May 31, 2001

Comments on Consultative Document, Operational Risk

A Private Research Group for Financial IT Risk in Tokyo

A. Our Understanding of the Document

We highly appreciated this document on operational risk, which was previously addressed as a part of other (unmeasured) risk. It is focused and it promotes further discussions regarding both the rational operational risk assessment approaches and the schemes of capital charge based on operational risk.

We assume that capital charge will be calculated by weighting the RPI (Risk Profile Index) initially determined by the financial supervision authorities and this approach will be used by each bank as part of its self-risk assessment control in the future.

We understand that there are various issues such as the building of the risk database, testing the validity of these approaches, and reaching a final consensus among the members to be resolved through more discussions.

We believe that it is time to commence discussion on the Pillar 2, the required conditions for the new internal control and risk management. The discussions will not only lead to practical definition of operational risk and capital charge (the Pillar 1) but also address the various required specific conditions necessary for appropriate operational risk management. These conditions should be disclosed and implemented as soon as possible to improve the risk management, even before the validity of the approaches for capital charge is established. This will accelerate the implementation of the Pillar 3 (detailed information disclosure about the process used to manage and control the operational risk and the regulatory capital allocation technique used) for market discipline.

B. Our Comments

We would like to take this opportunity to make three comments on the specification of loss types and on the detailed guidance on loss categorization and allocation of losses by risk type:

1. Maturity level of the IT risk control;
2. Management level of the catastrophe risk control; and
3. Risk monitoring function of external audit.

We hope that these comments will assist in the future discussions leading to refined definition of operational risk and capital charge.

1. Maturity level of the IT risk control

a. Discussion

We agree that “a rigorous control environment is essential to prudent management of, and limiting of exposure to, operational risk “ and “supervisors should also apply qualitative judgments based on their assessment of the adequacy of the control environment in each institution” as described as the Pillar 2 in the section III.

Paragraph 53 further describes:

“The qualitative judgments by supervisors in the Pillar 1 operational risk framework increase the relative importance of the supervisory assessments of a bank’s strategies, policies, practices and procedure contemplated under Pillar 2. This independent evaluation of operational risk by supervisors should incorporate a review of the followings:

- The bank’s particular capital framework for determining its Pillar 1 operational risk capital charge;
- The bank’s process for assessing overall capital adequacy for operational risk in relation to its risk profile and its internal capital targets;

- The effectiveness of the bank's risk management process with respect to operational risk exposures;
- The bank's system for monitoring and reporting operational risk exposures and other data quality considerations;
- The bank's procedure for the timely and effective resolution of operational risk exposures and events;
- The bank's process of internal controls, reviews and audit to ensure the integrity of overall operational risk management process; and
- The effectiveness of the bank's operational risk migration efforts."

We believe that some quantitative indicators should be set up to promote uniform acceptance and to reduce the possibility of arbitrary judgments.
Especially, as IT plays an integral part of in the business risk control by providing information and communication elements of internal control framework, it is necessary to define quantitative indicators for the IT risks as soon as possible.
The provision of the loss database system that is consistent with the operational risk framework is indispensably required for effective risk management and risk control, as described in the section VII. IT should provide these capabilities.

b. Recommendation
Information Systems Audit and Control Association, which provide leading edge products in IT control field, has established a management guideline of IT. This guideline provides management maturity level over IT internal control, and has been benchmarking the level of each enterprise by the industry. This benchmark could provide global standard control level indicators for the financial institution.
We also think it desirable that these indicators get a position equal to the RPI, or get a position as a part of the RPI.
In this guideline the level is divide into six classes from 0 to 5 similar to the Capability Maturity Model that Carnegie Mellon University proposed for the maturity of the software development management. The level interpretation for 34 IT resource process in for domain of actives- planning and organization, acquisition and implementation, deliver and services and monitoring are provided (See Annex I for more details).
The level is classified as:

0: Non-existent; Complete lack of any recognizable processes.
1: Ad hoc; There are no standardized control processes but ad hoc approaches.
2: Repeatable; Similar control procedures are followed by different people undertaking the same task.
3: Defined Process; Procedures have been standardized and documented. But it is left to the individual to follow these processes.
4: Managed and Measurable; Processes are under constant improvement and provide good practice.
5: Optimized; Processes have been refined to a level of best practice.

2. Management level of the catastrophe risk control

a. Discussion
Financial institutions have set up a management control structure for on-going monitoring of quality, cost and speed of operation using performance indicator such as interest profit rate, number of trouble-operation, the income and costs by the customer, etc. We believe that the level of this on-going risk monitoring capabilities directly affect the weighting factor of the RPI (Risk Profile Index) of the financial institutions comparing with an industry wide loss distribution.
However, another measurement should be established for catastrophe risk management where major concern is insolvency or survival of operation when a mega-catastrophe would take place once in several decades. These risks will not be identified nor monitored through on-going monitoring process.
The management decision is made on more strategic and long life cycle perspective.

We believe that catastrophe risk also should be considered as operation risk and included as a part of the risks to be measured for capital charge. This catastrophe risk could not be easily estimated based on loss database accumulated by business line and loss types. The actual past experience may not provide sufficient information of the losses for each business lines or each loss type even if accumulated on the industry wide bases as the frequency of the occurrence is very limited. Rather catastrophe risk has a tendency for more wide range impact over cross industries mixing different business lines and loss types.

We believe a uniform knowledge mangement model for catastrophe risk management should be established for scenario formation of exposure of various catastrophe risks. These bases have been considered as risk control environment/tone of at the top and not focused as detailed information disclosure about the process used to manage and control the operational risk. These information should be classified and disclosed in the Pillar 3.

b. Recommendations.

We recommend that a uniform knowledge management model be established for internal control over catastrophe risk management for the Pillar 2.

A knowledge management process are normally consists of:

- Information gathering
- Organizing information and knowledge
- Refining information and knowledge
- Dissemination information and knowledge

Scenario database should be provided for:

- Knowledge map/category
- Taxonomy
- Thesaurus

An illustrated example of catastrophe risk profile analysis and measurement procedures are described in the Annex II.

3. Risk monitoring function of external audit

a. Discussion.

We believe that independent assurance reviews carried out at regular interval could be considered to provide the basis on the fairness and soundness of the effectiveness of the operational risk monitoring process of the financial organizations.

We understand that there are various issues to be resolved to obtain the effectiveness of audit performance in this area and there is the need to identify the criteria for the judgment of the appropriateness of the risk measurements process or effectives of the risk monitoring process of the organizations.

We know that the needs to enhance the knowledge base for the benchmarking of internal control assessment against similar organizations or appropriate international standards/recognized industry best practices.

Auditors may understand that organization-wide risk management policies and procedures relating to risk control planning, managing, monitoring and reporting on the internal controls.

Auditors review IT policies and procedures relating to monitoring and reporting on internal controls.

By reporting on the operational risk management activities including IT risk control activities and maturity level of the IT risk control, we expect that such audit would contribute to the accelerate the implementation process of the operational risk management in financial institutions.

b. Recommendation

We believe that independent assurance reviews for the area of the effectiveness of the operational risk monitoring and evaluation of the maturity level of the IT risk control carried out by external auditors at regular intervals would support the financial institution managements' commitment to

monitoring internal controls. Further, the effectiveness of internal controls should be reviewed by external auditors in order to establish the independence and impartiality of the review from the management of the organizations as a strong monitoring process. This will also assist the supervisory review process in the Pillar 2.
We understand that further discussion would take into consideration about the following issues.

The needs of independent certifications and accreditation
The approach of independent effectiveness evaluations
The requirements of independent assurance of compliance with laws and regulatory requirements
Independent assurance of compliance with contractual commitments
Qualification requirements in order to maintain uniform quality of assurance in this area.
The cycle of audit involvement.

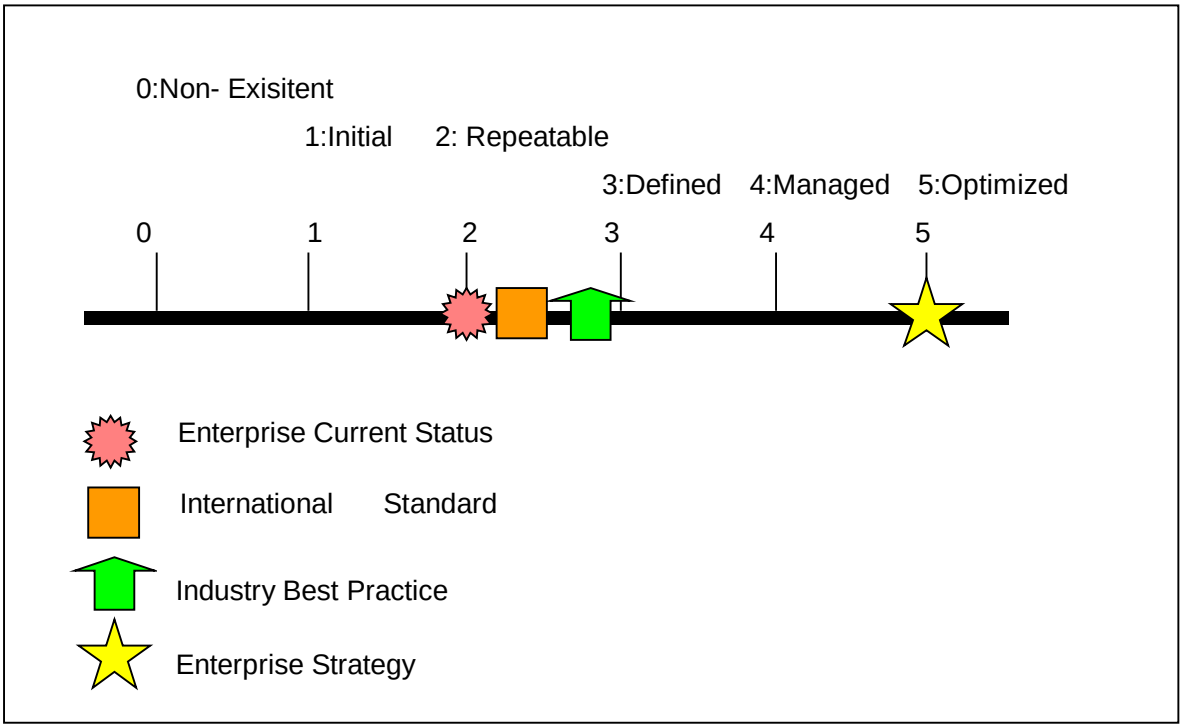
Member list (Alphabetical order)

Negawa ,Tadamichi The Tokio Marine And Fire Insurance Co., Ltd.
Suzuki ,Osamu The Tokio Marine And Fire Insurance Co., Ltd
Takahashi ,Hidetoshi The Tokio Marine And Fire Insurance Co., Ltd
Tsuge ,Masafumi The Tokio Marine And Fire Insurance Co., Ltd
Hakkaku ,Takao Tokio Marine Risk Consulting., Co.Ltd
Yanagihara ,Toshiro PricewaterhouseCoopers
Endo , Makoto PricewaterhouseCoopers
Kimura , Akinori PricewaterhouseCoopers
Maeda ,Nobuo PricewaterhouseCoopers
Matsuo ,Akira PricewaterhouseCoopers
Toyama, Maurice PricewaterhouseCoopers
And other 5 members

Annex . ISACA Maturity Model

MATURITY MODELS for control over IT processes consist of developing a method of scoring so that an organization can grade itself from non-existent to optimized (from 0 to 5). This approach has been derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability(2). Against these levels, developed for each of CobiT's 34 IT processes, management can map:

The current status of the organization - where the organization is today
The current status of (best-in-class in) the industry - the comparison
The current status of international standards - additional comparison
The organization's strategy for improvement - where the organization wants to be



The following table is a list of Cobit 34 IT processes.

Planning and Organization

PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage Human Resources
PO8	Ensure Compliance with External Requirements
PO9	Assess Risks
PO10	Manage Projects
PO11	Manage Quality

Acquisition and Implementation

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Develop and Maintain Procedures
AI5	Install and Accredit Systems
AI6	Manage Changes

Delivery and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-Party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Assist and Advise Customers
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
DS11	Manage Data
DS12	Manage Facilities
DS13	Manage Operations

Monitoring

M1	Monitor the Processes
M2	Assess Internal Control Adequacy
M3	Obtain Independent Assurance
M4	Provide for Independent Audit

For each of the 34 IT processes, there is an incremental measurement scale, based on a rating of "0" through "5." The scale is associated with generic qualitative maturity model descriptions ranging from "Non Existent" to "Optimized" as follows:

0 Non-Existent. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is

disorganised.

2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.

3 Defined. Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

The following pages provide PO1 Maturity Model, for the example.

Control over the IT process Define a Strategic IT Plan with the business goal of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

0: IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals

1: The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organisation-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2: IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organization strategy. The risks and user benefits of major strategic decisions are being recognized, but their definition is intuitive.

3: A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process and there are no procedures to examine the process on a regular basis. The overall IT strategy includes a consistent definition of risks that the organization is willing to take as an innovator or follower. The IT financial, technical and

human resources strategies increasingly drive the acquisition of new products and technologies.

4: IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior level responsibilities. With respect to the IT strategic planning process, management is able to monitor it, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisation-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

5: IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernable business value through investments in IT. Risk and value added considerations are continuously updated in the IT strategic planning process. There is an IT strategic planning function that is integral to the business planning function. Realistic long-range IT plans are developed and constantly being updated to reflect changing technology and business-related developments. Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated, as changes occur. Benchmarking against well-understood and reliable industry norms is a well-defined process and is integrated with the strategy formulation process. The IT organisation identifies and leverages new technology developments to drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Annex II An Example of Catastrophe Risk Management Model

A. Risk Profile Analysis.

The following process is followed to assess the risk profile of the financial institution . (About once a year).

1.Information gathering about the risk

The past incident and its impact in our organization and industry.

Potential risk consideration based on its own business environment and internal business process, with system technologies.

2.Business impact analysis is roughly done in order to estimate the order of the amount of damages with the several typical scenarios classified by the event and/or by the impact.

3.The critical risks which can not be left from the viewpoint of going-concern are recognised by management based on the above analysis result with a forecast on the PML (probable maximum loss) in the present conditions.

B. Scenario for Measurement.

A measure against the critical risk is planned in the following process.

1.As for the critical risk, a detailed scenario analysis is done. On the other hand, the validity of the measure is reviewed with the technique such as a time series analysis and the additional conditions (worse conditions or available internal and external support)

2.The investigation on the effect of the measure which will become a risk management control or a change control on the business procedures, implementation costs, period for preparation is done and reviewed.

3.The best combination is chosen from the various countermeasures. And risk reduction effect (especially, the effect of the forecast on the maximum amount of damages base) is estimated precisely.

C . Monitoring

1.As for the countermeasure to the important risk, a promotion procedure, project management organization and project owner is defined.

2.As a mechanism which ensures a self-assessment, internal and external audits are established to monitor the effectiveness and consistency with the organization policy.

The statutory auditor, or the external auditor commissioned by management initiates and controls this mechanism.