Combining Internal Loss Data, Scorecards and Scenario Analysis

Presentation for RMG Conference
May 30, 2003
Final version 1.0

Kenji Fujii

Risk Management Department

UFJ Holdings, Inc.

Outline of presentation

- Objectives of presentation
- Introduction: Operational risk management initiative at UFJ Group
- Overview of UFJ operational risk management approach
- UFJ operational risk measurement approach
  - Qualitative assessment – Scorecard analysis
  - Scenario generation
  - Internal loss data
  - Risk model - Quantitative measurement
- Risk reports
- UFJ operational risk management approach – risk mitigation actions
- UFJ approach – preliminary self-assessment

Objectives of presentation

- To provide a case study for combination of qualitative assessment, scenarios, and internal loss data
  - Why does qualitative assessment provide solid ground for the scenario analysis
  - How is qualitative assessment effectively designed
  - How is a scenario-based AMA implemented in practice
- To provide a case study of how risk management framework is used to reduce operational risk exposure

*In developing our operational risk management approach, UFJ have emphasized the integration of qualitative assessment, scenario-analysis, and internal loss data in a single framework. In particular, we have conducted comprehensive **qualitative assessment** as a base work for the overall framework. Also, our implementation will indicate a case study of how a **scenario-based AMA** ("**sbAMA**") is implemented in practice. Our presentation consists of the following two main topics.*

** **UFJ operational risk measurement approach***

** **Integration of the measurement to operational risk management** and risk mitigation actions.*

Introduction: What is UFJ Group?

- Established in 2001, unifying the operations of the former Sanwa, Tokai and Toyo Trust
- As of 2002/3;
  - * Total Combined Asset: US$593Bil
  - * Total Shareholders's Equity: US$21Bil
- UFJ Bank is an internationally active bank with worldwide network

Introduction:

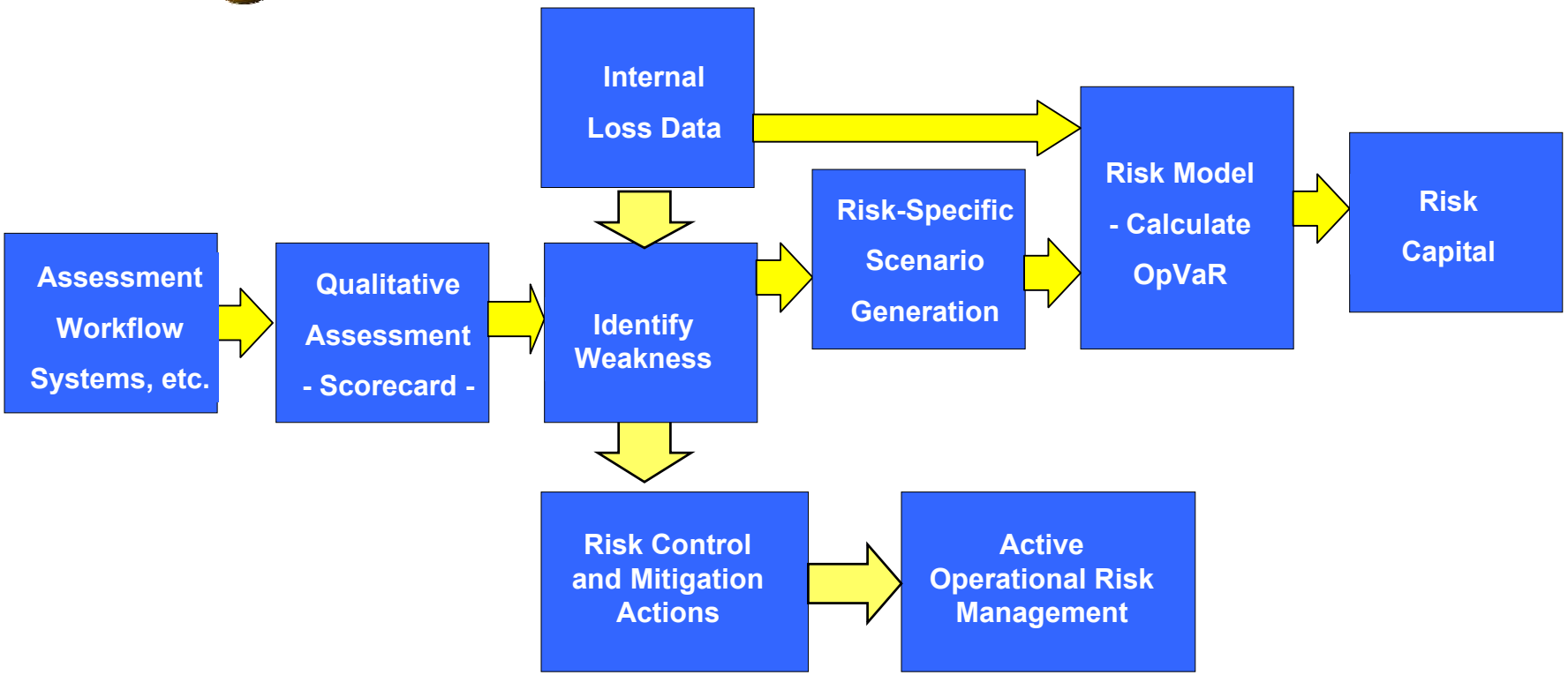
Operational risk management initiative at UFJ

UFJ		BIS Initiative	
Dec-98	* Sanwa started risk quantification project for processing risk and system risk	Jun-99	* Capital charge for other risks (including 'operational risk') proposed under "Basle CP1"
Apr-00	* Operational Risk Project Team formed at Sanwa		
Oct-00	* Operational Risk Desk established at Risk Management Dept of Sanwa * Aiming at scenario-centered approach		
		Jan-01	* Capital charge for operational risk proposed under "Basle CP2"
Apr-01	* UFJ Holdings established, Operational Risk Desk transferred enabling groupwide approach		
	* Risk Management Policies on operational risk sub-categories (IT Systems, Processes, etc.) approved by the board of UFJH and each subsidiary bank		
	*OpVaR calculated and Operational Risk Capital introduced	Sep-01	"Working Paper on the Regulatory Treatment of Operational Risk" published
		Feb-03	"Sound Practices for the Management and Supervision of Operational Risk" published
Mar-03	* Comprehensive Operational Risk Management Policy approved by the board of UFJH and each subsidiary bank		

UFJ Group has started to apply "modern" operational risk management approach in 2000, echoing the initiative shown in the CP1 in 1999. Our framework has consistently focused on integration of proactive risk management actions and risk control activities.

UFJ operational risk management approach

Overview



UFJ' overall operational risk management approach is summarized as above.

Please note this process shares a lot of essence with that of Scenario-based AMA approach. Thus, UFJ's approach will be categorized as a Scenario-based AMA.

UFJ operational risk management approach

- **Combination of qualitative assessment, scenario analysis, and quantitative measurement**
  - **Comprehensive and extensive use of qualitative assessment throughout the organization**
  - **Full utilization of scenarios**
- **Emphasis on the seamless link between risk measurement process and risk management actions**
- **Applying risk management cycle which combines bottom-up and top-down approach**

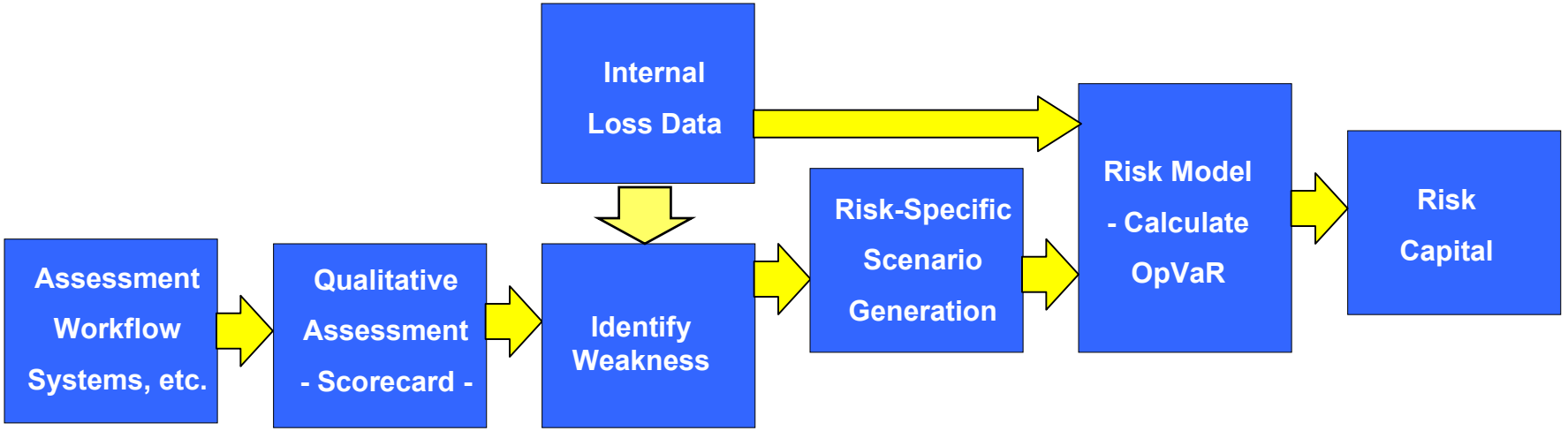
  [Bottom-up approach]: Quantitative risk measurement to calculate risk capital

  [Top-down approach]: Risk capital allocation, based on the measurement result

UFJ' operational risk management approach can be characterized as above. The key features comes from ***comprehensive qualitative assessment****, possibly called as "scorecards," and* ***reliance of scenarios****, which plays the central role of the framework.* ***Internal loss data*** *are also included in the risk model.*

UFJ operational risk measurement approach

Overview

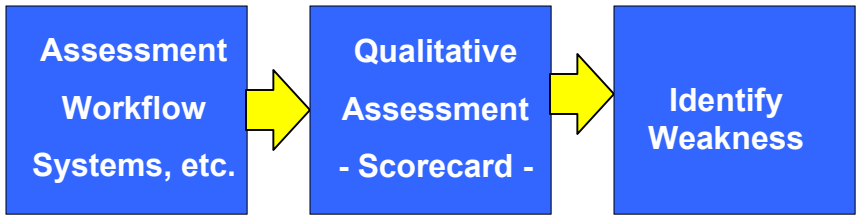


*This is the **UFJ's operational risk measurement workflow**, part of the overall approach in the previous slide. The uniqueness lies in our comprehensive use of qualitative assessment of each work process, system, etc.*

We identify operational weaknesses by the assessment and generate scenarios for the weaker operations. Risk model to calculate risk capital is loaded with scenario losses and internal operational loss data.

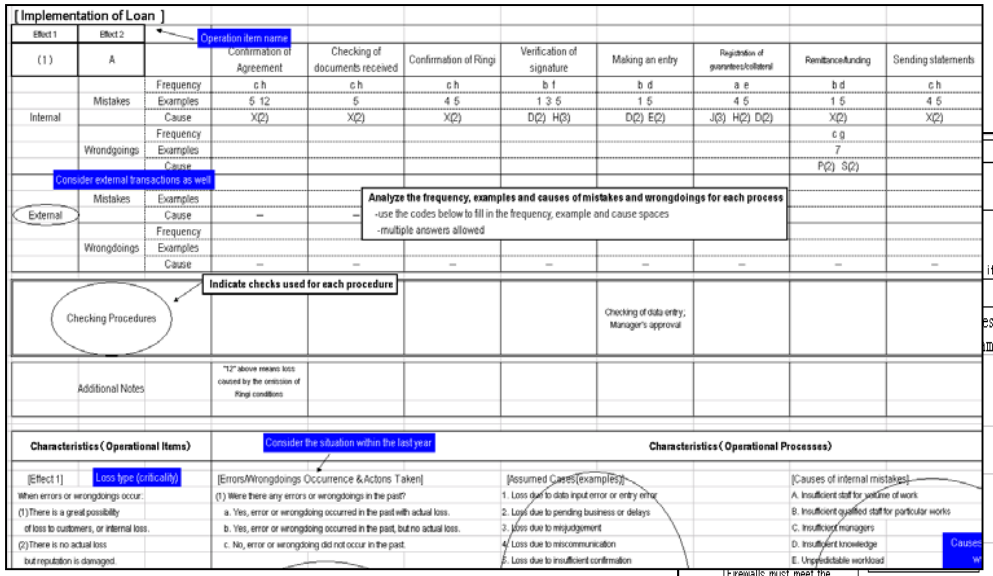
In the following, we will explain our practices, taking examples of processing risk and system risk.

Qualitative assessment – "Scorecards"



- Qualitative assessment for every material process/system throughout the group
  - Approximately six thousand pieces of assessment for processing (2002)
  - Five hundred for systems (2002)
- Group-wide standard assessment format
- Standard assessment keys to evaluate control level and to identify control weakness
  - 20 keys for processing
  - 180 keys for system
- Assessment of the current (and planned, if applicable) process flows/systems
  - Proactive management and accommodation to change of business environment
- A "score" attached to each assessment key
- Scoring of assessment result by the summing the scores for the identified keys
- Higher-scored processes/systems eligible for scenario generation

Qualitative assessment - format


[Implementation of Loan]

Operation item name

Effect 1 | Effect 2 | (1) | A

		Confirmation of Agreement	Checking of documents received	Confirmation of Ringi	Verification of signature	Making an entry	Registration of guarantees/collateral	Remittance/funding	Sending statements
Internal	Mistakes Frequency	c h	c h	c h	b f	b d	a e	b d	c h
	Mistakes Examples	5 12	5	4 5	1 3 5	1 5	4 5	1 5	4 5
	Mistakes Cause	X(2)	X(2)	X(2)	D(2) H(3)	D(2) E(2)	J(3) H(2) D(2)	X(2)	X(2)
	Wrongdoings Frequency							c g	
	Wrongdoings Examples							7	
	Wrongdoings Cause							P(2) S(2)	
External	Mistakes Examples								
	Mistakes Cause	–	–						
	Wrongdoings Frequency								
	Wrongdoings Examples								
	Wrongdoings Cause	–	–	–	–	–	–	–	–

Consider external transactions as well

Analyze the frequency, examples and causes of mistakes and wrongdoings for each process
-use the codes below to fill in the frequency, example and cause spaces
-multiple answers allowed

Indicate checks used for each procedure

Checking Procedures: Checking of data entry; Manager's approval

Additional Notes: "12" above means loss caused by the omission of Ringi conditions

Characteristics (Operational Items) | Consider the situation within the last year | Characteristics (Operational Processes)

[Effect 1] Loss type (criticality)
When errors or wrongdoings occur:
(1) There is a great possibility of loss to customers, or internal loss.
(2) There is no actual loss but reputation is damaged

[Errors/Wrongdoings Occurrence & Actons Taken]
(1) Were there any errors or wrongdoings in the past?
a. Yes, error or wrongdoing occurred in the past with actual loss.
b. Yes, error or wrongdoing occurred in the past, but no actual loss.
c. No, error or wrongdoing did not occur in the past.

[Assumed Cases (examples)]
1. Loss due to data input error or entry error
2. Loss due to pending business or delays
3. Loss due to misjudgment
4. Loss due to miscommunication
5. Loss due to insufficient confirmation

[Causes of internal mistakes]
A. Insufficient staff for volume of work
B. Insufficient qualified staff for particular works
C. Insufficient managers
D. Insufficient knowledge
E. Unpredictable workload

Table of Operation Process

(Processing Risk)

System Risk Evaluation Sheet

(IT System Risk)

Supervisor

Evaluate each circled line item, based on system characteristics (below)
DEV: internally developed (or purchased) and used systems ranked A or B in ledger system importance
ORD: using above ranking, systems whose development and/or maintenance was ordered from other firms
OUT: using above ranking, development outsourced systems (in use by other firms)
INF: systems or PCs maintaining customer or corporate data privacy, ranked C in importance

items	DEV	ORD	OUT	INF	N/A	R	present status
ess mming	○			○		1	Universal protocols (TCP/IP, etc.) are not used. When they are used, a firewall is in place, with the use of multiple defensive functions (packet filtering, application gateways, etc.) relevant to the importance of the business being handled, and with regular reviews of the strength of the system.
						2	When using universal protocols, the firewall is set to simplified functioning (packet filtering).
						3	No firewall is in place, but there is a division between the LAN having outside access and the strictly internal-use LAN. The LAN with outside access maintains no important functions or data.
						4	Universal protocols are used on dedicated lines, or the party with whom the connection is made uses only specified public lines.
infrastructure						5	No firewall is in place and no strategies, as outlined above, are used.
Firewalls must meet the following requirements: * response for hacks (high traffic attacks) * packet filtering (mimic strategy) * application gateway (business-related e-	Monitoring for Inappropriate Access Status 7.1.2(1)⑤	○			○		1 Constant supervision for inappropriate access from outside sources is accomplished with monitoring software and/or the review of access logs.
infrastructure						2・3	Nearly as indicated above, with room for improvement in operations.
						4・5	No monitoring implemented.

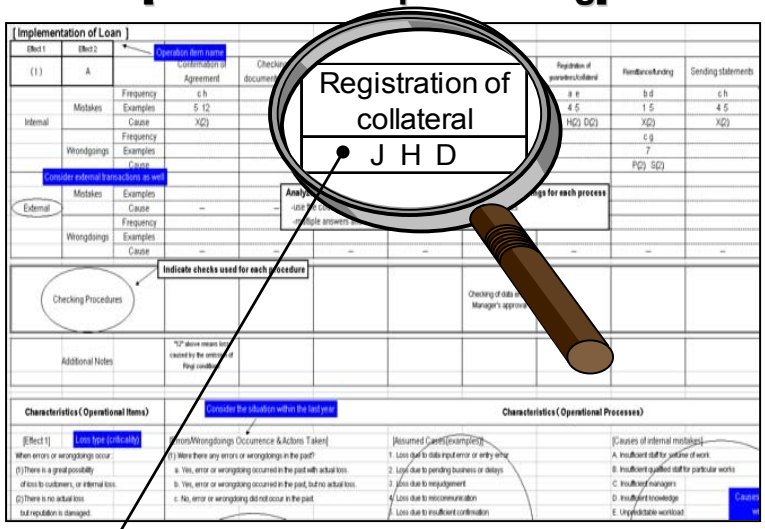
Qualitative assessment is made, using group-wide forms. In processing and systems risk, we use;

- *Table of Operation Process (processing risk)*
- *System Risk Evaluation Sheet (system risk)*
- *Threat Handling Table (system risk)*

Qualitative assessment

Examples of assessment keys and scoring

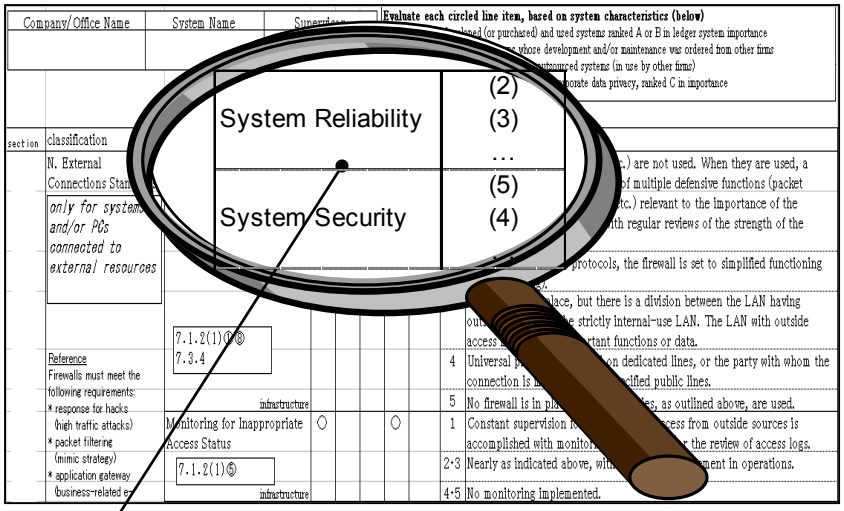
[Ex. ABC loan processing]



Assessment Keys : Causes		Score
J	No System Support	0.30
H	No Standardised documents	0.25
D	Insufficient Knowledge	0.17
…	…	…
…	…	…
Total Score of "Loan" Process		1.50

Approx. 20 keys

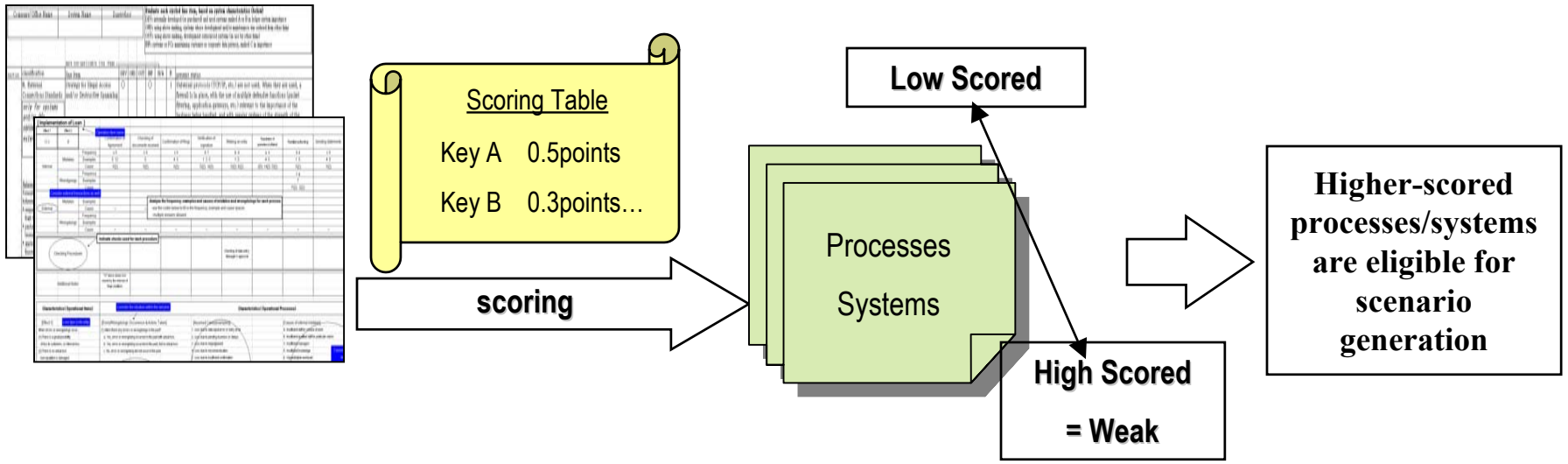
[Ex.XYZ business system]



Assessment Keys	Score
System Reliability	15
(2)Backup measures are taken but there is business restriction during backup	2
…	…
System Security	23
(5)No firewall is in place and no strategies	5
…	…
Total Score of XYZ System	38

Approx. 180 keys

Qualitative assessment - summary



This is the summary of the qualitative assessment part of the risk measurement process

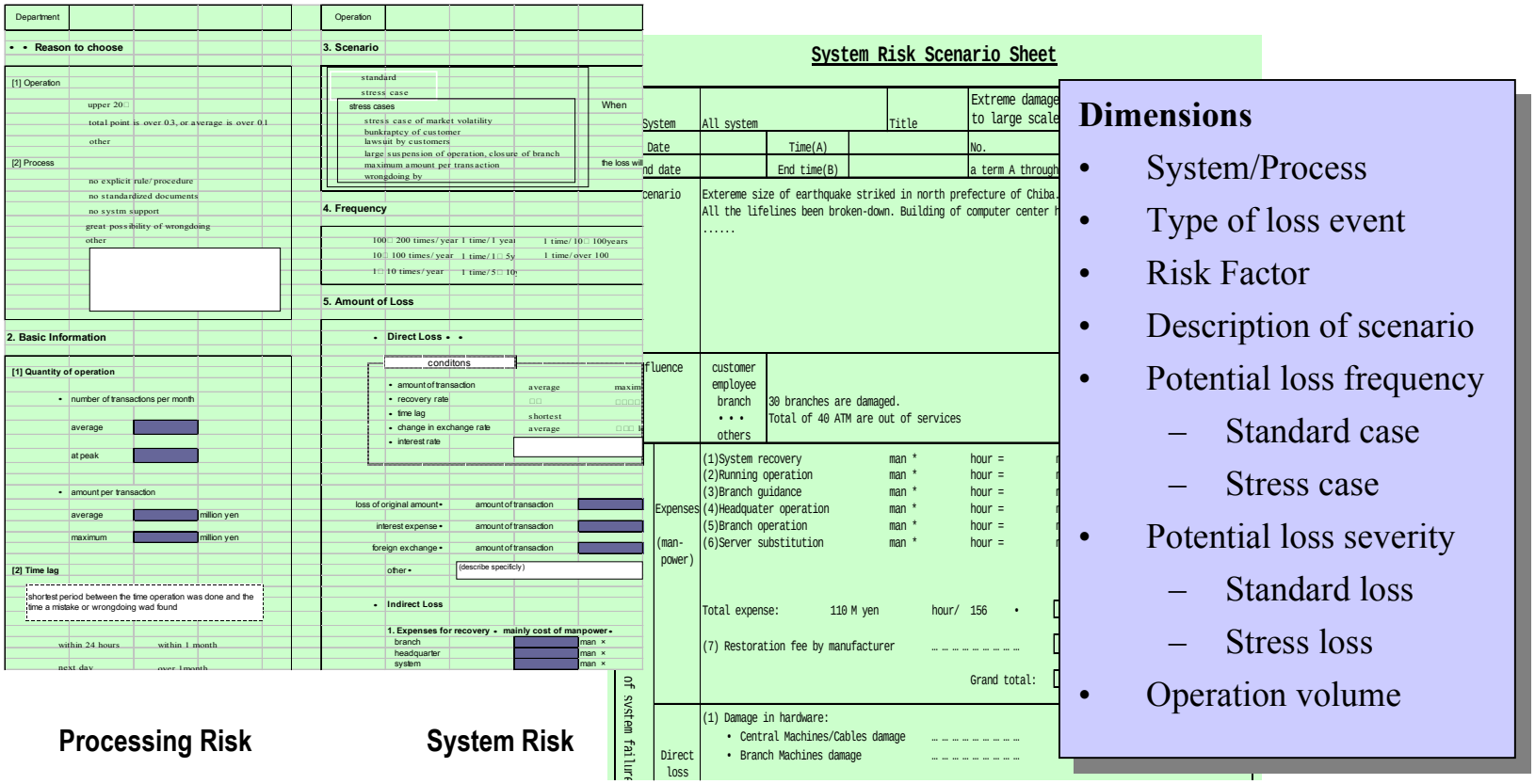
** Our approach, with the comprehensive coverage of operations, enables identification of control weaknesses in a consistent manner*

** Challenges exist in its workload as well as assurance of assessment quality,*

Scenario generation

- Operational loss "**generic scenarios**" and "**stress scenarios**" generated for the processes/systems with higher scores.
  - Each scenario includes estimated operational risk loss amount (severity) and frequency.
    - Generic Scenarios include tail-event losses as well as expected/unexpected losses
    - Stress scenarios indicate catastrophic loss
- Group-wide scenario generation format
- Scenarios generated by the same business experts, who completed the qualitative assessment
- Verification by risk management departments under "reasonableness check"

Scenario generation - format



Dimensions

- System/Process
- Type of loss event
- Risk Factor
- Description of scenario
- Potential loss frequency
  - Standard case
  - Stress case
- Potential loss severity
  - Standard loss
  - Stress loss
- Operation volume

Scenarios are generated, using group-wide forms. Business experts determines the individual scenarios, which cover the necessary measurement dimensions.

Example of scenario generation

Result of qualitative assessment

[Case] ABC loan processing

[Assessment result]

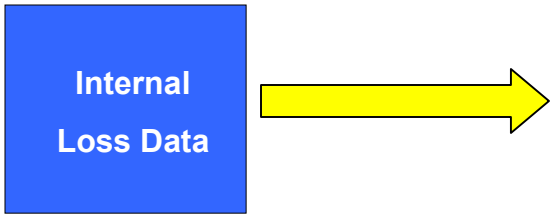
- The weakest step among the processing flow is "registration of collateral" because it has no system support, no standardized documents.
- There has been one error recorded (but no financial loss) in this operation in the last five years.
- Operation volume is approximately 5,000 trades/year with the average amount of JPY10 million.

Generated Scenario – generic scenario

Risk Factor:	Processing risk
Loss Event:	Transaction capture, Execution & Maintenance / Collateral management failure
Description of scenario:	Due to **an insufficient system support and complicated documents**, a staff **forgets to register the collateral of loan**. As a result, the bank cannot reimburse the loan from the collateral.
Loss Severity:	50 million yen (considering the analysis of ABC loan amount distribution)
Loss Frequency:	**once in five years** (considering the analysis of historical loss frequency)

*Scenarios are generated based on the result of the qualitative assessment. Factors such as **the identified control weakness, internal loss experience, business environment, and relevant industry loss experiences**, are taken into consideration in generating the scenario. Stress scenarios are created at the same time.*

Internal loss data



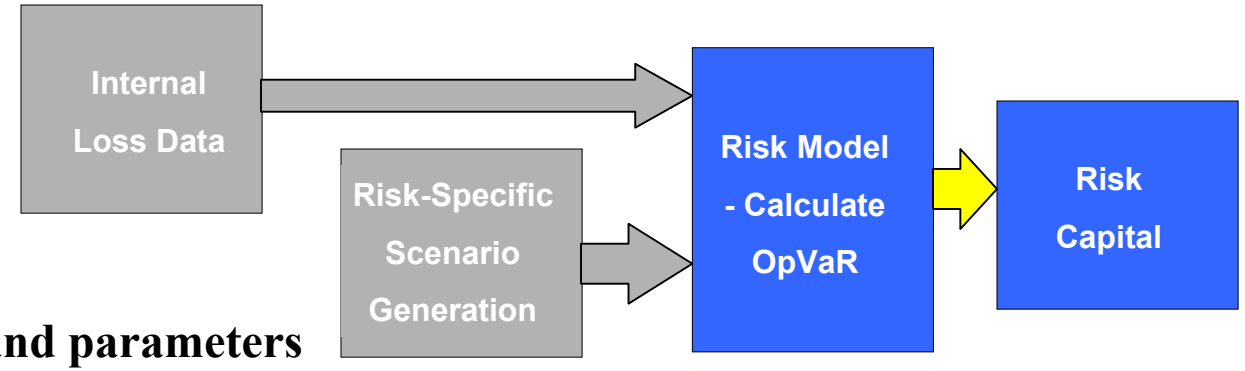
Internal loss data

Observation period:	Five years for system risk, three years for processing risk
Data threshold:	No threshold (all data with financial loss (from JPY1) collected)
Consolidation:	Covers material group companies on a consolidated basis
Loss Data Type:	Direct loss: payments to clients, accounting loss, penalty, etc.
	Indirect loss: recovery cost, overtime, opportunity income cost, etc.

*In addition to the scenario losses, **internal loss experiences** are also regarded core parts in our risk measurement framework.*

*Internal loss data have been collected based on the above specifications. **Not only direct losses but also indirect losses** are included as loss amount based on best estimate.*

Quantitative measurement



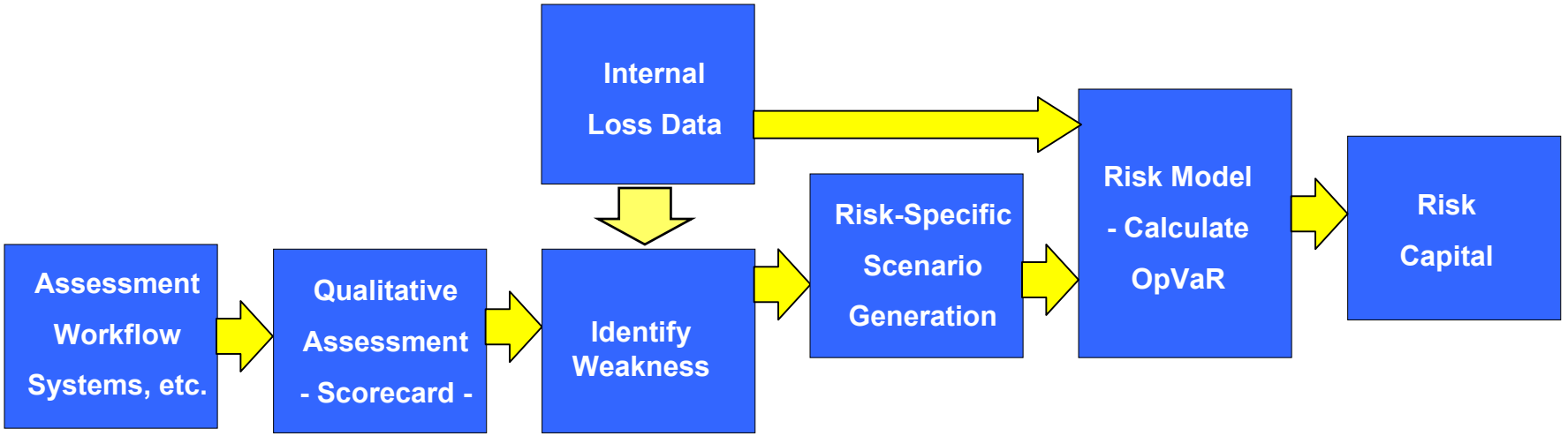
Risk model and parameters

Model Type:	analytical
Underlying Theory:	Panjer model
Confidence interval:	99% (one-tailed)
Holding period:	one year
Data:	Internal loss data and scenario loss data

*As for risk model, UFJ decided to apply **analytical model** after investigation between Monte Carlo simulation model and analytical model. Consideration has been taken in the stability for the calculation result. Internal loss data as well as scenario loss data are loaded into the model.*

*UFJ applies the model output, or operational risk amount, as group-wide **operational risk capital** in our **risk capital management framework**.*

Summary



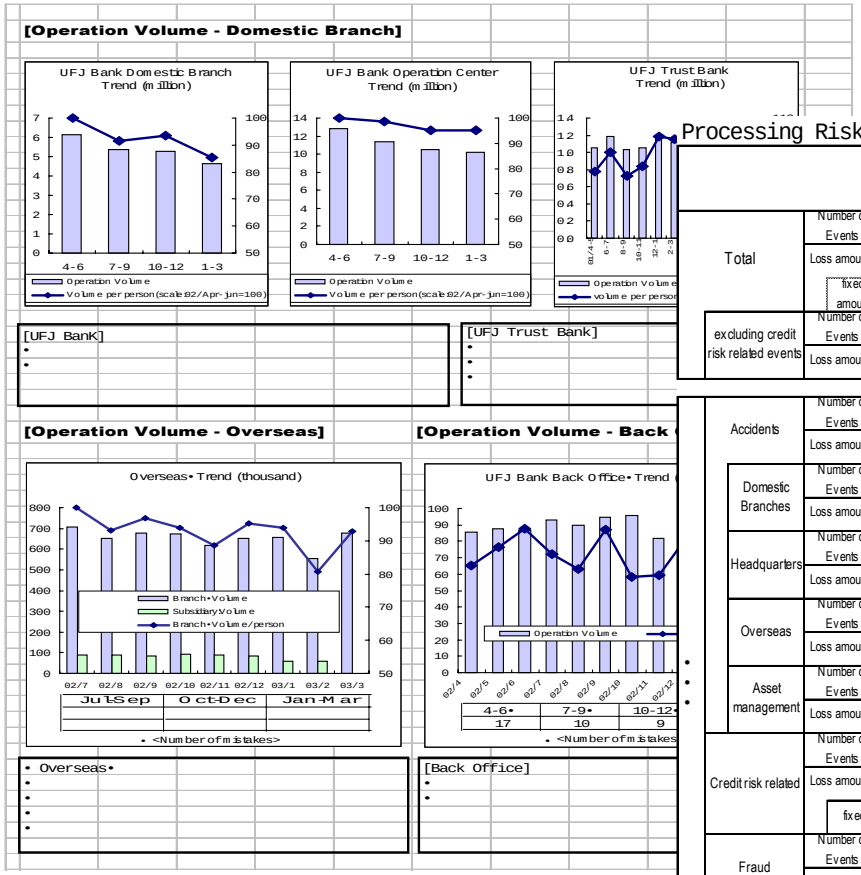
This concludes the process for the UFJ's operational risk measurement approach.

Risk reporting

- Quarterly operational risk report to the board of directors and group risk management committee
- Contents of the report:
  - Operational loss events with;
    - Loss amount
    - Number of events
  - Operational risk analysis with;
    - Summary analysis of qualitative assessment result
    - Quantitative measurement result – Operational risk amount
    - Key Risk Indicators

*Operational risk is reported to the board of directors and group risk management committee quarterly. The reports includes analysis of **operational loss events** for the previous quarters, together with the analysis of the **qualitative assessment**. Analysis on the performance of operational risk **Key Risk Indicators (KRI)** is also included in the report, intending to forecast the operational risk exposure in the near future, thus enabling proactive operational risk management actions.*

Operational risk report – layout (1)



KRI Analysis Report

Operational Loss Report

Processing Risk

		Group Total			UFJ Bank (*1)			UFJ Trust Bank		
		2002 Jul-Sep	Oct-Dec	2003 Jan-Mar	2002 Jul-Sep	Oct-Dec	2003 Jan-Mar	2002 Jul-Sep	Oct-Dec	2003 Jan-Mar
Total	Number of Events									
	Loss amounts									
	fixed amount									
excluding credit risk related events	Number of Events									
	Loss amounts									
Accidents	Number of Events									
	Loss amounts									
Domestic Branches	Number of Events									
	Loss amounts									
Headquarters	Number of Events									
	Loss amounts									
Overseas	Number of Events									
	Loss amounts									
Asset management	Number of Events				•	•	•			
	Loss amounts				•	•	•			
Credit risk related	Number of Events									
	Loss amounts									
	fixed									
Fraud	Number of Events									
	Loss amounts									
Criminal	Number of Events									
	Loss amounts									

Operational risk report – layout (2)

Risk Assessment Report (System Risk)

Result of System Risk Evaluation

Level of Importance	Risk Level	March 2002 System Department	Headquater	Overseas Branchs	Domestic Subsidiarie	Overseas Subsidiarie	Total	Mar.2001 Grand Total
A	Ex.Low	XX	X	X	X	X	0	XX
	Low	X	XX	X	XX	XX	0	XX
	Acceptable	X	X	X	X	X	0	XX
	High	X	X	X	X	X	0	X
	total	**XX**	**XX**	**X**	**XX**	**XX**	**0**	**XXX**
B	Ex.Low	X	XX	XX	X	X	0	XX
	Low	X	XX	X	XX	X	0	XX
	Acceptable	X	X	X	X	X	0	X
	High	X	X	X	X	X	0	X
C								
Grand Total								

Result of Evaluation by System

SYSTEM	Importance Level	Overall Risk Level	Reliability	Durability	Result
XXX	A	1	1	1	Extremely Small
XXXX	A	1	1	1	Extremely Small
XXX	A	1	1	1	Extremely Small
XXX XXXX	B	1	1	1	Extremely Small
XXXX	B	1	1	1	Extremely Small
XX XXX XXXX	C	1	-	1	Extremely Small
XXX	C	1	-	1	Extremely Small

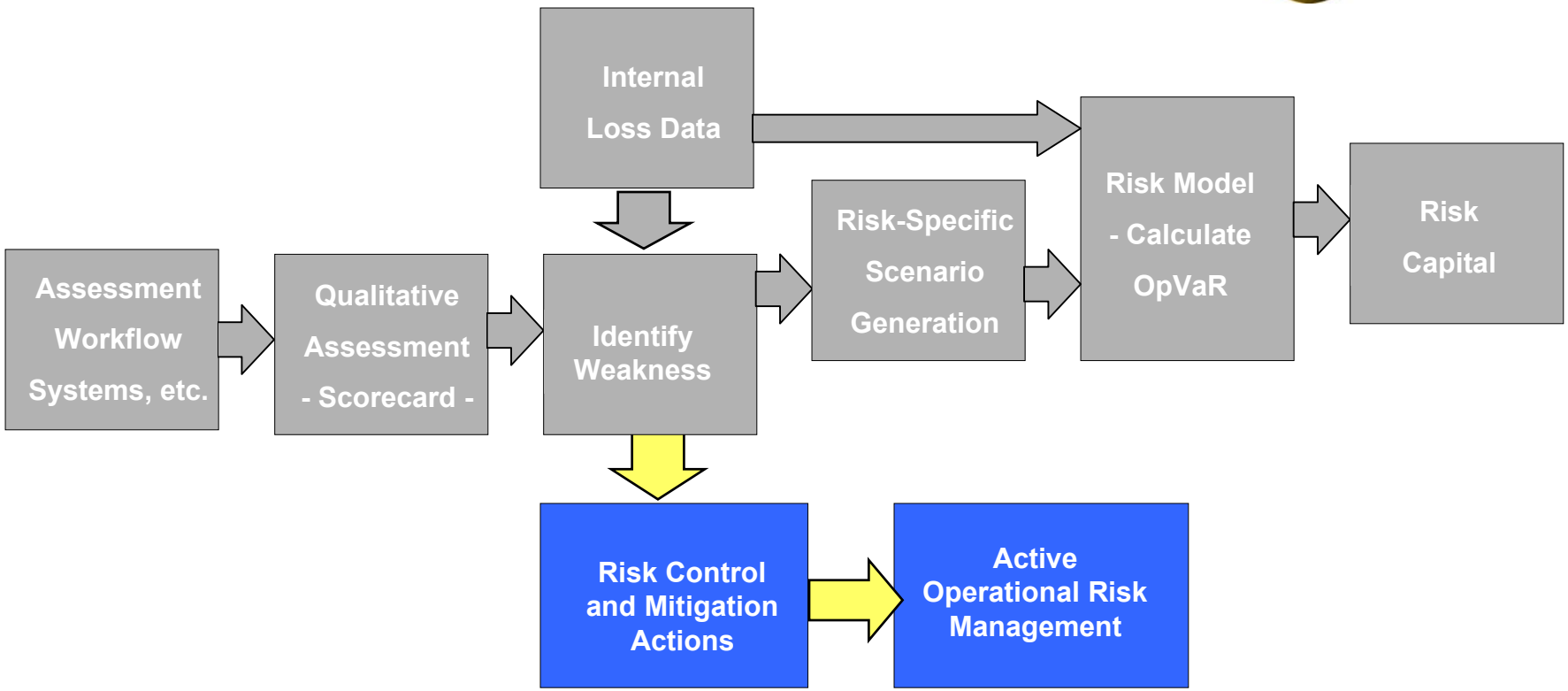
Durability = System durability against information bleach

SYSTEM	SCENARIO	Standard Frequency	Standard Severity	Stress Frequency	Stress Severity
1	Computer Center Breakdown by Earthquake	XX	XXXX	XXX	XXXX
2	"Online" Breakdown by Earthquake in Tokyo pref.	XX	XXXX	XX	XXXX
3	Earthquake in Osaka prefecture	XX	XXX	XX	XXXX
4	"Online" Breakdown in Osaka pref.	XX	XX	XX	XXX
5	Main Accounting System Breakdown	XX	XXX	XX	XXX
6	"Online" Breakdown in Nagoya pref.	XX	XXX	XX	XXX
7	"Banking Association Network" breakdown	XX	XX	XX	XXX
8	ATM theft	XX	XX	XX	XXX
9	Fraud (using forged Bankcard)	XX	XX	XX	XX
10	Miss Operation in Computer Center	XX	XX	XX	XX

h "C" then
then the results of evaluation

	Overseas Subsidiarie	Total	Mar.2001 Grand Total
%	97%	98%	96%

UFJ operational risk management approach



At UFJ, it is emphasized to utilize the qualitative assessment results to the operational risk control and mitigation actions. This ***operational risk management approach*** *concludes our overall approach.*

Once control weakness is identified through the qualitative assessment, we develop and apply ***risk control and mitigation actions*** *and improve the quality of the weak points. These actions include such actions as changing the procedure, process automation, upgrading or replacing system, etc.*

UFJ operational risk management approach

- Assignment of operational risk management departments in charge of operational risk sub-categories
- Responsibilities of the operational risk management departments
  - establishing policy and procedures for the relevant sub-category
  - day-to-day control activities of the sub-category
  - risk mitigation activities of the relevant sub-category

In order to promote this active operational risk management, UFJ Group has defined ***operational risk sub-categories*** *and assigns "****operational risk management departments****" in charge of each sub-category.*

Each department is responsible for planning risk management and control practice, establishing policy and procedures, day-to-day risk control activities, risk mitigation through change of procedures, etc., for the relevant sub-category.

Operational risk factor – Scenario classes

Risk sub-categories and departments in charge

Sub-Category		Definition	Department in charge
Operational Risk		Operational risk refers to the risk of losses resulting from inadequate or failed internal processes, people and systems, or from external events. Due to the different causes of operation lrisk, it is subdivided into the following sub-factors.	*Risk Management Dept.*
	Processing Risk	Processing risk refers to the risk of financial losses from failed processing due to mistakes, negligence, accident or fraud by directors, staff and other personnel within the organization.	*Systems & Operations Planning Dept.*
	System Risk	System risk refers to the risk of financial losses due to system and telecommunication failures, including temporary system shutdown, system malfunction, system hacking, and system disruption caused by external events.	*IT Dept.*
	Human Resources Risk	Human resources risk refers to the risk of financial losses due to loss of key personnel or failure to maintian staff morale.	*Human Resources Dept.*
	Tangible Asset Risk	Tangible asset risk refers to the risk of financial loss or damage to tabgible assets from such events as natural disasters or utility accidents.	*General Affairs Dept.*
	Regulatory Risk	Regulatory risk refers to the risk of financial losses due to the change of regulatory environment, including tax systems, accounting systems, or regulatory treatment.	*Risk Management Dept.*
	Reputational Risk	Reputational risk refers to the risk of financial losses from the adeverse impact on the group's reputation among customers or the market due to unfounded rumors.	*Corporate Communication Dept.*

The operational risk sub-category definitions and the assigned departments in charge are shown as above.

With regard to the relationship with the operational risk events defined in the BISII, we have assured that risk management by sub-categories covers all the operational risk events under BISII.

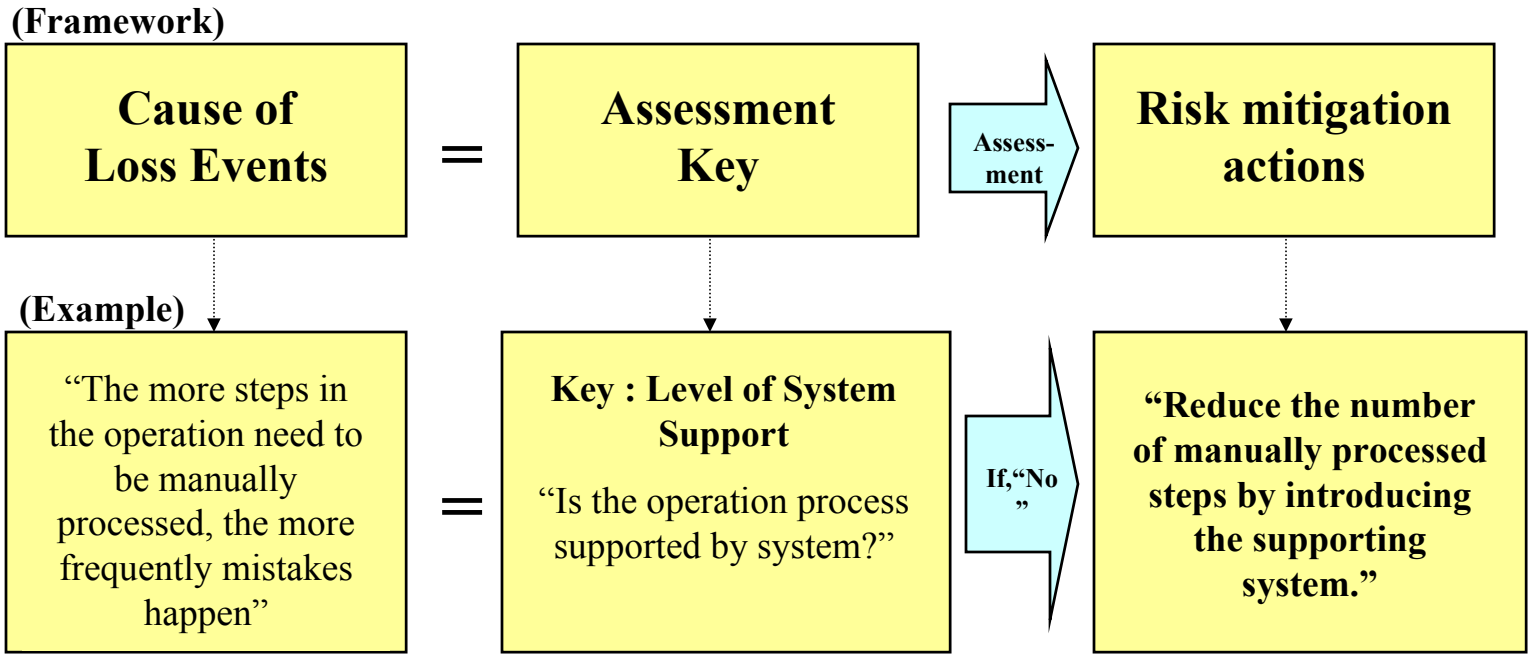
Operational risk factors – event mapping

Event-Type (Level 1)	Categories (Level 2)	Sub-category			
		Processing Risk	System Risk	Tangible Asset Risk	Human Resources Risk
Internal Fraud	Unauthorized Activity	X			X
	Theft and Fraud	X		X	X
External Fraud	Theft and Fraud	X		X	
	System Security	X	X		
Employment Practices and Workplace Safety	Employee Relations				X
	Safe Environment				X
	Diversity & Discrimination				X
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary	X			X
	Improper Business or Market Practices	X			X
	Product Flaws	X	X		X
	Selection, Sponsorship & Exposure	X	X		
	Advisory Activities				X
Damage to Physical Assets	Disasters and other events		X	X	
Business Disruption and System Failures	Systems		X		
Execution, Delivery & Process Management	Transaction, Capture, Execution & Maintenance	X	X		X
	Monitoring & Reporting	X			X
	Customer Intake and Documentation	X			X
	Customer/Client Account Management	X	X		
	Trade Counterparties	X	X		X
	Vendors & Suppliers	X	X		X

The above table is a high-level summary of mapping between event-type and sub-category.

Operational risk mitigation actions

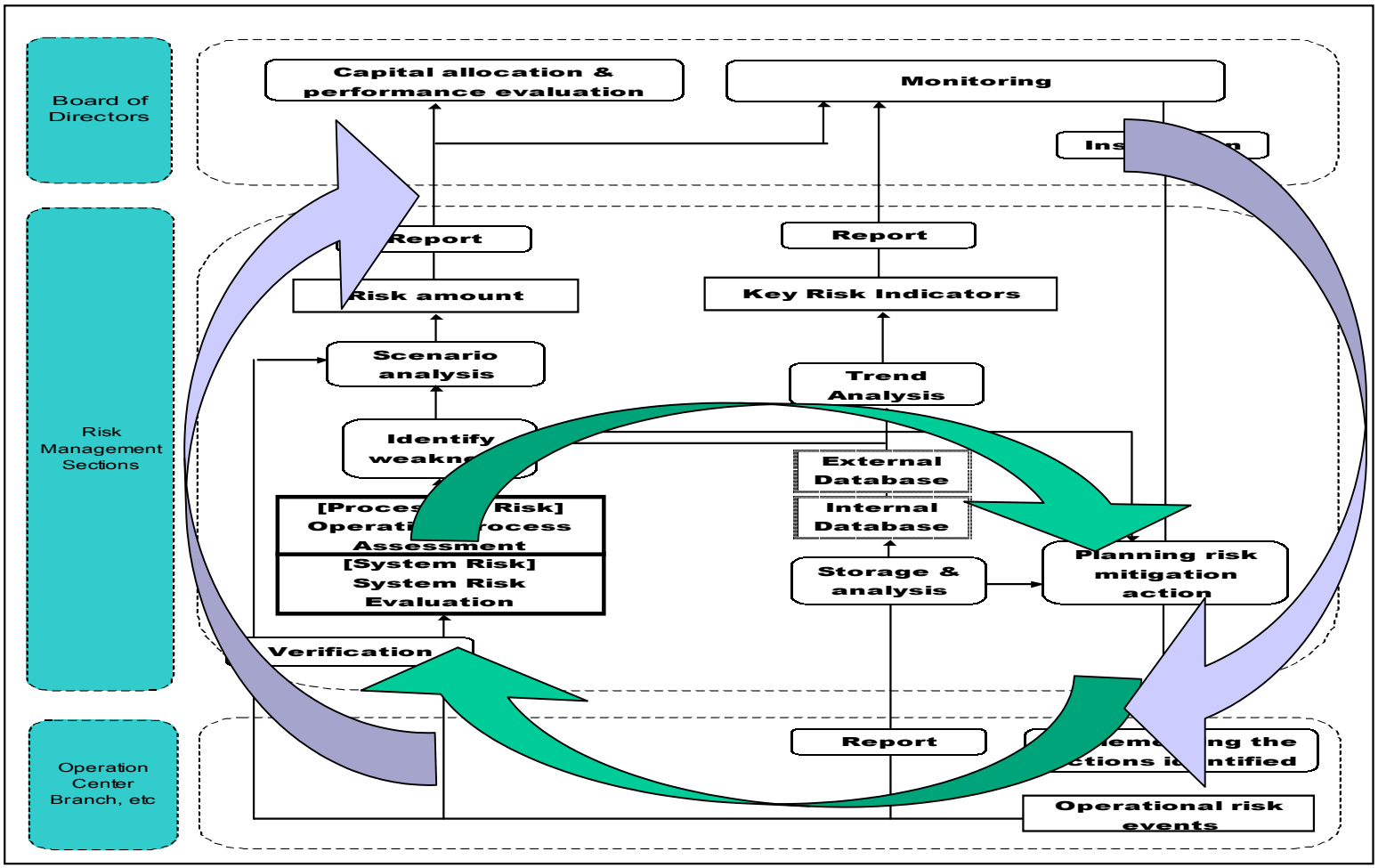
Risk mitigation actions determined through analysis of the identified assessment keys



Since risk assessment keys are arranged as closely linked to "causes" of operational loss events, analysis of the assessment keys identified helps formulation of the risk mitigation actions directly.

The qualitative assessment not only contribute to risk measurement but also helps to determine risk mitigating actions.

Risk management cycle



UFJ approach – use of the four key elements

- **Internal loss data**
  - *Collection of internal loss data with zero threshold by sub-categories within each business line, covering all the event-types*
  - *Material group company coverage*
- **External data**
  - *Relevant industry loss experience considered in scenario generation process*
- **Scenario analysis**
  - *Scenario analysis placed as the core of the framework, in addition to its supplementary role to loss data*
  - *Coverage of tail-end losses*
- **Business environment and internal control factors**
  - *Business environment and internal control factors fully considered in scenario generation process*

High level self-assessment of our approach in relation to the four key elements could be described as above.

UFJ approach as a scenario-based AMA

- Scenario analysis as a core of the framework
- At UFJ approach,
  - Scenario classes similar to other sbAMA
  - More detailed organizational parts, or individual process, system, etc., applied
    - more scenarios than typical sbAMA
    - accordingly, no assumption on severity distribution and parameters
  - Direct use of internal loss data into the risk model
    - similarity with LDA approach

UFJ 's approach will be categorized as a scenario-based AMA ("sbAMA"), with its emphasis on the use of scenarios at its central role of the framework. As a variation of sbAMA, UFJ's approach might be unique in the much more detailed organizational parts into individual process, system, etc., within the sbAMA's scenario class and organizational part concept. Also, as the internal loss data are directly included in the risk model, our approach might be viewed as carrying similar features of LDA approach.

Preliminary SWOT analysis

- **Strengths**
  - **Extensive group-wide qualitative assessment in practice, which provides consistent analysis with scenario generation process and operational risk identification**
  - **Close link of risk measurement and risk mitigation actions in a single framework**

- **Weaknesses**
  - Significant workload required to maintain and update qualitative assessment and scenarios, including verification process
  - Third party review, including internal audit, necessary

- **Opportunities**
  - Utilization of the qualitative assessment methodology for group-wide internal control benchmark

- **Threats**
  - Mechanical mass-production of undigested scenarios
  - Loss of assessment and scenario quality

Challenges ahead

- Improving the quality of scenarios to;
  - reflect operational risk exposure more properly
  - certain operational risk subcategories
- Utilization of internal loss data to “back-test” qualitative assessment and scenarios
- System development to process loss data and scenarios
- Effective utilization of Key Risk Indicators
  - to enable proactive operational risk management
  - verification of hypothesis provided by KRIs
- Introduction of a third party review of the framework
  - including review of measurement result
- Satisfaction of AMA qualifying criteria

Contact

- Kenji Fujii, Deputy General Manager,
  Risk Management Dept., UFJ Holdings, Inc.
  k_fujii@ufj.co.jp or
  kenji.fujii.wg87@wharton.upenn.edu
- Takayuki Ishida, Manager, Risk Management Dept.,
  UFJ Holdings, Inc.
  takayuki_isida@ufj.co.jp
- Daisuke Fujita, Manager, Risk Management Dept.,
  UFJ Holdings, Inc.
  daisuke_fujita@ufj.co.jp