Key Points of Scenario Analysis

Takashi Arai
Director
Center for Advanced Financial Technology,
Financial Systems and Bank Examination Department,
Bank of Japan

July 18, 2006

1. Scenario Analysis

■Tasks

- Identification of key risks on bank's business
  - —— Forward-looking point of view
  - —— "Ex post analysis" (data collection of incidents, accidents, operational errors, etc.) vs. "Ex ante analysis" (scenario analysis)

■Objectives

- Assessment of risks across a bank (→improve risk management when necessary)
- Operational risk quantification
  - —— A type of input data for operational risk quantification model
    - cf. Internal loss data, external data, business environment, internal control factors

■Process of scenario analysis

(1) Basic plan

- Scenario extraction (“brainstorm”)

  e.g. Disasters (earthquakes, typhoons, peculiar risks in specified regions—radioactive leaks from nuclear power plants, droughts), serious frauds, (embezzlements, illegal remittances), operational errors, large-scale IT system troubles, leaks of customer information, asbestos problems

- Impact analysis assuming scenarios become reality

  e.g. Earthquake: Cost of removal and restoration of damaged buildings and equipment, personnel expenses, lost profit during operation outage

  Large-scale IT system trouble: Recovery cost, personnel expenses, lost profit during operation outage, cost of sending apology letters to clients

- Comparison with net worth of the bank

  The bank can conclude that “Even a large earthquake would not affect our bank’s capital adequacy” can be made.

(2) Advanced plan

- Review of a bank's risk management to lessen the impact of problems or reduce the possibility of their occurrence

  e.g. Earthquake: Quake-resistance structure, quake insurance

  Fraud: Various check systems

  Lawsuit arising from trouble with client: Tighter checks on contracts, and proposal documents with/for clients

  System trouble: Improvement of system quality, shorter operation outage through improvement of business continuity plan

  Labor-related trouble: Correction of unpaid overtime work, setup of a contact point for workers on

  abuse of power and sexual harassment

- Utilization as input data for the operation risk quantification model

  ――Various ideas about the range of scenario data for the model

  e.g. "All scenario data," "high severity scenario data only"

  "scenario data for range of lacking internal losses only"

2. Scenario Extraction

(1) Method

a. Bottom-up approach

■ Each department sets its own scenario through comprehensive analysis of operational errors and accidents, internal control condition, business environment, etc.

——Unfamiliarity with cases of scenario analysis by each domestic branch (as there is not much difference in operation profiles among domestic branches)

——Business line headquarters which are responsible for each business: (retail banking, private banking, corporate market, investment banking, including operating units) makes scenarios including risks associated with each domestic branch

——Management discussion of each department on whether all possible major risks have been identified

- “Middle” section (risk management section, etc.) reviews scenarios set by each department from a point of view of checking clear irregularities

  Motives of each department

  a) “Honest” analysis of scenario often means confession of weakness of risk control and may draw stricter checks from the head office.

  → Preference for less strict scenario

  b) Presentation of all possible risks, whether they are worth calling “risks”, in order to get much budget and workforce by pretending needs for enhancing risk management.

  → Preference for stricter scenario

- Different approaches by departments or people in charge
  - －－ Different sensitivity or tolerance to risks and different philosophy on risk management
- Inclusion of external cases especially overseas ones and cases associated with risks which are newly discussed among people
  - －－ Enhancing compliance and risk control based on revisions of the securities exchange law (Financial Instruments and Exchange Law), enforcement of the Private Information Protection Law, etc.

b. Top-down approach

■ Generation of “key scenarios” that reflect the senior management policies and direction of business strategies

－－ A scenario based on senior management view is not necessarily equivalent to a scenario generated at each department

－－ A senior management is responsible for top-down scenarios. But it might be also okay for senior management to instruct the planning /corporate risk management section or others to produce a draft of top-down scenarios as long as senior management are responsible for them

－－ The number of top-down scenarios may be controlled so that senior management can review each scenario efficiently

■Samples of top-down scenarios

——Not only in the operational risk area but also in the business risk area

・Failure in M&A, new business

・Negative impact on own reputation due to improper conduct by group companies and associates

・Failure in the large-scale development of a large-scale system

・Improper conduct by executive directors

■Samples of firm-wide scenarios associated with common risk factors

・Major disasters (earthquakes, terrorist attacks, etc.)

—— It is usually more efficient if the head office (risk management section) sets a premise for the likely frequency of earthquakes and other disasters

・Information leaks, violation of compliance, etc.

—— There should often be more effective cases where middle section in charge of customer information control and compliance on firm-wide level sets basic patterns of scenarios

(2) Possible events

- Area of operational risks
  - ・Natural disasters (earthquakes, typhoons, tsunamis, lightning strikes)
  - ・Man-made disasters (terrorist attacks, radiation leaks from nuclear power plants)
  - ・Damage to real estate properties, equipments (caused by inadequate structural calculation with fake quake resistance data, faulty construction, soil contamination, asbestos)
  - ・Frauds of employees (embezzlement from client's account, inappropriate mediation of loan, illegal remittance)
  - ・Operational errors (remittance error, cash losses, leaks of client information)
  - ・External frauds (attack on cash delivery vehicle, ATM destruction outside of the branch)
  - ・System trouble (system breakdown, double remittance)
  - ・Trouble with clients and counterparties (inadequate risk explanation to client, obscure articles in a contract)
  - ・Violations of laws (violation of antimonopoly law, securities exchange law, unpaid overtime work, illegal labor practice)

- Boundary of operational risk and business risk
  ——Business risks outside the range of Basel II-Pillar I
  ・Failure in system development such as cancellation due to change in business environment
  ・Cancellation of a joint project with clients and associates
  ・Loss from the failure of new business as a result despite very careful due diligence
- Scenarios can also include credit risks, market risks, and liquidity risks
  ——Example: Big earthquake
    → business deterioration of the borrowers
    → aggravating credit cost

3. Estimating frequency, and severity

(1) Frequency

- Natural disasters (earthquakes, floods, etc.)

—— Use statistics released to the public

- Others

—— Dependent on experts' judgment to some degree

(2) Severity

- Direct losses

・Financial loss caused by crimes such as embezzlement

—— Based on average / maximum account of settlement transactions

・Penalty, charge, heavy additional tax

——Based on judicial precedents, publicly disclosed examples

・Damage to real estate properties (building, equipment)

——Book value / reminder price or replacement cost

➢ Indirect losses

- Personnel cost for handling problems
  - ——Regular or overtime payment for the time of handling them
- Cost for lawyers, apology advertisements, gifts for clients
- Opportunity cost that could have been made
  - ——Fee discount, loss of clients to other banks

    e.g.: Opportunity cost can be simply calculated as follows:

    “planned profit per day” multiplied by “number of affected days”

4. Challanges

(1) Appropriateness of scenarios

■ Estimate future risk → Difficulty in obtaining “exact” estimates

Not easy to judge the appropriateness of scenario even if it is based on objective data. God only knows future.

→ Need to rely, to some degree, on “subjective” experts’ judgment

→ All the same, such “subjective judgment” must be persuasive

- Judgment based on opinions of several people /organization, not of single person
- Need to work out a scenario based on “objective” data—own past cases or other banks’ / firms’ examples
- Need to document a series of scenario generating processes, in order to clarify who is involved and how the judgment is made

cf. Idea: “judgment based on due process is justifiable.”

■ Validation and Check

——Validation by middle section

——Check by internal audit including check on scenario production process itself

cf. Who validates / checks top-down scenarios made by the management?

(2) Burden of scenario production

■Consider burden of scenario analysis in each department

——Desirable number of scenarios varies depending on the size and profile of a financial institution

■ Principle of materiality

——The bigger the impact of a scenario (tail scenario) for the bank's business, the more intensively it should be analyzed, validated and checked

- Anyone who wishes to transfer or make a copy of the contents of this material is requested to contact the Center for Advanced Financial Technology, Financial Systems and Banking Examination Department, Bank of Japan in advance for permission.
- All efforts are made to ensure the accuracy of the information in this material, but the Bank of Japan under no condition will be held responsible for any actions using information taken from this material.