessively burdensome.

Chairman Greenspan has recently pointed to the problem of retaining the leverage standard as the new risk-based rules are implemented. At an April 20 hearing before the Senate Banking Committee, Sen. John Corzine questioned retaining the leverage rule because, he rightly said, it undermines the whole point of mirroring economic risk with regulatory capital. A flat percentage capital charge against assets regardless of risk – the leverage requirement – totally contradicts the whole point of the Basel II exercise. Chairman Greenspan said he thought the leverage ratio might be phased out over time. We think it should be phased out immediately, especially given the many floors imposed in the Basel II Accord that would significantly limit any benefit from the new rules and, therefore, any risks associated with an overly-aggressive drop in regulatory capital for low-risk assets.

Quite simply, the U.S. rules must drop the leverage standard and readjust the well-capitalized one to reflect the fact that some banks will in fact be very well capitalized at far different ratios than now apply. Failure to drop these arbitrary ratios – especially if the ORBC requirement remains in Pillar 1 – would seriously undermine the goals of the ANPR and the larger policy interests served by alignment of regulatory and economic capital.

---

[5] *Comptroller's Handbook for Large Bank Supervision*, Office of the Comptroller of the Currency, May 2001.

Conclusion

In conclusion, Mellon again thanks the Committee for focusing on this important issue. While, as noted above, the ORBC charge poses serious concerns for institutions like Mellon, we are hopeful that the continued support of the Committee, as well as cooperation with our regulators will ensure that the final U.S. rules do not contain a regulatory capital charge for operational risk.

PROPOSED PILLAR 2 FOR OPERATIONAL RISK-BASED CAPITAL

The following proposed Pillar 2 for operational risk is adapted from the Basel Committee's "Sound Practices for the Management and Supervision of Operational Risk" and also draws heavily on the Federal Reserve's SR 99-18. The FGG believes it outlines a comprehensive framework for effective measurement, management and mitigation of operational risk based on allocation of appropriate economic capital against it. Thus, this approach ensures a comparable framework for banks and their supervisors without the numerous hazards resulting from a Pillar 1 ORBC requirement.

As discussed in detail in the accompanying comment letter, the FGG believes U.S. regulators have ample ability to ensure supervisory guidance without resort to the crude capital charge on which some foreign supervisors feel they must rely. Numerous instances in which the regulators have mandated significant sanctions – up to and including closure – in cases of violations of prudential rules make this clear.

PROPOSED PILLAR 2

I. Background

While the exact approach for effective operational risk management chosen by an individual bank will depend on a range of factors, including its size, sophistication and the nature and complexity of its activities, clear strategies and oversight by the board of directors and senior management, a strong operational risk and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for banks of any size and scope.

Deregulation and globalization of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their risk profiles more complex. Greater use of automation has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems. Further, growth of e-commerce brings with it potential risks (e.g., internal and external fraud and system security issues). Large-scale acquisitions, mergers, de-mergers and consolidations test the viability of new or newly integrated systems, while the emergence of banks as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems. Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements, and asset securitizations) to optimize their exposure to market risk and credit risk, but these techniques may in turn produce other forms of risk. Finally, growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.

II. Operational Risk

In sum, all of these types of risk are operational risk, which the agencies define as the risk of loss from inadequate or failed internal processes, people and systems or from external events.

Operational risk includes:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- External fraud. For example, robbery, forgery, check kiting, and damage from computer hacking.
- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.
- Damage to physical assets. For example, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty non-performance, and vendor disputes.

Operational risk exists in the natural course of corporate activity. However, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses. In some business lines with minimal credit or market risk (e.g., asset management, and payment and settlement), the decision to incur operational risk, or compete based on the ability to manage and effectively price this risk, is an integral part of a bank's risk/reward calculus.

III. Keys to Effective Operational Risk Management and Mitigation

1. Role of the Board of Directors

The board or a designated committee is responsible for monitoring and oversight of a bank's risk management functions, and should approve and periodically review the operational risk management framework prepared by the bank's management. The framework should provide a firm-wide definition of operational risk and establish the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

The board of directors should approve the implementation of a firm-wide framework to explicitly manage operational risk as a distinct risk to the bank's safety and soundness. The board should provide senior management with clear guidance and direction

regarding the principles underlying the framework, be responsible for reviewing and approving a management structure capable of implementing the bank's operational risk management framework, and should approve the corresponding policies developed by senior management.

2. Internal Audit

The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the internal audit program focused on operational risk is appropriately risk focused. Audits should periodically validate that the firm's operational risk management framework is being implemented effectively across the firm. The board, or the audit committee, should ensure that the internal audit program is able to carry out these functions independently, free of management directive.

To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities. Some banks may involve the internal audit function in developing an operational risk management program as internal audit functions generally have broad risk management skills and knowledge of the bank's systems and operations. Where this is the case, banks should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner.

3. Role of Senior Management

Senior management must ensure that the board-approved operational risk framework is implemented at all levels of the organization and that all levels of staff understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes, and procedures for managing operational risk in all of the bank's material products, activities, processes, and systems.

Management should translate the operational risk management framework approved by the board of directors into specific policies, processes, and procedures that can be implemented and verified within the different business units. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures, and controls within its purview, senior management should clearly assign authority, responsibility, and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

Senior management should ensure that bank activities are conducted by qualified staff with necessary experience, independence, technical capabilities and access to resources to carry out their duties. Management should ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels in units that incur material operational risks.

Senior management should ensure that the operational risk management framework is integrated with efforts to manage credit, market, and other risks. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management program.

Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes, and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

4. Operational Risk Identification

Banks should identify and assess the operational risk inherent in all material products, activities, processes, and systems. Banks should also ensure that, before new products, activities, processes, and systems are introduced or undertaken, the operational risk inherent in them is identified.

Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organizational changes, and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

Amongst the possible tools used by banks for identifying and assessing operational risk are:

- Self or Risk Assessment: a bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used by banks to allocate economic

capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

- Risk Mapping: in this process, various business units, organizational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritize subsequent management action.
- Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.
- Measurement: some firms have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events.

5. Risk Monitoring

Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes, and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

In addition to monitoring operational loss events, banks should identify appropriate indicators that may provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, and system downtime, among others. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a bank's activities. The results of these monitoring activities should be included in regular management reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory

authorities may also be useful in this monitoring and should likewise be reported internally to senior management, where appropriate.

Senior management should receive regular reports from appropriate areas such as business units, group functions, the operational risk management office and internal audit.

The operational risk reports should contain internal financial, operational, and compliance data that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the bank on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures, and practices.

In general, the board of directors should receive sufficient higher-level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

6. Operational Risk Mitigation

Banks should have policies, processes, and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Control activities are designed to address the operational risks that a bank has identified. For all material operational risks that have been identified, the bank should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include, for example:

- top-level reviews of the bank's progress towards the stated objectives;
- auditing for compliance with management controls;
- policies, processes, and procedures concerning the review, treatment and resolution of non-compliance issues; and
- a system of documented approvals and authorizations to ensure accountability to an appropriate level of management.

Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and subject to careful independent monitoring and review.

In addition to segregation of duties, banks should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

- close monitoring of adherence to assigned risk limits or thresholds;
- maintaining safeguards for access to, and use of, bank assets and records;
- ensuring that staff have appropriate expertise and training;
- identifying business lines or products where returns appear to be out of line with reasonable expectations; and
- regular verification and reconciliation of transactions and accounts.

Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. Moreover, in many such instances, firms do not ensure that the risk management control infrastructure keeps pace with the growth in the business activity. A number of the most sizeable and highest-profile losses in recent years have taken place where one or more of these conditions existed. Therefore, it is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or program can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalize the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

However, banks should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place

to quickly recognize and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control (e.g., external events). Such problems may cause serious difficulties for banks and could jeopardize an institution's ability to conduct key business activities. As discussed below, banks should establish disaster recovery and business continuity plans that address this risk and comply fully with all agency rules, guidance and orders.

Banks should also establish policies for managing the risks associated with outsourcing activities, doing so in full compliance with all applicable agency rules, guidance, and orders. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialized business activities. However, a bank's use of third parties does not diminish the responsibility of management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services.

Depending on the scale and nature of the activity, banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. Management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. The bank should pay particular attention to use of third-party vendors for critical activities.

In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organization and should be consistent with the bank's overall business strategy and appetite for risk.

7. Contingency Planning

Senior management should ensure compliance with all applicable agency rules, guidance and orders regarding contingency planning. Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfill some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banks establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

Banks should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banks should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption, including the construction of appropriate backup facilities.

Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the bank would be able to withstand high-severity risk.

IV. Allocation of Appropriate Economic Capital

To a large extent, a robust, diversified earnings stream is often the best protection against both expected and unexpected operational losses. While capital is important, it should only focus on unexpected loss. Expected losses should always be considered as an expense, and covered by revenue, earnings, or reserves. A banking organization's capital should reflect the perceived level of precision in the risk measures used, and the relative importance to the institution of the activities producing the risk. Capital adequacy should be assessed after evaluation of the sum total of an organization's activities, with appropriate adjustments made for risk correlations between activities and the benefit resulting from diversified lines of business that, in aggregate, reduce operational risk to the consolidated organization. Capital levels should also reflect that historical correlations among exposures can rapidly change.

Explicit goals for operational risk capitalization should be included in evaluation of capital adequacy. Goals may differ across institutions, which should evaluate whether their long-run capital targets might differ from short-run goals, based on current and planned changes in risk profiles and the recognition that accommodating new capital

needs can require significant lead time. The goals should be reviewed and approved by the board and implemented by senior management.

1. Assessing Conformity to the Institution's Stated Objectives

Both the target level and composition of capital, along with the process for setting and monitoring such targets, should be reviewed and approved periodically by the institution's board of directors.

2. Composition of Capital

Analysis of capital adequacy should couple a rigorous assessment of the particular measured and unmeasured risks faced by the institution with consideration of the capacity of the institution's paid-in equity and other capital instruments to absorb unexpected losses. Common equity (that is, common stock and surplus and retained earnings) should be the dominant component of a banking organization's capital structure.

Common equity allows an organization to absorb losses on an ongoing basis and is permanently available for this purpose. Further, this element of capital best allows organizations to conserve resources when they are under stress because it provides full discretion as to the amount and timing of dividends and other distributions. Consequently, common equity is the basis on which most market judgements of capital adequacy are made.

Consideration of the capacity of an institution's capital structure to absorb unexpected losses should also take into account how that structure could be affected by changes in the institution's performance, or by the outside economic environment. For example, an institution experiencing a net operating loss - perhaps due to realization of unexpected losses - not only will face a reduction in its retained earnings, but also possible constraints on its access to capital markets. Other issues may arise in relation to use of optionality in its capital structure. Such adverse magnification effects could be further accentuated should adverse events take place at critical junctures for raising or maintaining capital, for example, as limited-life capital instruments are approaching maturity or as new capital instruments are being issued.

3. Examiner Review of Internal Capital Adequacy Analysis

As part of the regular supervisory and examination process, examiners should review internal capital assessment processes at large and complex banking organizations as well as the adequacy of their capital and their compliance with regulatory standards. In general, this review should assess the degree to which an institution has in place, or is making progress toward implementing, a sound internal process to assess capital adequacy. Examiners should briefly describe in the examination report the approach and internal processes used by the institution to assess its capital adequacy with respect to the risks it takes. Examiners should then document their evaluation of the adequacy and appropriateness of these processes for the risk profile of the institution, along with their

assessment of the quality and timing of the institution's plans to develop and enhance its processes for evaluating capital adequacy with respect to risk.

In all cases, the findings of this review should be considered in determining the institution's supervisory rating for management. Examiners should expect complex institutions to have sound internal processes for assessing capital adequacy in place.

Beyond its consideration in evaluating management, over time this review should also become an integral element of assessing, and assigning a supervisory rating for capital adequacy as the institution develops appropriate processes for establishing capital targets and analyzing its capital adequacy as described above. If these internal assessments suggest that capital levels appear to be insufficient to support the risks taken by the institution, examiners should note this finding in examination and inspection reports, discuss plans for correcting this insufficiency with the institution's directors and management and, as appropriate, initiate follow-up supervisory actions.

4. Relating Capital to the Level of Operational Risk

Banking organizations should be able to demonstrate through internal analysis that their capital levels and composition are adequate to support the risks they face and that these levels are properly monitored by senior management and reviewed by directors. Examiners should review this analysis, including the target levels of capital chosen, to determine whether it is sufficiently comprehensive and relevant to the current operating environment. Examiners should also consider the extent to which the institution has provided for unexpected events in setting its capital levels. In this connection, the analysis should cover a sufficiently wide range of external conditions and scenarios, and the sophistication of techniques used should be commensurate with the institution's activities. Finally, supervisors should consider the quality of the institution's management information reporting and systems, the manner in which business risks and activities are aggregated, and management's record in responding to emerging or changing risks.

As a final matter, in performing this review, supervisors and examiners should be careful to distinguish between a comprehensive process that seeks to identify an institution's capital requirements on the basis of measured economic risk, and one that focuses only narrowly on the calculation and use of allocated capital or "economic value added" (EVA) for individual products or business lines for internal profitability analysis. This latter approach, which measures the amount by which operations or projects return more or less than their cost of capital, can be important to an organization in targeting activities for future growth or cutbacks. It requires, however, that the organization first determine - by various methods - the amount of capital necessary for each area of risk. It is that process for determining the necessary capital that is the topic of this guidance, and it should not be confused with related efforts of management to measure relative returns of the firm or of individual business lines, given an amount of capital already invested or allocated. Moreover, such EVA approaches often are unable to meaningfully aggregate

the allocated capital across business lines as a tool for evaluating the institution's overall capital adequacy.

Financial Guardian Group

900 Seventeenth Street, N.W., Suite 506
Washington, D.C. 20006
Phone: (202) 296-5240
Fax: (202) 452-6816

Karen Shaw Petrou
Executive Director

February 2, 2004

Mr. Roger Ferguson
Board of Governors of
the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551

Mr. Donald Powell
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Mr. Jerry Hawke
Office of the Comptroller of the Currency
250 E Street, S.W.
Washington, D.C. 20219

Mr. James Gilleran
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

RE: Suggested disclosure requirements for operational risk in a Pillar 2 environment

Dear Sirs:

The Financial Guardian Group was pleased in our comments on the advance notice of proposed rulemaking regarding Basel implementation (68 Fed Reg 45,900) to include a suggested Pillar 2 approach to operational risk. Since then, questions have arisen about how disclosures would accompany this approach. In this supplement to our comment, we would like to suggest specific disclosures that would promote the comparability goals of the Pillar 1 operational risk-based capital proposal without the rest of the adverse and perverse consequences discussed in the comment letter. It is assumed that, in such an environment, Pillar 1 would continue to govern both credit and market risk, Pillar 2 would govern supervisory oversight, including dimensioning operational risk and related capital requirements, and that Pillar 3 would govern disclosure requirements. We address below what we feel would be appropriate operational risk and capital disclosures.

Within a Pillar 2 operational risk approach, we favor inclusion of those elements discussed in the Federal Reserves Supervisory Release 99-18. At a high level, each institution must have processes to address the “Fundamental Elements of a Sound Internal Capital Adequacy Analysis.” This would require institutions meaningfully to tie the identification, monitoring and evaluation of risk to the determination of the institution’s capital needs. To support that evaluation, an institution would have to have in place processes to support:

- Identifying and measuring all material risks;
- Relating capital to the level of risk;
- Stating explicit capital adequacy goals with respect to risk; and
- Assessing conformity to the institution's stated objectives.

As in our proposed Pillar 2 approach and SR 99-18, this would be the cornerstone of each institution's process to work with regulators to define an appropriate capital level.

The public disclosures related to this system would address each of these points, and the activities the institution undertakes to accomplish them.

Institutions would discuss as relevant:

(a) A description of the bank’s operational risk management function, which could include discussion of:
- Corporate governance;
- Independence of the risk management function;
- The design and implementation of the operational risk management framework, including the use of risk policies;
- Risk identification, measurement and control methodologies;
- Risk-reporting systems for operational risk; and
- Strategies to identify, measure, monitor and control/mitigate operational risk.

(b) Required reviews of the operational risk management processes and measurement systems by internal staff, auditors and external auditors. This review includes both the activities of the business units and of the independent operational risk management function.

(c) How validation of the operational risk measurement system occurs.

(d) The role and use of internal and external data, scenario analysis, and event analysis in the institution’s operational risk management function.

(e) How the institution evaluates exposure to low-frequency, high-severity events.

(f) The institution’s methods for the review/consideration of business environment and internal control factors potentially impacting the firm’s operational risk profile.

(g) Steps taken by the institution to mitigate risk in daily business processes, including the use of insurance.

(h) Techniques for the calculation and allocation of economic risk capital across all risk types, including the role of operational risk capital allocation in the bank’s management process and the interaction of operational risk capital with capital allocated for other risk categories.

Thank you for the opportunity to comment on Operational Risk disclosures in a Pillar 2 environment. We would be pleased to discuss this further and assist in the development of a specific proposal for inclusion in the next notice of proposed rulemaking in the United States on Basel and in the final version of the Basel rules. We believe strongly that all of these rules would be significantly improved with a Pillar 2 approach to ORBC, eliminating the current proposal for Pillar 1 requirements, with these expanded disclosure standards ensuring that Pillar 2 is a strong bulwark against this important source of financial risk at banks and their parent companies.

Sincerely,

Karen Shaw Petrou
Executive Director

Cc: Mr. Roger Cole
Federal Reserve Board

Mr. Edward Ettin
Federal Reserve Board

Mr. Richard Spillenkothen
Federal Reserve Board

Mr. Kevin Bailey
Office of the Comptroller of the Currency

Mr. Tommy Snow
Office of the Comptroller of the Currency

Mr. Michael Zamorski
Federal Deposit Insurance Corporation

Mr. Richard Riccobono
Office of Thrift Supervision