Scenario-based AMA

Presentation for RMG-Conference 29./30. May 2003
May 2003 (final version 1.0)

The following banks have contributed to the content and drafting of the presentation. Such contributions do not imply that the institutions will implement the approach set out in the paper, but rather that they believe a Scenario-based AMA is conceptually sound and, if implemented with integrity, should be recognised as qualifying for AMA status. The views expressed do not necessarily reflect the overall view of each individual institution.

Banca Intesa
Barclays Bank
Credit Suisse First Boston
Dresdner Bank
Fortis Bank
Halifax Bank of Scotland
Lloyds TSB
The Royal Bank of Scotland Group
UFJ Holdings, Inc
Euroclear

Outline of presentation

- Objectives of presentation
- Introduction
- Overview of concept
- **How to determine appropriate scenarios for OR?**
- **How to ensure that scenarios are consistent, relevant and capture all material OR?**
- **How to evaluate scenarios in an organisation?**
- **How to use scenarios for modelling purposes?**
- Why a scenario based AMA improves OR management (example application)
- Key benefits of a scenario based AMA
- How other building blocks link into a scenario based AMA
- Overlap / similarities with LDA / Scorecard
- Illustrations

Objectives of the presentation

- To demonstrate that a scenario based approach is conceptually sound
- To define the key features of implemented scenario-based AMA approaches
- To prove that a scenario based approach is a valuable basis for managing risks
- To indicate that banks are fairly aligned in terms of thinking about scenarios
- To describe how scenarios can form an integral part of economic and regulatory capital calculations
- To illustrate how scenarios can be constructed in the most useful way

Executive Summary

A scenario based AMA

- is focused on a forward looking assessment of the key operational risks in an organisation taking into account both the internal control environment and external threats
- is an approach that employs the technique of individual scenario evaluation in a similar fashion to market and credit risk
- is based on all available information (expert experience, internal / external losses, KRIs, quality of control environment)
- leads via a model to a sound economic capital number that helps to incentivise prudent and pro-active OR management
- bridges the gap between LDA and Scorecard approach
  (or at least has a considerable overlap with each)
- has been or is being successfully implemented in a number of international banks

Introduction

- Scenarios are defined as potential events (i.e. events that could happen in the future).
- Risk is inextricably linked to the evaluation of „what-if“ certain scenarios occur. The evaluation process involves providing answers to two fundamental questions:
  - How likely are certain scenarios to happen?
  - How severe could their impact be?
- Scenarios are already an important technique in the evaluation of market and credit risk as illustrated in the following questions:
  - *What is the impact if the yield curve shifts by 20bp? How likely is this?*
  - *What is the impact if this customer defaults? How likely is this?*
- Scenarios are also an essential component in the assessment of operational risks and determination of capital.

Overview of concept

Scenario Generation

How to determine appropriate scenarios for OR?

Scenario Assessment

How to evaluate scenarios in an organisation?

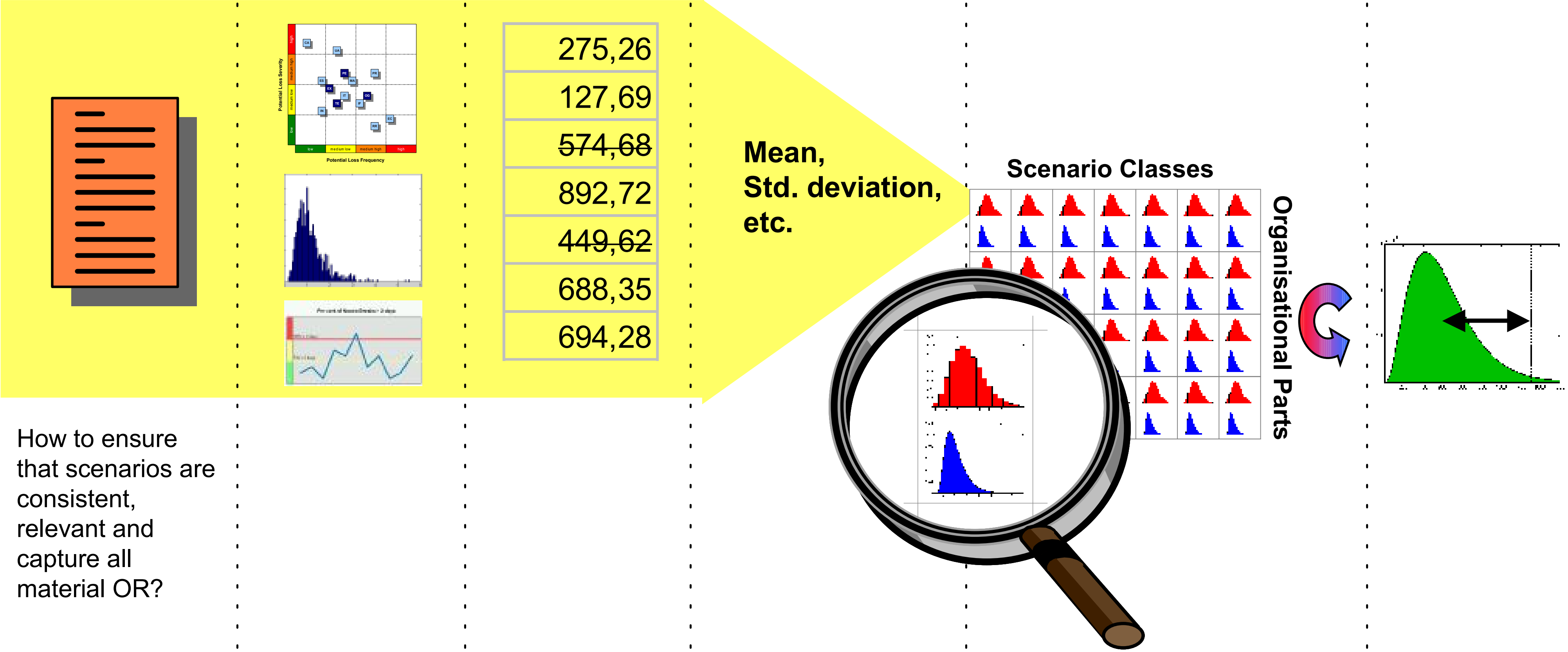
Data Quality

Determination of Parameter Values

Model & Parameters

How to use scenarios for modelling purposes?

Model Output

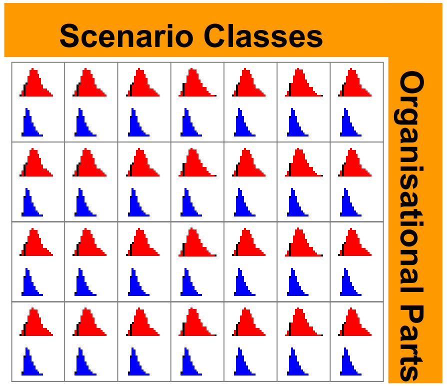


275,26
127,69
~~574,68~~
892,72
~~449,62~~
688,35
694,28

Mean,
Std. deviation,
etc.

How to ensure that scenarios are consistent, relevant and capture all material OR?

How to determine appropriate scenarios?



- The determination of a appropriate scenarios that are representative for OR is key to the scenario based AMA
- Scenario classes – one or more – are classes that are derived from loss event types or risk factors and that contain scenarios. (Example: Scenario class = IT-break down.)
- Organisational parts are the parts of the organisation for which OR is separately evaluated.
- Generate scenario(s) per scenario class and organisational part based on:-
  - guided discussions with the business in workshops (eg. Dresdner; Fortis, HBOS)
  - a matrix of „critical resources and states of risk“ (eg. Banca Intesa)
  - weaknesses per risk factor (eg. UFJ Holdings)
  - a specification of critical resources and failure periods by the organisational parts (eg. Dresdner)
  - addressing particular management concerns (all)
- All scenarios are fully documented to allow independent review and assessment

How to ensure that scenarios are consistent, relevant and capture all material operational risks?

- *Consistent?*
  - Every organisational part must consider as a minimum each of the common set of scenario classes, thereby achieving consistency of the overall framework.
  - Techniques such as workshops assist to achieve consistency of scenarios across organisational units
  - Review by Internal Audit and Risk Functions provides further consistency between organisational parts.
- *Relevant?*
  - Every organisational part assesses the relevance of all scenarios to its business thereby ensuring relevance to them (e.g. if a org-unit is not dependent on IT, it does not make sense to evaluate the risk due to IT break-down).
- *Capture all material operational risks?*
  - The techniques to determine the scenario classes (eg use of expert judgement and historical loss data) maximise coverage of known and foreseen risks.
  - This coverage is further enhanced when applied to the organisational parts and discussed with them to ensure that their specific risks are covered.

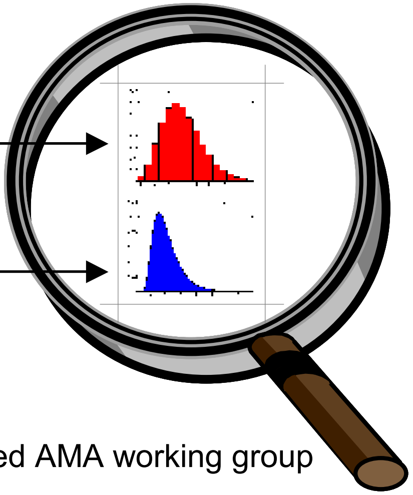
How to evaluate scenarios in an organisation?

- For each scenario banks assess potential loss frequencies and potential loss severities.
- The organisational process of evaluation is based on:
  - questionnaires
  - guided workshops
  - central (management) expertise
- In order to come up with plausible answers banks base their evaluation on information relevant to the scenario, such as
  - an assessment of operational quality / quality of control environment
  - past losses, key risk indicators, insurance
  - industry and managerial experience
- To validate the scenario evaluations banks apply techniques such as
  - 4-eye principle
  - Internal audits of assessment process and resulting quality
  - Comparison between actual losses and expert expectations
  - Consistency checks (e.g. psychometric analysis, Group functions challenge profiles of organisational parts, comparison to internal audit findings and validation.)

How to use evaluated scenarios for modelling purposes?

- A good risk model must be **consistent, robust, and stable over time**, so that changes in economic capital result from changes in the underlying risk profile and not from changes in the model.
- A model on risk requires **plausible assumptions** where distributions or analytical solutions are used
- The model requires the **estimation of its parameters**.
- The data required for the parameter estimation must go through a rigorous data **quality assurance**.

Raw Data AFTER data cleansing					*Parameter Estimates for Distribution*			
Scenario Class	**Typical Frequency**	**Frequency Upper Bound**	**Typical Severity**	**Severity Upper Bound**	***Mean Frequency***	***Standard Deviation***	***Mean Severity***	***Standard Deviation***
IT					***4***	***2***	***200***	***233***
* Scenario 1	1	6	50	300				
* Scenario 2	6	10	300	1000				
* Scenario 3	5	7	250	700				
Control					***6***	***3***	***250***	***125***
* Scenario 1	3	6	100	500				
* Scenario 2	7	10	400	100				
* Scenario 3	8	20	250	900				
...					***...***	***...***	***...***	***...***



Why a scenario based AMA improves OR management

- In order to reduce risk OR managers may decide to improve the quality of their risk factors (such as controls, IT, special knowledge, etc.)
- The process of evaluating and analysing the risk factors and controls associated with scenarios provides important information on how to improve OR management.
- Once such improvements have been achieved, i.e., organisational parts have reduced their operational risk profile, the corresponding scenarios can be re-assessed.
- If the re-assessment leads to lower frequency and severity estimates this will result in a lower economic capital requirement.
- In this way an incentive is created to improve the quality of their risk factors.
- This in turn leads to an improvement in overall OR management.

Key benefits of a scenario based AMA

- Forward looking, pro-active risk management
- Direct link to the management process (use test)
- Takes account of internal losses, KRIs and external events
- Responsive to changes in the environment
- Immediately incorporates changes in the organisational environment
- Focusses on „key risk exposures“ / material exposures
- Relatively transparent
- Supports risk culture
- Incentivises risk management
- Strong link between controls and risk
- Linkage between economic / regulatory capital and business risk profile
- Business specific / flexible to adjust to the business needs
- Helps identify mitigation priorities (cost/benefit)

How other building blocks (Losses, KRIs, Control Environment) link into scenario based AMA

Scenario Generation:

- External losses to build sensible scenarios
- Loss types to devise sensible scenario classes

Scenario Evaluation:

- Loss data where available as a mean to assess scenarios or to validate expert evaluations
- External loss data where available to help assess certain scenarios
- Key risk indicators to validate the assessment of certain scenarios
- Quality of control environment is considered when assessing frequency and severity of the scenarios and in some cases explicitly rated.

Model building:

- Historical losses where available to determine and justify assumptions about statistical distributions in the risk capital model

Validation of aggregated potential loss distribution:

- Historical losses to check on plausibility of certain quantiles of aggregated potential loss distribution

Example of how other building blocks link into scenario assessment

- External loss data, loss event types and knowledge about necessary operational resources generate the following scenario:
- What if a particular IT-system (e.g. a key payments system) breaks down for a critical time period?
- An expert in payments systems estimates on the basis of his experience:
  - a potential loss severity for this scenario of $100,000
  - a potential loss frequency for this scenario of 1in 5 years.
- An analysis of past losses shows that he has indeed estimated a reasonable severity number.
- An analysis of the corresponding key risk indicators (e.g system downtime / IT staff turnover) shows, however, that he has underestimated the potential loss frequency which will subsequently be corrected in the data quality assurance process.
- Thus other building blocks can be used both to generate scenarios and assure the quality of the assessment thereby influencing the resulting economic capital.

Overlap / similarities with LDA and Scorecard Approach

An „Scorecard Approach“ and a Scenario based AMA both

- employ scenarios to be evaluated as part of the „scorecard“
- are sensitive to changes in the actual operational risk profile in an organisational part
- make use of expert opinion as part of the data to assess the operational risk

A Loss Distribution Approach and a Scenario based AMA both:

- employ a statistical model
- recognize the fact that loss data alone is not forward looking
- rely on scenarios where losses are sparse

Illustrations

Overview of implemented industry practices

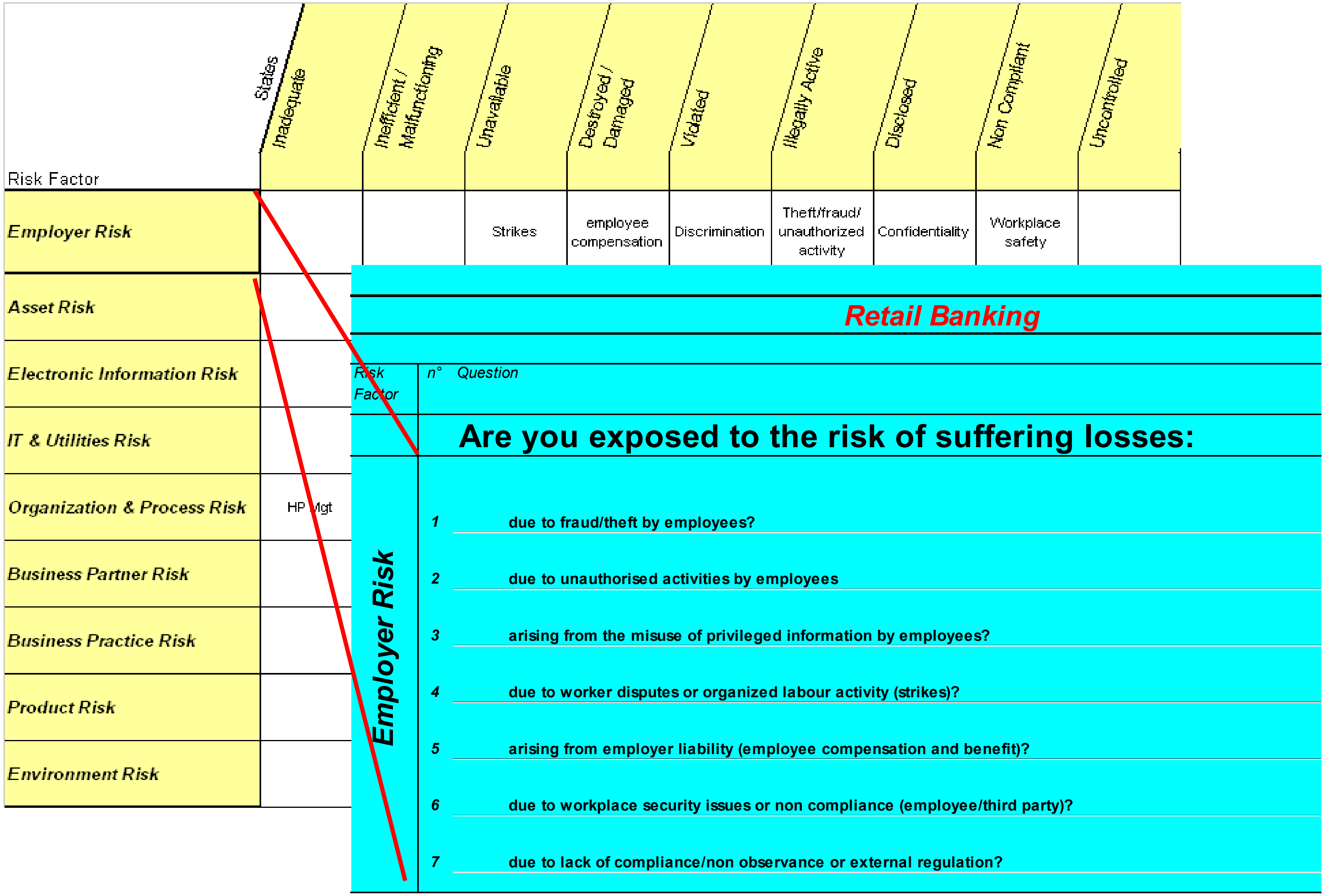
How to determine appropriate scenarios?

Banca Intesa

Employer relations, policy & Employment law

Employee criminal activity / repudiation of law

Institution criminal activity / repudiation of law



Risk Factor \ States	Inadequate	Inefficient / Malfunctioning	Unavailable	Destroyed / Damaged	Violated	Illegally Active	Disclosed	Non Compliant	Uncontrolled
Employer Risk			Strikes	employee compensation	Discrimination	Theft/fraud/ unauthorized activity	Confidentiality	Workplace safety	
Asset Risk									
Electronic Information Risk									
IT & Utilities Risk									
Organization & Process Risk	HP Mgt								
Business Partner Risk									
Business Practice Risk									
Product Risk									
Environment Risk									

Retail Banking

Risk Factor	n°	Question
		Are you exposed to the risk of suffering losses:
Employer Risk	1	due to fraud/theft by employees?
	2	due to unauthorised activities by employees
	3	arising from the misuse of privileged information by employees?
	4	due to worker disputes or organized labour activity (strikes)?
	5	arising from employer liability (employee compensation and benefit)?
	6	due to workplace security issues or non compliance (employee/third party)?
	7	due to lack of compliance/non observance or external regulation?

Dresdner Bank

- We have defined 10 risk factors, that we believe are the most important usual resources in any process or any organisational part in any organisation.
- For these 10 risk factors we have build 10 scenario classes, i.e. the resource fails, breaks down, is of poor quality, does not work, is not existent etc.

Example:

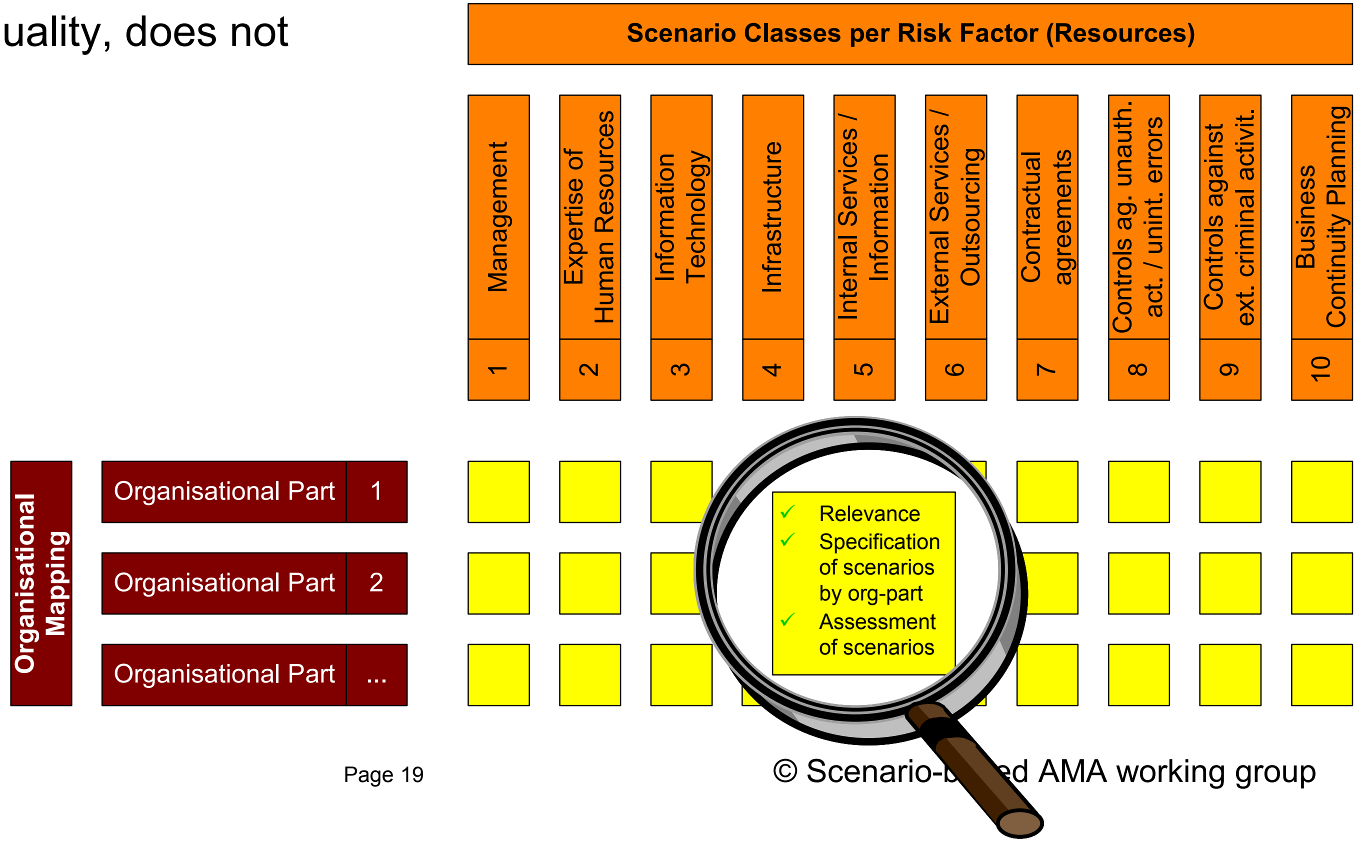
Resource = IT.

Generic scenario class = IT breaks down critical time period.

Organisational part = Front office equity trading.

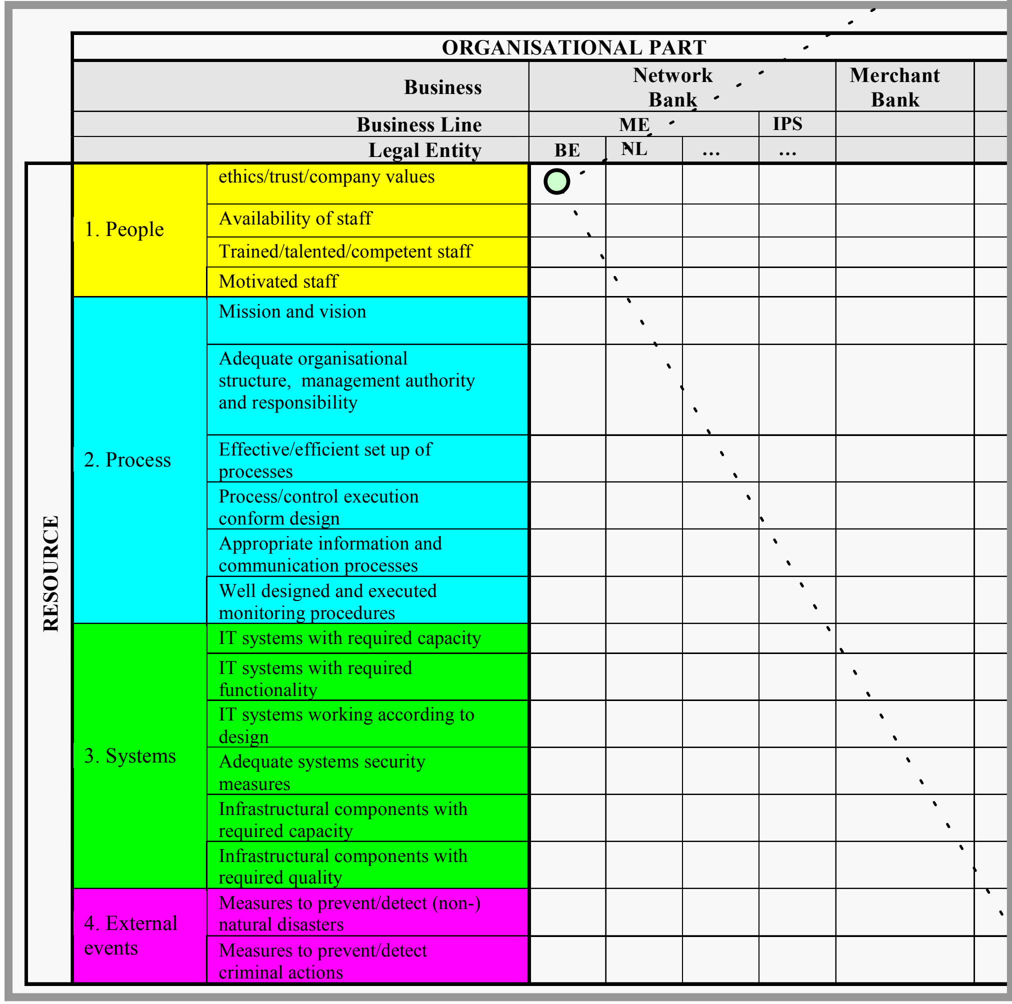
Specified scenario = IT-system (e.g. Imagine) for equity trading breaks down 1 day.

- In order to determine specific scenarios that are meaningful for a particular organisational part, we ask whether each scenario class is relevant for the organisational part in question. If yes, scenarios of this class are specified and evaluated by experts of the organisational part.

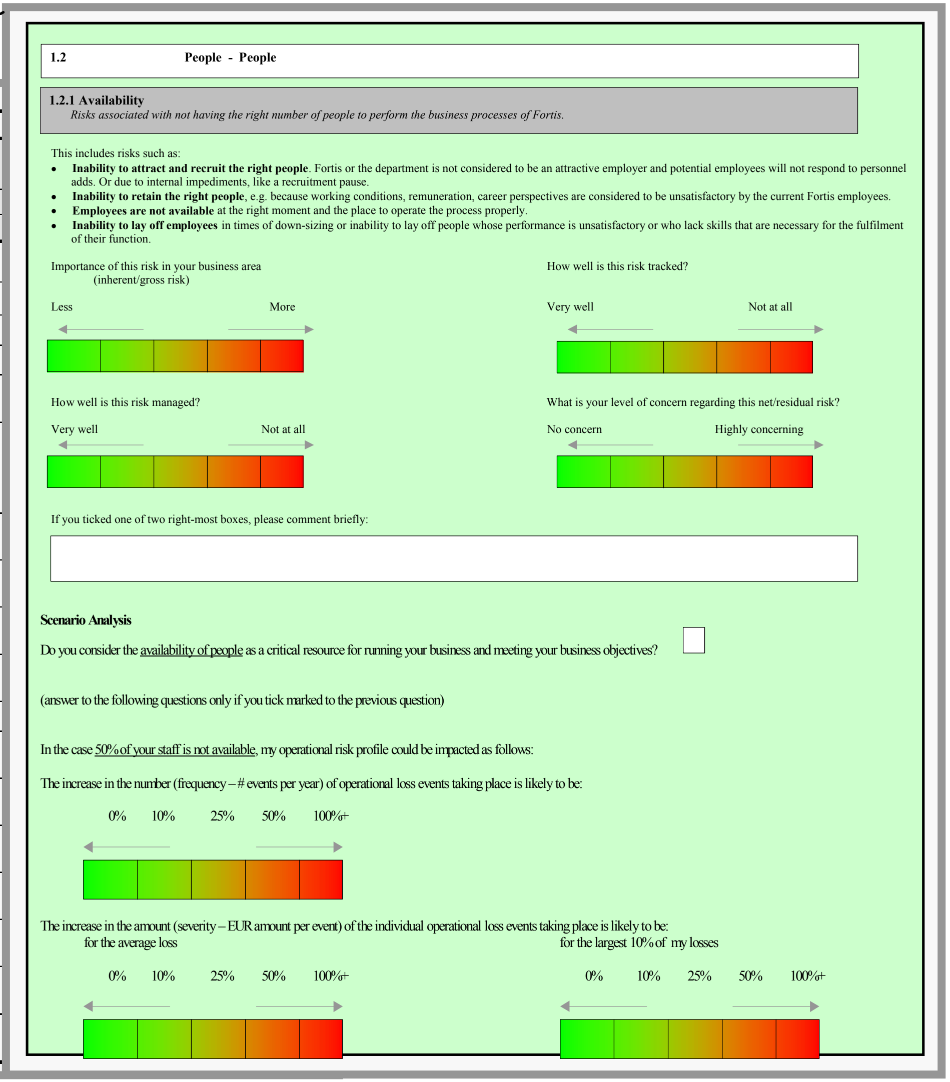


Scenario Classes per Risk Factor (Resources)
Management 1
Expertise of Human Resources 2
Information Technology 3
Infrastructure 4
Internal Services / Information 5
External Services / Outsourcing 6
Contractual agreements 7
Controls ag. unauth. act. / unint. errors 8
Controls against ext. criminal activit. 9
Business Continuity Planning 10
Organisational Mapping
Organisational Part 1
Organisational Part 2
Organisational Part ...
✓ Relevance
✓ Specification of scenarios by org-part
✓ Assessment of scenarios

FORTIS



		ORGANISATIONAL PART					
		Business	Network Bank				Merchant Bank
		Business Line	ME			IPS	
		Legal Entity	BE	NL	…	…	
RESOURCE	1. People	ethics/trust/company values	○				
		Availability of staff					
		Trained/talented/competent staff					
		Motivated staff					
	2. Process	Mission and vision					
		Adequate organisational structure, management authority and responsibility					
		Effective/efficient set up of processes					
		Process/control execution conform design					
		Appropriate information and communication processes					
		Well designed and executed monitoring procedures					
	3. Systems	IT systems with required capacity					
		IT systems with required functionality					
		IT systems working according to design					
		Adequate systems security measures					
		Infrastructural components with required capacity					
		Infrastructural components with required quality					
	4. External events	Measures to prevent/detect (non-) natural disasters					
		Measures to prevent/detect criminal actions					



1.2 People - People

1.2.1 Availability

Risks associated with not having the right number of people to perform the business processes of Fortis.

This includes risks such as:

- **Inability to attract and recruit the right people**. Fortis or the department is not considered to be an attractive employer and potential employees will not respond to personnel adds. Or due to internal impediments, like a recruitment pause.
- **Inability to retain the right people**, e.g. because working conditions, remuneration, career perspectives are considered to be unsatisfactory by the current Fortis employees.
- **Employees are not available** at the right moment and the place to operate the process properly.
- **Inability to lay off employees** in times of down-sizing or inability to lay off people whose performance is unsatisfactory or who lack skills that are necessary for the fulfilment of their function.

Importance of this risk in your business area
(inherent/gross risk)

Less ← → More

How well is this risk tracked?

Very well ← → Not at all

How well is this risk managed?

Very well ← → Not at all

What is your level of concern regarding this net/residual risk?

No concern ← → Highly concerning

If you ticked one of two right-most boxes, please comment briefly:

Scenario Analysis

Do you consider the availability of people as a critical resource for running your business and meeting your business objectives? □

(answer to the following questions only if you tick marked to the previous question)

In the case 50% of your staff is not available, my operational risk profile could be impacted as follows:

The increase in the number (frequency – # events per year) of operational loss events taking place is likely to be:

0% 10% 25% 50% 100%+

The increase in the amount (severity – EUR amount per event) of the individual operational loss events taking place is likely to be:

for the average loss

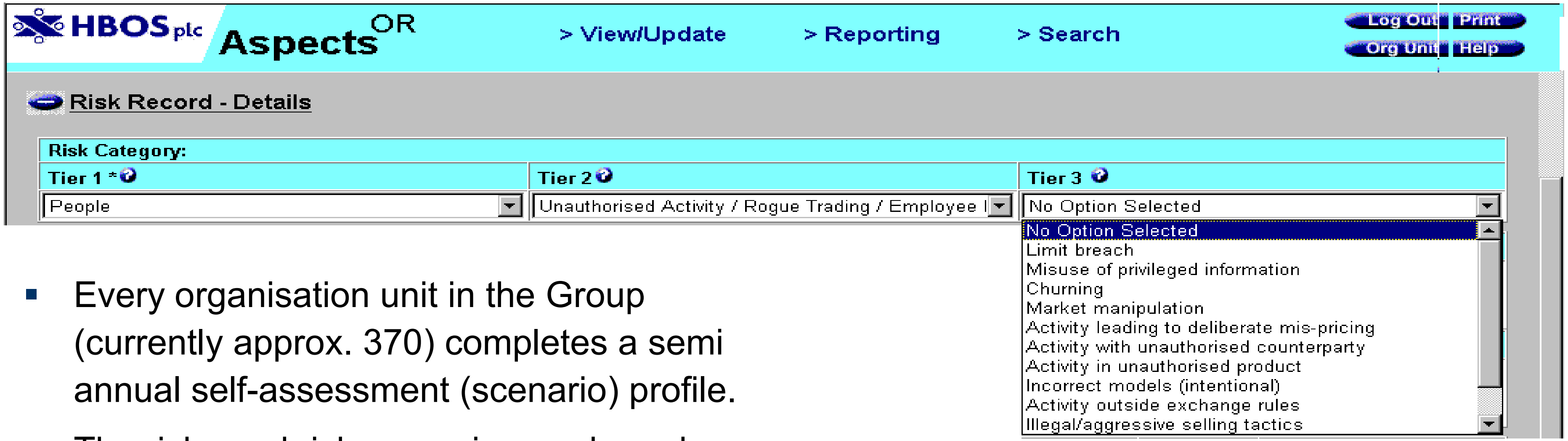
0% 10% 25% 50% 100%+

for the largest 10% of my losses

0% 10% 25% 50% 100%+

- We have defined a comprehensive list of risk factors (resources). The criticality of each risk factor is analysed together with the business during the yearly self-assessment exercise.
- One scenario is built for each identified critical resource. The scenario consists of the non-availability of one specific critical resource. It involves frequency and severity estimations relative to the current situation.

Halifax Bank of Scotland



Risk Record - Details

Risk Category:

Tier 1 *	Tier 2	Tier 3
People	Unauthorised Activity / Rogue Trading / Employee I	No Option Selected

No Option Selected
Limit breach
Misuse of privileged information
Churning
Market manipulation
Activity leading to deliberate mis-pricing
Activity with unauthorised counterparty
Activity in unauthorised product
Incorrect models (intentional)
Activity outside exchange rules
Illegal/aggressive selling tactics

- Every organisation unit in the Group (currently approx. 370) completes a semi annual self-assessment (scenario) profile.
- The risks and risk scenarios are based on a 3 tiered categorisation framework, tier 1 being people process, systems, external and business (shown above).
- The process involves considering internal & external losses, together with changes in the businesses environment relating to the categorisation framework.
- It is a Group-wide exercise with the ability to cross reference risks and responsibility between business areas (i.e. Where the potential impact will effect one area but the process is owned in another).

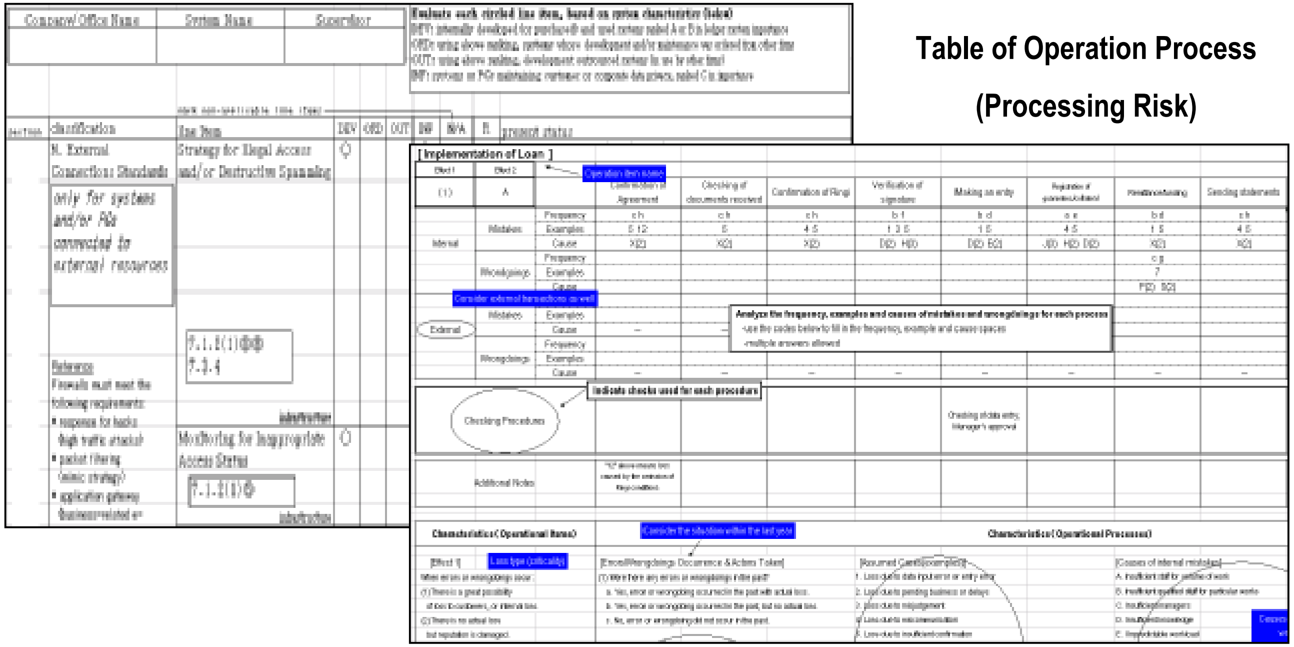
UFJ Holdings, Inc.

System Risk Evaluation Sheet

(IT System Risk)

Table of Operation Process

(Processing Risk)



Company/Office Name	System Name	Supervisor

Evaluate each circled line item, based on system characteristics (below)
DEV: [illegible]
ORD: [illegible]
OUT: [illegible]
INF: [illegible]

section	classification	line item	DEV	ORD	OUT	INF	N/A	R	present status
	N. External Connection Standards only for systems and/or PCs connected to external resources	Strategy for Illegal Access and/or Destructive Spamming 7.1.2(1)①② 7.3.4	○						
	Reference Firewalls must meet the following requirements: • response for hacks (high traffic attacks) • packet filtering (static strategy) • application gateway (business-related or [illegible]	Monitoring for Inappropriate Access Status 7.1.2(1)⑥	○						

[Implementation of Loan]

Operation item name

Effect 1	Effect 2			Confirmation of Agreement	Checking of documents received	Confirmation of Ringi	Verification of signature	Making an entry	Registration of [illegible]	[illegible]	Sending statements
(1)	A										
Internal	Mistakes	Frequency		c h	c h	c h	b f	b d	a e	b d	c h
		Examples		5 12	5	4 5	1 3 5	1 5	4 5	1 5	4 5
		Cause		X(2)	X(2)	X(2)	D(2) H(0)	D(2) E(2)	J(0) H(2) D(2)	X(2)	X(2)
	Wrongdoings	Frequency								c g	
		Examples								7	
		Cause								F(2) S(2)	
External	Mistakes	Examples									
		Cause		–	–						
	Wrongdoings	Frequency									
		Examples									
		Cause		–	–	–	–	–	–	–	–
Checking Procedures								Checking of data entry, Manager's approval			
Additional Notes				"X" above means loss caused by the omission of [illegible]							

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

Characteristics (Operational Items)

Consider the situation within the last year

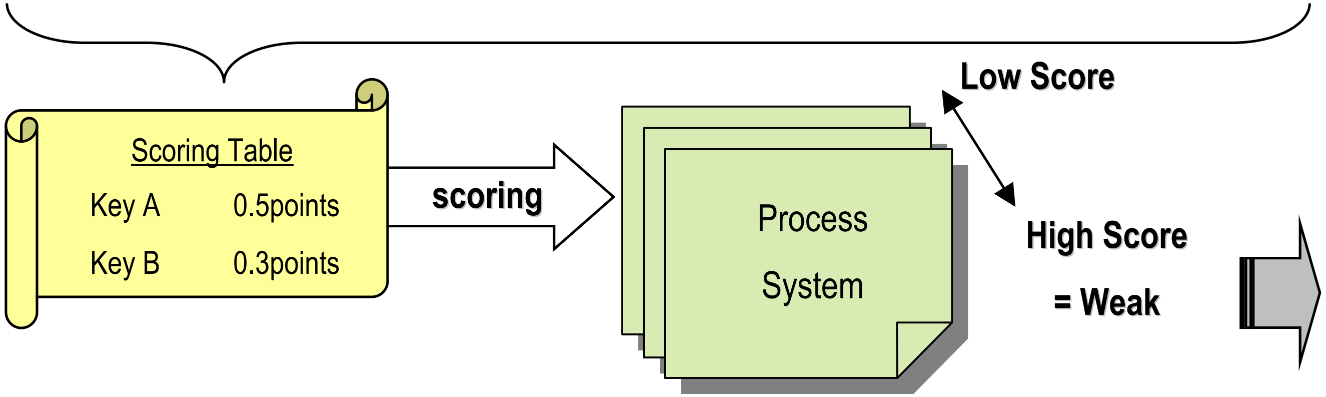
Characteristics (Operational Processes)

[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 & Actions 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 misjudgement
4. Loss due to miscommunication
5. Loss due to insufficient confirmation

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

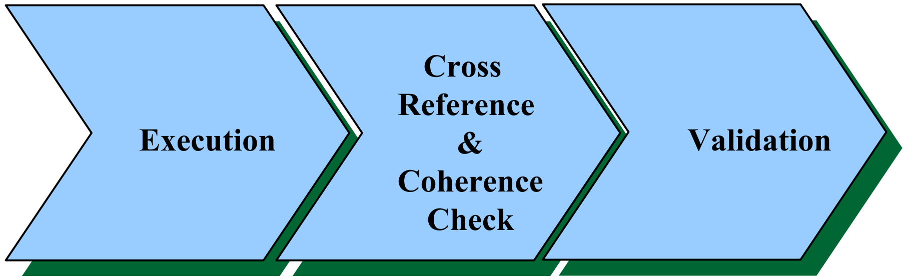


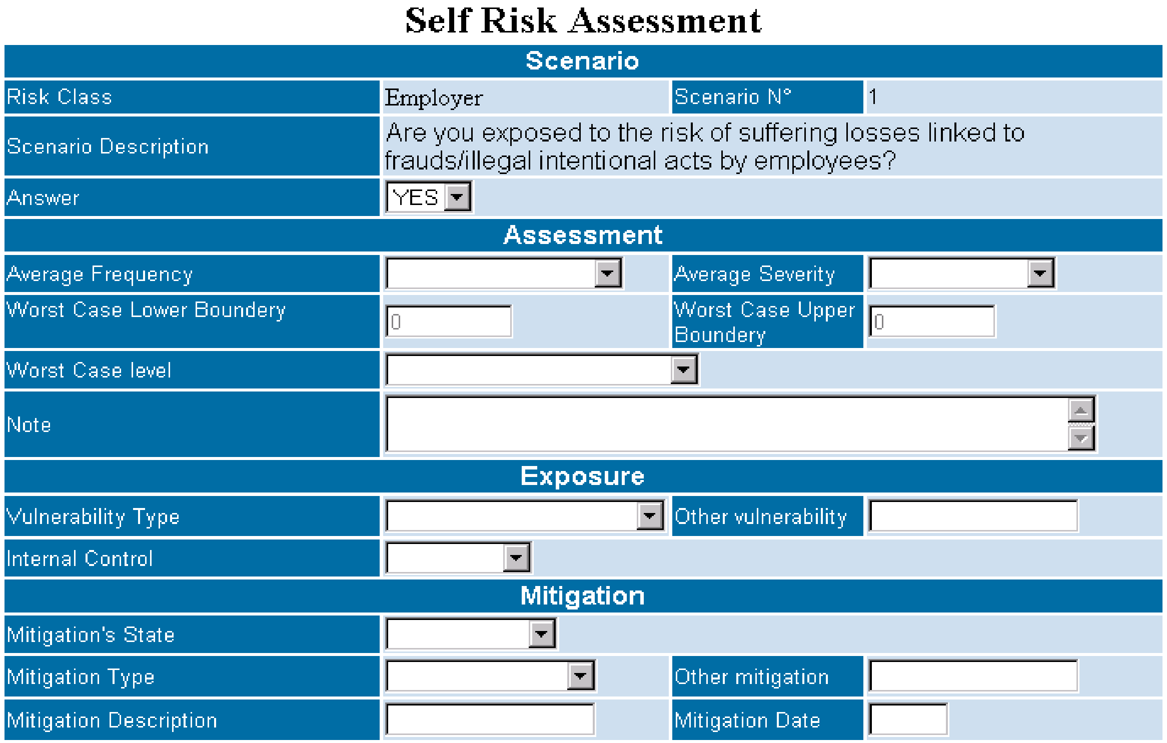
- Self risk assessment are made via group-wide tools for every material process/system.
- Weaknesses against operational risk events are identified for each process/system via standard assessment keys.
- The risk assessment process involves evaluating the control level and considering changes in the business environment.
- Completed evaluation sheets are scored by using a scoring table which assigns a score to each assessment key.
- Higher-scored processes/systems are eligible for scenario generation.

How to evaluate scenarios in an organisation?

Banca Intesa

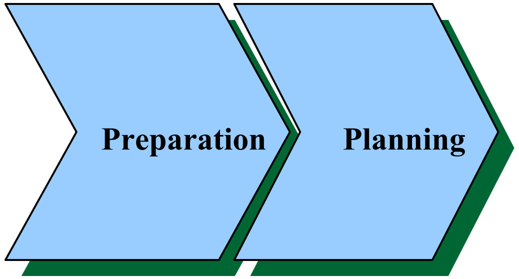
- The scenario forms (questionnaires) are distributed by an Intranet based (Java) assessment tool (GARI)
- Each questionnaire refers to a part of the organisation based on an organisational mapping. The Head of each Division or department executes the assessment
- The results of each questionnaire is validated by Internal Audit and the Security Office





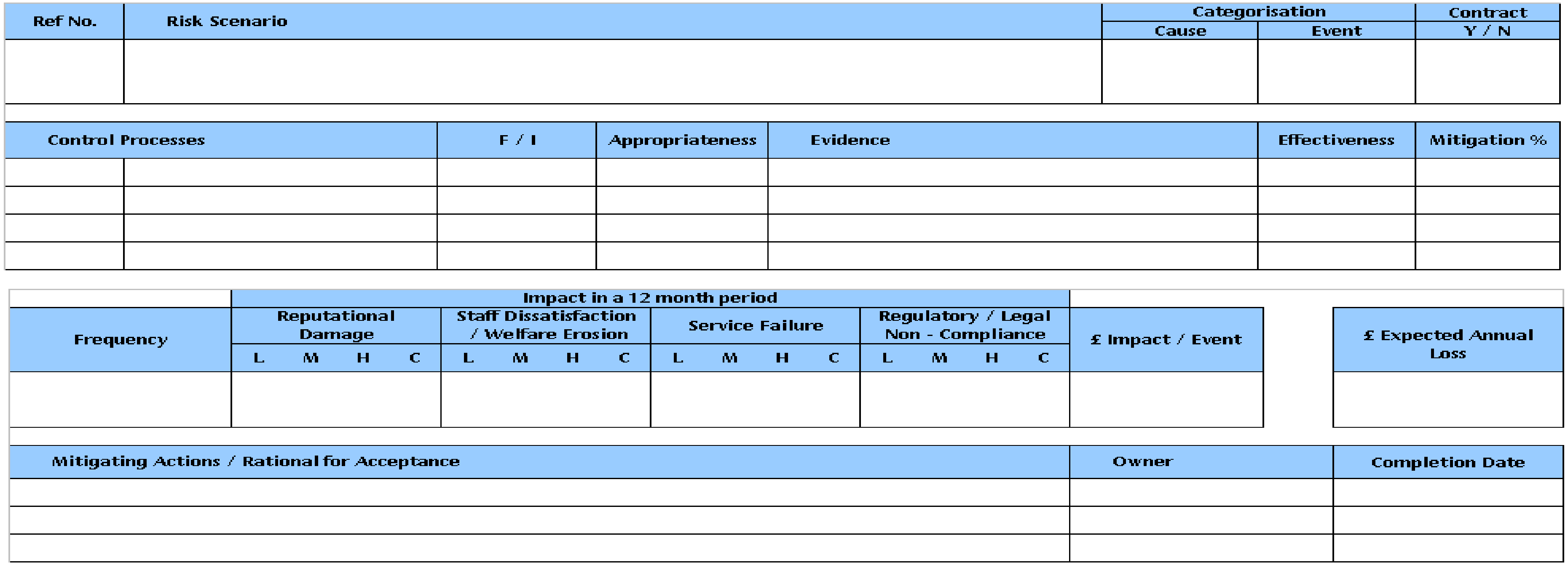
Self Risk Assessment

Scenario			
Risk Class	Employer	Scenario N°	1
Scenario Description	Are you exposed to the risk of suffering losses linked to frauds/illegal intentional acts by employees?		
Answer	YES		
Assessment			
Average Frequency		Average Severity	
Worst Case Lower Boundery	0	Worst Case Upper Boundery	0
Worst Case level			
Note			
Exposure			
Vulnerability Type		Other vulnerability	
Internal Control			
Mitigation			
Mitigation's State			
Mitigation Type		Other mitigation	
Mitigation Description		Mitigation Date	



- Inputs
  - Internal/External Loss Data
  - KRI / Last years SRA
  - Audit & security reports
  - ORM correspondents
  - Organizational structure of the bank
  - Risk Class Model
  - Predefined severity/WC classes

Barclays



Ref No.	Risk Scenario	Categorisation		Contract
		Cause	Event	Y / N

Control Processes		F / I	Appropriateness	Evidence	Effectiveness	Mitigation %

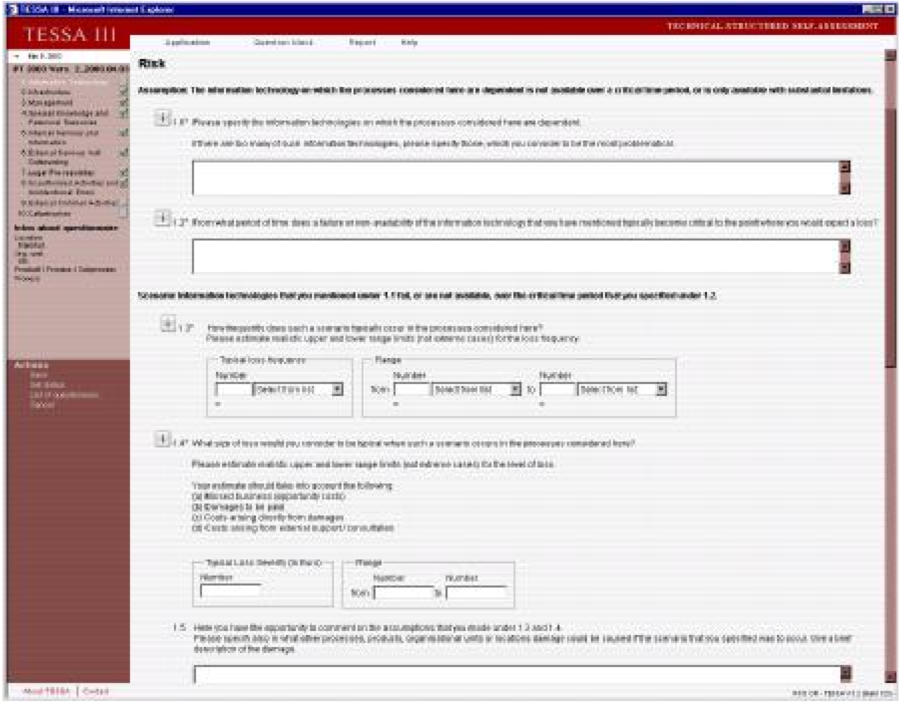
	Impact in a 12 month period					
Frequency	Reputational Damage	Staff Dissatisfaction / Welfare Erosion	Service Failure	Regulatory / Legal Non - Compliance	£ Impact / Event	£ Expected Annual Loss
	L M H C	L M H C	L M H C	L M H C		

Mitigating Actions / Rational for Acceptance	Owner	Completion Date

- Risk scenarios are evaluated by relevant business expertise either through a facilitated risk workshop or through self assessment questionnaires.
- Key inputs into the evaluation are Loss experience, KRIs and Audit Information.
- The appropriateness and effectiveness of the controls are assessed and a decision taken whether further investment is required in controls or whether the risk is within appetite and should be accepted in line with Group Risk Acceptance Policy.

Dresdner Bank

- The scenarios are distributed by a Web-Tool called TESSA (a module of ORTOS)
- The distribution follows a defined workflow.
- Each questionnaire refers to a part of the organisation based on an organisational mapping.
- For each organisational part an assessor and an approver are determined.
- The assessors fill in the questionnaires, the approvers approve them.
- Questionnaires also serve as a guidence for workshops.
- Subsequently the analysis and quality assurance take place.



TESSA III

TECHNICAL STRUCTURED SELF-ASSESSMENT

Risk

Assumption: The information technology on which the processes considered here are dependent is not available over a critical time period, or is only available with substantial limitations.

1.1* Please specify the information technologies on which the processes considered here are dependent.

If there are too many of such information technologies, please specify those, which you consider to be the most problematical.

1.2* From what period of time does a failure or non-availability of the information technology that you have mentioned typically become critical to the point where you would expect a loss?

Scenario: Information technologies that you mentioned under 1.1 fail, or are not available, over the critical time period that you specified under 1.2.

1.3* How frequently does such a scenario typically occur in the processes considered here?
Please estimate realistic upper and lower range limits (not extreme cases) for the loss frequency.

Typical loss frequency: Number [ ] Select from list
Range: Number from [ ] Select from list to Number [ ] Select from list

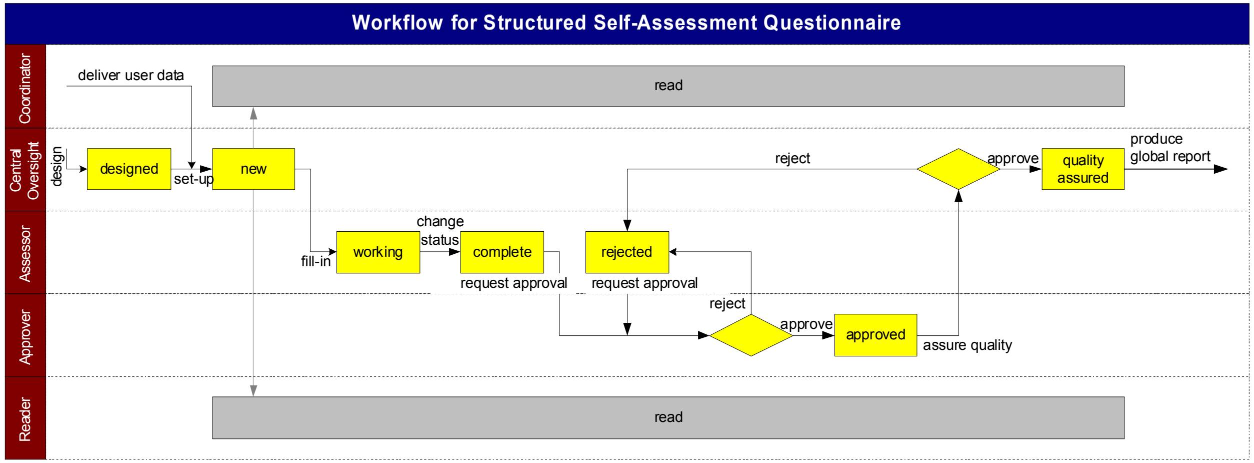
1.4* What size of loss would you consider to be typical when such a scenario occurs in the processes considered here?

Please estimate realistic upper and lower range limits (not extreme cases) for the level of loss.

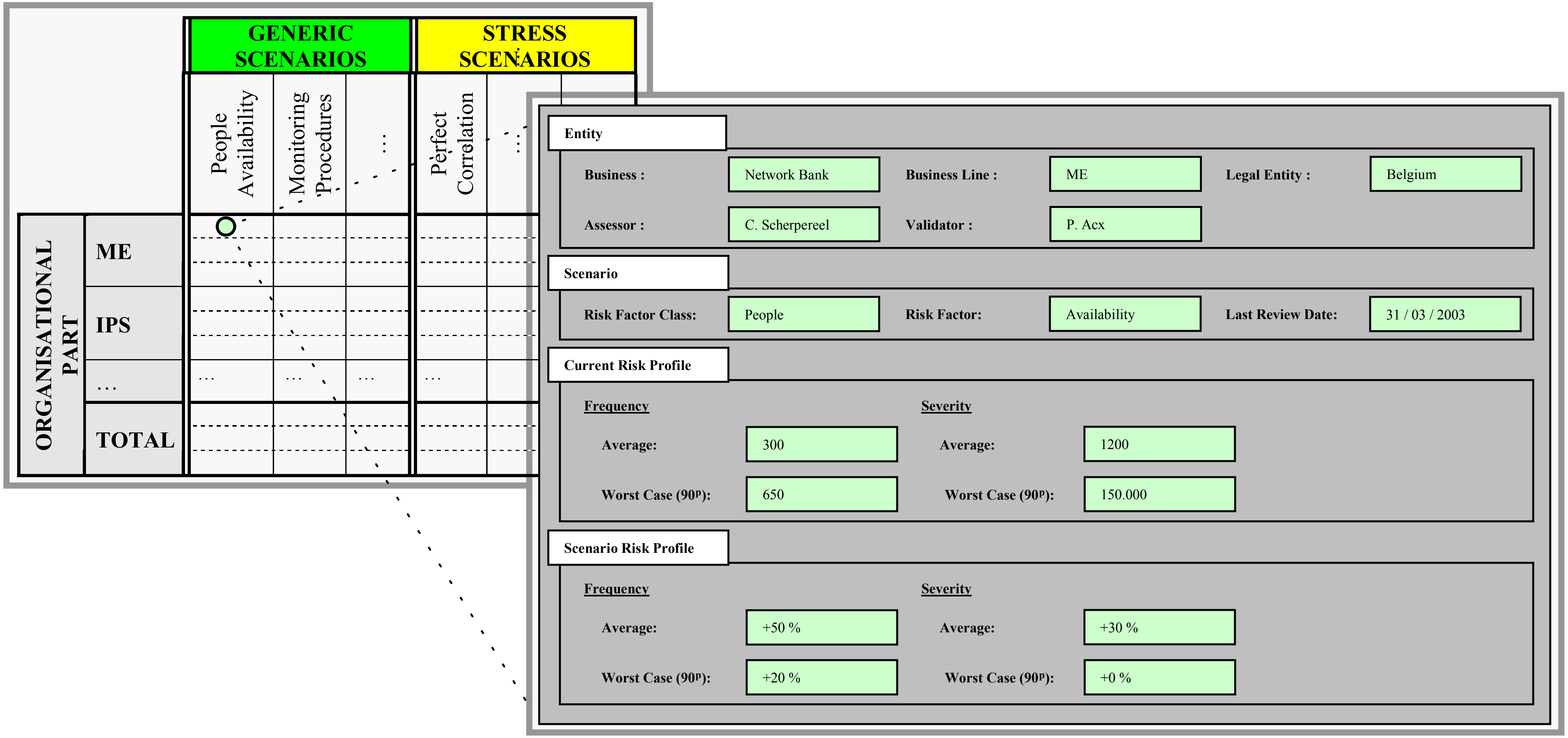
Your estimate should take into account the following:
(a) Missed business opportunity costs
(b) Damages to be paid
(c) Costs arising directly from damages
(d) Costs arising from external support/ consultation

Typical Loss Severity (in Euro): Number [ ]
Range: Number from [ ] to Number [ ]

1.5 Here you have the opportunity to comment on the assumptions that you made under 1.3 and 1.4.
Please specify also in what other processes, products, organisational units or locations damage could be caused if the scenario that you specified was to occur. Give a brief description of the damage.



FORTIS



		GENERIC SCENARIOS			STRESS SCENARIOS	
		People Availability	Monitoring Procedures	…	Perfect Correlation	…
ORGANISATIONAL PART	ME	○				
	IPS					
	…	…	…	…	…	
	TOTAL					

Entity

Business :	Network Bank	Business Line :	ME	Legal Entity :	Belgium
Assessor :	C. Scherpereel	Validator :	P. Acx		

Scenario

Risk Factor Class:	People	Risk Factor:	Availability	Last Review Date:	31 / 03 / 2003

Current Risk Profile

Frequency		Severity	
Average:	300	Average:	1200
Worst Case (90^{p}):	650	Worst Case (90^{p}):	150.000

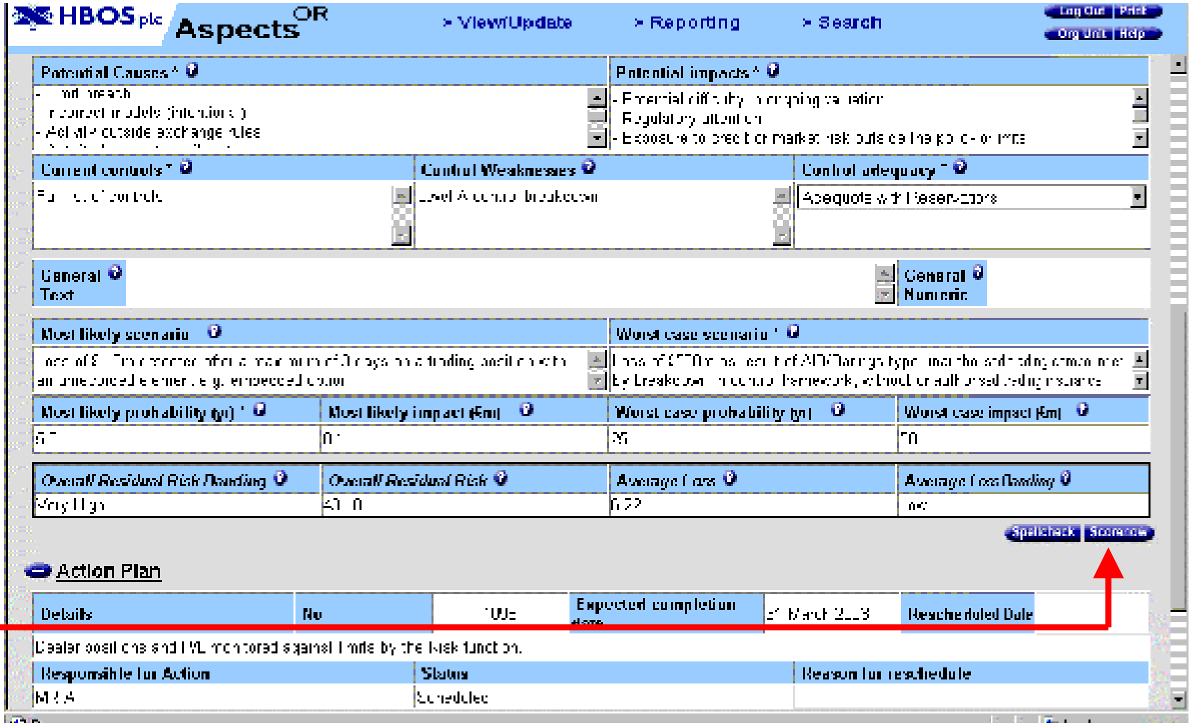
Scenario Risk Profile

Frequency		Severity	
Average:	+50 %	Average:	+30 %
Worst Case (90^{p}):	+20 %	Worst Case (90^{p}):	+0 %

- The scenarios are stored in a central database (OPERA) and are reviewed on yearly basis.
- Scenarios are currently built for each organisational part, i.e. business line/legal entity. Scenario outcomes, together with self-assessment results, KRIs, loss experience, etc, are discussed with the business risk management team/business risk committee.

Halifax Bank of Scotland

- Delivered through AspectsOR, an inhouse built, intranet based tool.
- Facilitated workshops define the scenarios (full training undertaken, including lessons learnt, for the facilitators after each exercise).
- Identify 2 scenarios per risk, most likely and worse case scenario.
- A residual and average risk exposure figure is then calculated per risk within AspectsOR.



Potential Causes *
- [illegible] breach
Incorrect models (intentional)
- Activity outside exchange rules

Potential impacts *
- Financial difficulty [illegible] valuation
Regulatory attention
- Exposure to credit or market risk outside the [illegible] limits

Current controls *
[illegible] controls

Control Weaknesses
Level A control breakdown

Control adequacy *
Adequate with Reservations

General Text

General Numeric

Most likely scenario
Loss of £[illegible] [illegible] days on a trading position with an unreconciled element e.g. embedded option

Worst case scenario *
Loss of £[illegible] as a result of [illegible] by breakdown in control framework, [illegible]

Most likely probability (yr) *	Most likely impact (£m)	Worst case probability (yr)	Worst case impact (£m)
[illegible]	0.1	25	50

Overall Residual Risk Banding	Overall Residual Risk	Average Loss	Average Loss Banding
Very High	[illegible]	0.72	[illegible]

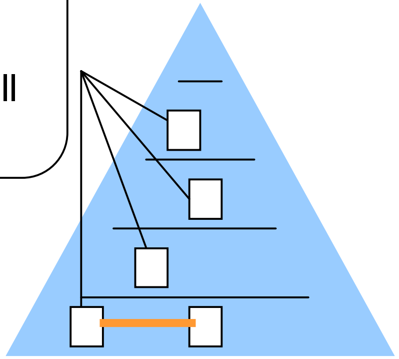
Action Plan

Details	No	1005	Expected completion date	31 March 2003	Rescheduled Date	

Dealer positions and P&L monitored against limits by the Risk function.

Responsible for Action	Status	Reason for reschedule
M&A	Scheduled	

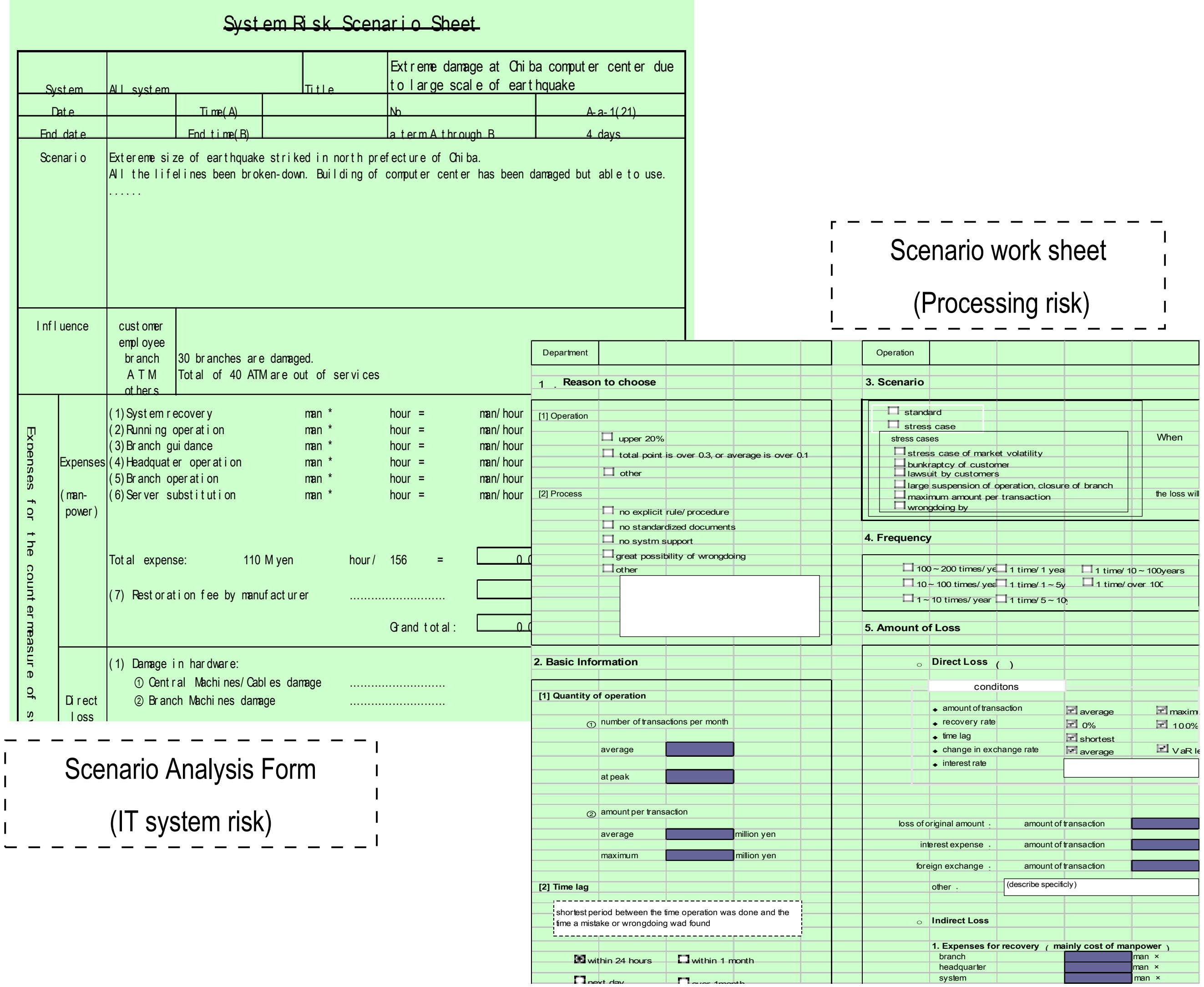
Business units complete Operational Risk Profiles (ORP) at all levels.



- Annual loss distribution obtained on the basis of the scenario results by convolution.
- Correlation between risk types introduced via monte carlo, preformed with a common seed.
- Potential double counting of risk is mitigated by aggregation and adopt functionailty in AspectsOR

UFJ Holdings, Inc.

- Operational loss “generic scenarios” and “stress scenarios” are created for the weaker (or, “higher-scored”) processes/systems.
- Scenario worksheets which are group-wide tools are distributed in Excel format.
- The expert, who completed the original risk assessment, create the scenario.
- Risk management sections verify the scenarios.



System Risk Scenario Sheet

System	All system		Title	Extreme damage at Chiba computer center due to large scale of earthquake	
Date		Time(A)		No	A-a-1(21)
End date		End time(B)		a term A through B	4 days
Scenario	Exterme size of earthquake striked in north prefecture of Chiba. All the lifelines been broken-down. Building of computer center has been damaged but able to use.				
Influence	customer employee branch A T M others	30 branches are damaged. Total of 40 ATM are out of services			

Expenses for the countermeasure of s

Expenses (man-power)

(1) System recovery man * hour = man/ hour
(2) Running operation man * hour = man/ hour
(3) Branch guidance man * hour = man/ hour
(4) Headquater operation man * hour = man/ hour
(5) Branch operation man * hour = man/ hour
(6) Server substitution man * hour = man/ hour

Total expense: 110 M yen hour/ 156 = 0.0

(7) Restoration fee by manufacturer ....

Grand total : 0.0

Direct loss

(1) Damage in hardware:
① Central Machines/Cables damage ....
② Branch Machines damage ....

Scenario Analysis Form

(IT system risk)

Scenario work sheet

(Processing risk)

Department

1 . Reason to choose

[1] Operation
□ upper 20%
□ total point is over 0.3, or average is over 0.1
□ other

[2] Process
□ no explicit rule/ procedure
□ no standardized documents
□ no systm support
□ great possibility of wrongdoing
□ other

2. Basic Information

[1] Quantity of operation

① number of transactions per month
average
at peak

② amount per transaction
average million yen
maximum million yen

[2] Time lag

shortest period between the time operation was done and the time a mistake or wrongdoing wad found

☒ within 24 hours □ within 1 month
□ next day □ over 1month

Operation

3. Scenario

□ standard
□ stress case

stress cases
□ stress case of market volatility
□ bunkraptcy of customer
□ lawsuit by customers
□ large suspension of operation, closure of branch
□ maximum amount per transaction
□ wrongdoing by

When

the loss will

4. Frequency

□ 100～200 times/ ye □ 1 time/ 1 yea □ 1 time/ 10～100years
□ 10～100 times/ yea □ 1 time/ 1～5y □ 1 time/ over 100
□ 1～10 times/ year □ 1 time/ 5～10y

5. Amount of Loss

○ Direct Loss ( )

conditons
◆ amount of transaction ☒ average ☒ maxim
◆ recovery rate ☒ 0% ☒ 100%
◆ time lag ☒ shortest
◆ change in exchange rate ☒ average ☒ VaR le
◆ interest rate

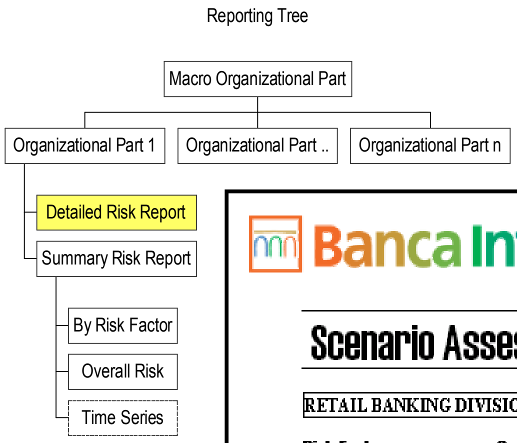
loss of original amount : amount of transaction
interest expense : amount of transaction
foreign exchange : amount of transaction
other : (describe specificly)

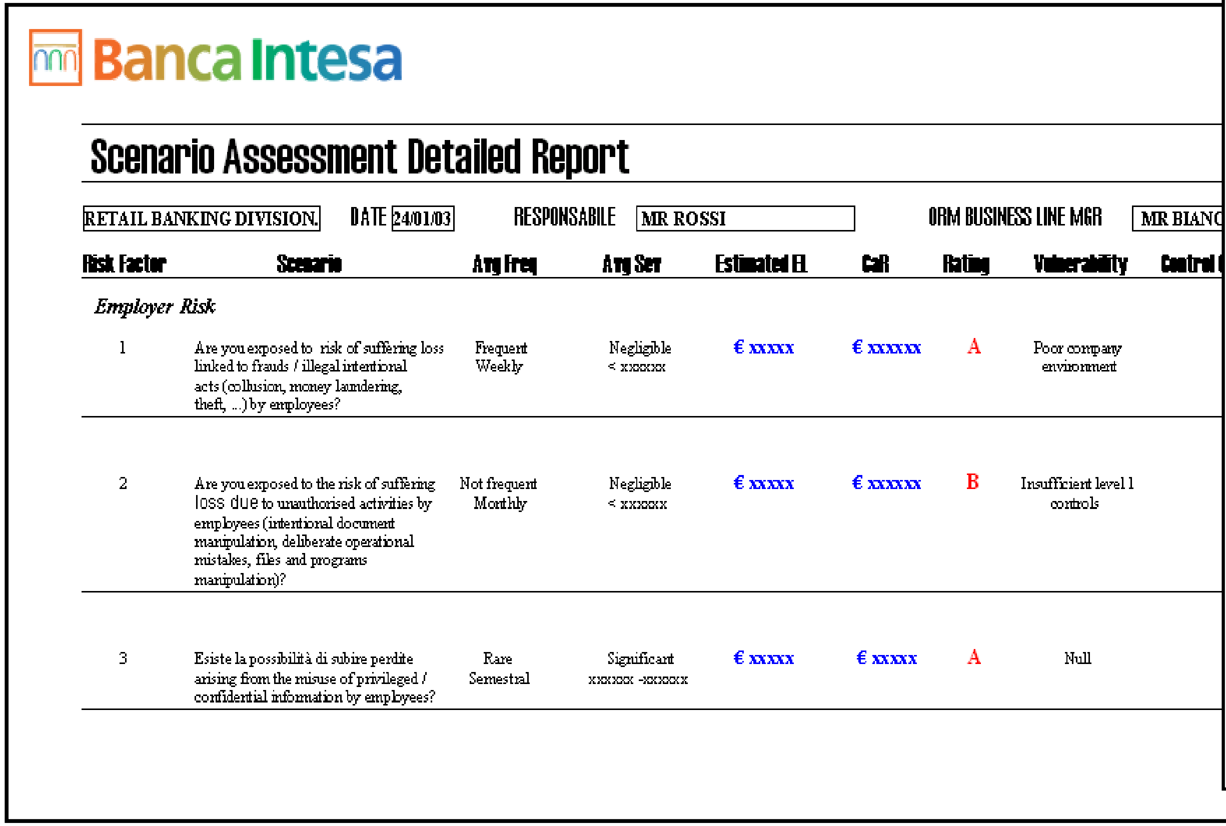
○ Indirect Loss

1. Expenses for recovery (mainly cost of manpower)
branch man ×
headquarter man ×
system man ×

What do reports resulting from assessments look like?
What are the dimensions on which reports are based?

Banca Intesa




Banca Intesa

Scenario Assessment Detailed Report

RETAIL BANKING DIVISION. DATE 24/01/03 RESPONSABILE MR ROSSI ORM BUSINESS LINE MGR MR BIANC

Risk Factor	Scenario	Avg Freq	Avg Ser	Estimated EL	CaR	Rating	Vulnerability	Control
Employer Risk								
1	Are you exposed to risk of suffering loss linked to frauds / illegal intentional acts (collusion, money laundering, theft, ...) by employees?	Frequent Weekly	Negligible < xxxxxx	€ xxxxx	€ xxxxxx	A	Poor company environment	
2	Are you exposed to the risk of suffering loss due to unauthorised activities by employees (intentional document manipulation, deliberate operational mistakes, files and programs manipulation)?	Not frequent Monthly	Negligible < xxxxxx	€ xxxxx	€ xxxxxx	B	Insufficient level 1 controls	
3	Esiste la possibilità di subire perdite arising from the misuse of privileged / confidential information by employees?	Rare Semestral	Significant xxxxxx -xxxxxx	€ xxxxx	€ xxxxx	A	Null	

Dimensions:

- Risk factor
- Description of scenario
- Potential loss frequency
- Potential loss severity (average + worst case)
- EL + CaR (Gross)
- Rating
- Vulnerability type
- Quality of control
- Mitigation Type

Barclays

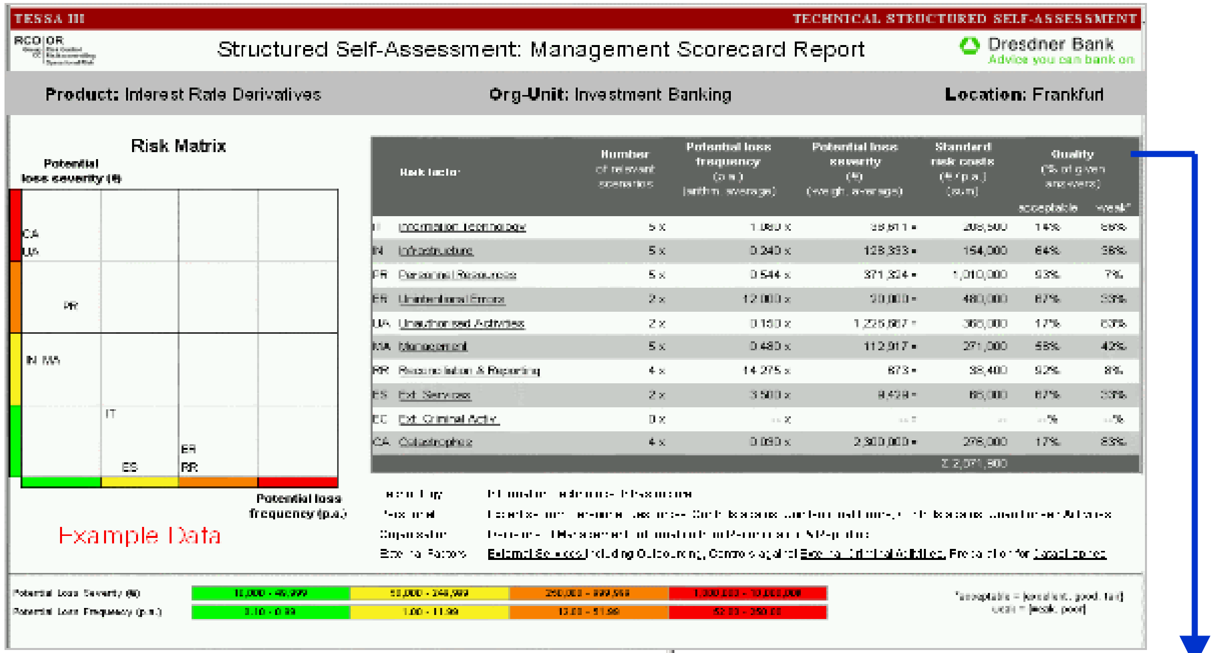
General Info				Data for EC model												
No	Type	Cluster	SBU	Business Activity	Risk Description	Con Effect	Freq	Impact (£m)	Fin Loss (£m)	Fin Loss	Rep Dam	Staff Diss/ Welfare Erosion	Service Failure	Reg/ Legal non Comp	Mit %	Overall Risk Rank

- The outputs of the scenario assessments feed the Business Area and Group Risk Profile Reports.
- The output informs management action including investment in controls, risk transfer and capital allocation.
- The scenario ‘potential loss’ data is modelled in conjunction with actual internal loss data to calculate the economic capital requirement for Business Areas and the Group.

Outputs include:

- Risk description
- Frequency
- Impact
- Annualised Financial Loss
- Indirect Impacts
- Level of Mitigation
- Required Management Actions

Dresdner Bank



TESSA III — TECHNICAL STRUCTURED SELF-ASSESSMENT

RCO | OR

Structured Self-Assessment: Management Scorecard Report

Dresdner Bank
Advice you can bank on

Product: Interest Rate Derivatives — **Org-Unit:** Investment Banking — **Location:** Frankfurt

Risk Matrix

Example Data

	Risk factor	Number of relevant scenarios	Potential loss frequency (p.a.) (arithm. average)	Potential loss severity (€) (weigh. average)	Standard risk costs (€ / p.a.) (sum)	Quality (% of given answers) acceptable	Quality (% of given answers) "weak"
IT	Information Technology	5 x	1.080 x	38,611 €	208,500	14%	86%
IN	Infrastructure	5 x	0.240 x	128,333 €	154,000	64%	36%
PR	Personnel Resources	5 x	0.544 x	371,324 €	1,010,000	93%	7%
ER	Unintentional Errors	2 x	12.000 x	30,000 €	480,000	67%	33%
UA	Unauthorised Activities	2 x	0.150 x	1,226,667 €	368,000	17%	83%
MA	Management	5 x	0.480 x	112,917 €	271,000	58%	42%
RR	Reconciliation & Reporting	4 x	14.275 x	673 €	38,400	92%	8%
ES	Ext. Services	2 x	3.500 x	8,429 €	66,000	67%	33%
EC	Ext. Criminal Activ.	0 x	-- x	-- €	--	--%	--%
CA	Catastrophes	4 x	0.090 x	2,300,000 €	276,000	17%	83%
					Σ 2,071,900		

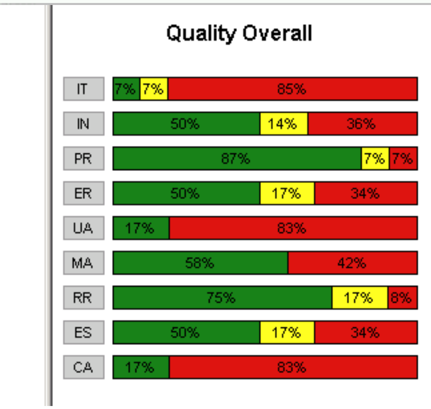
Technology: [illegible]
Personnel: [illegible] Unintentional Errors, [illegible] Unauthorised Activities
Organisation: [illegible] Management [illegible] Reconciliation & Reporting
External Factors: External Services including Outsourcing, Controls against External Criminal Activities, Precaution for Catastrophes

Potential Loss Severity (€)	10,000 - 49,999	50,000 - 249,999	250,000 - 999,999	1,000,000 - 10,000,000
Potential Loss Frequency (p.a.)	0.10 - 0.99	1.00 - 11.99	12.00 - 51.99	52.00 - 250.00

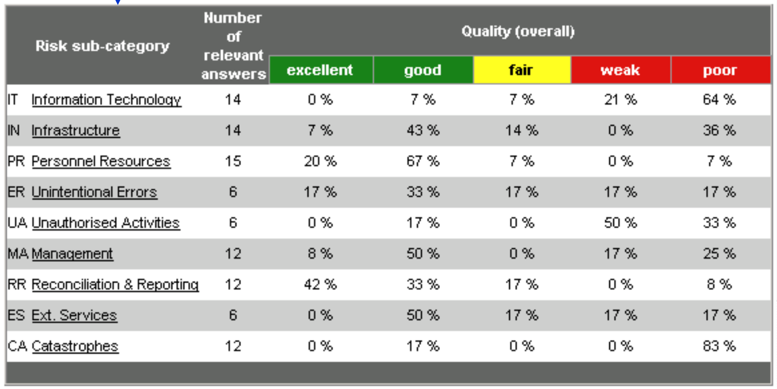
*acceptable = [excellent, good, fair]
weak = [weak, poor]

Dimensions:

- Organisational part
- Risk factor
- Nb relevant scenarios
- Potential loss frequency
- Potential loss severity
- Standard risk cost
- Quality of risk factor



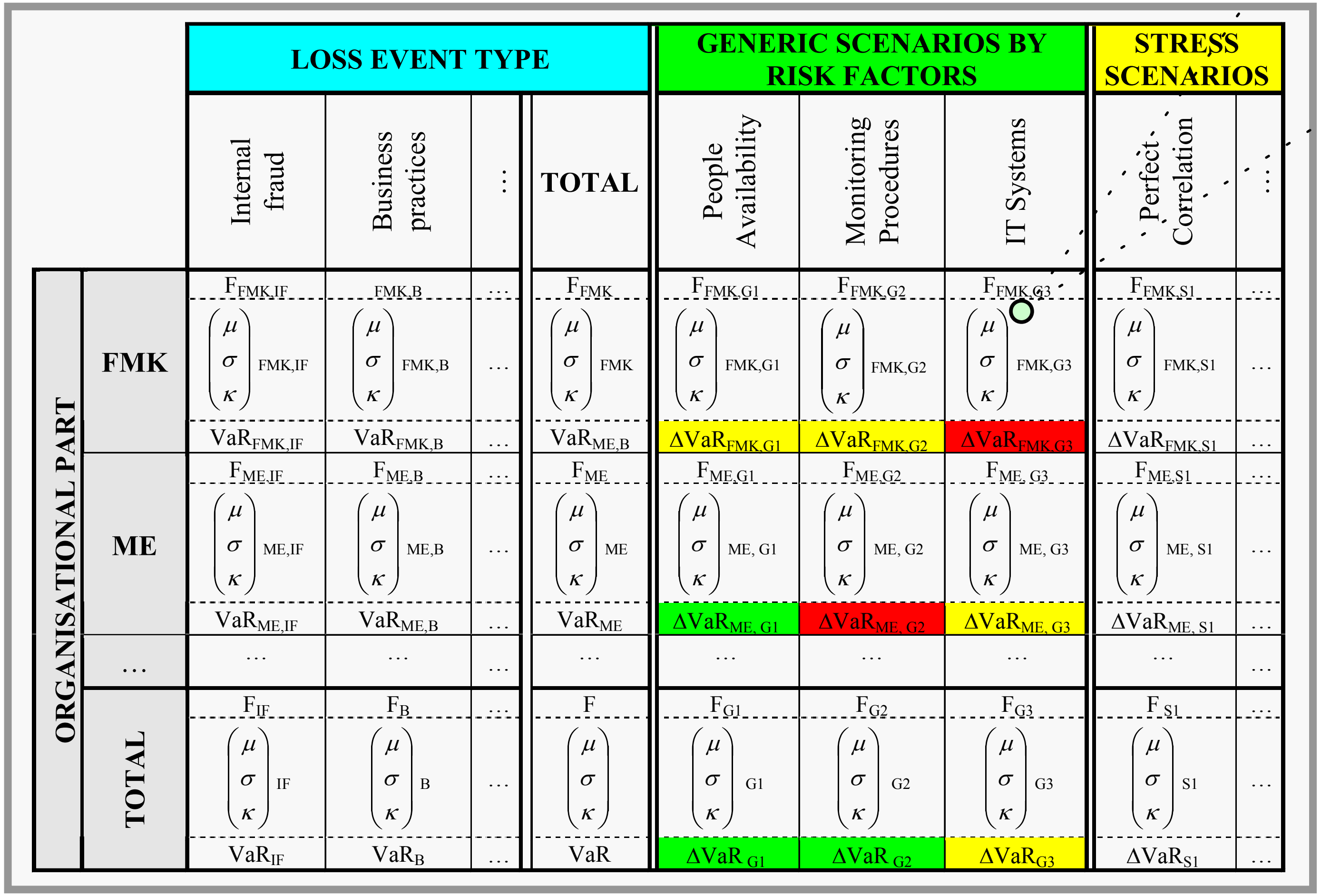
Quality Overall



Risk sub-category		Number of relevant answers	Quality (overall)				
			excellent	good	fair	weak	poor
IT	Information Technology	14	0 %	7 %	7 %	21 %	64 %
IN	Infrastructure	14	7 %	43 %	14 %	0 %	36 %
PR	Personnel Resources	15	20 %	67 %	7 %	0 %	7 %
ER	Unintentional Errors	6	17 %	33 %	17 %	17 %	17 %
UA	Unauthorised Activities	6	0 %	17 %	0 %	50 %	33 %
MA	Management	12	8 %	50 %	0 %	17 %	25 %
RR	Reconciliation & Reporting	12	42 %	33 %	17 %	0 %	8 %
ES	Ext. Services	6	0 %	50 %	17 %	17 %	17 %
CA	Catastrophes	12	0 %	17 %	0 %	0 %	83 %

FORTIS

- A group-wide operational risk report is built each quarter.



		LOSS EVENT TYPE				GENERIC SCENARIOS BY RISK FACTORS			STRESS SCENARIOS	
		Internal fraud	Business practices	⋮	TOTAL	People Availability	Monitoring Procedures	IT Systems	Perfect Correlation	⋮
ORGANISATIONAL PART	FMK	$F_{FMK,IF}$	$_{FMK,B}$	…	F_{FMK}	$F_{FMK,G1}$	$F_{FMK,G2}$	$F_{FMK,G3}$	$F_{FMK,S1}$	…
		$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,IF}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,B}$	…	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,G1}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,G2}$	○ $\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,G3}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{FMK,S1}$	…
		$VaR_{FMK,IF}$	$VaR_{FMK,B}$	…	$VaR_{ME,B}$	🟨 $\Delta VaR_{FMK,G1}$	🟨 $\Delta VaR_{FMK,G2}$	🟥 $\Delta VaR_{FMK,G3}$	$\Delta VaR_{FMK,S1}$	…
	ME	$F_{ME,IF}$	$F_{ME,B}$	…	F_{ME}	$F_{ME,G1}$	$F_{ME,G2}$	$F_{ME, G3}$	$F_{ME,S1}$	…
		$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME,IF}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME,B}$	…	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME, G1}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME, G2}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME, G3}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME, S1}$	…
		$VaR_{ME,IF}$	$VaR_{ME,B}$	…	VaR_{ME}	🟩 $\Delta VaR_{ME, G1}$	🟥 $\Delta VaR_{ME, G2}$	🟨 $\Delta VaR_{ME, G3}$	$\Delta VaR_{ME, S1}$	…
	…	…	…	…	…	…	…	…	…	…
	TOTAL	F_{IF}	F_{B}	…	F	F_{G1}	F_{G2}	F_{G3}	F_{S1}	…
		$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{IF}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{B}$	…	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{G1}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{G2}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{G3}$	$\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{S1}$	…
		VaR_{IF}	VaR_{B}	…	VaR	🟩 ΔVaR_{G1}	🟩 ΔVaR_{G2}	🟨 ΔVaR_{G3}	ΔVaR_{S1}	…

Potential loss frequency profile : $F_{ME,G1}$

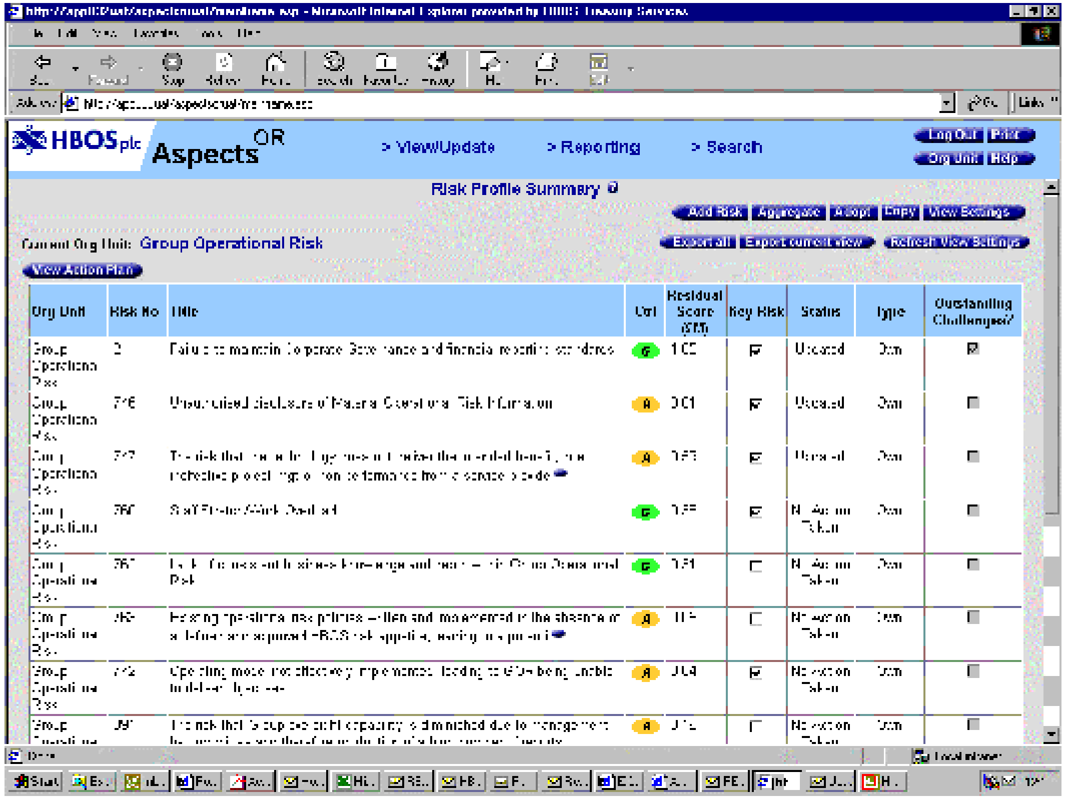
Potential loss severity profile : $\begin{pmatrix}\mu\\\sigma\\\kappa\end{pmatrix}_{ME, G1}$

Potential impact on VaR : $\Delta VaR_{ME, G1}$

- Scenarios are used for the calculation of sensitivity (ΔVaR) to non-availability of a risk resource.
- Although scenarios are used in the operational risk management process, they do not contribute directly to the calculation of economic capital, which is performed on the basis of loss data with defined qualitative adjustment

Halifax Bank of Scotland

- Tailorable summary views in AspectsOR for users (dummy example shown below).
- Automated paper based reporting generated around risk categories, business units, action plans etc.

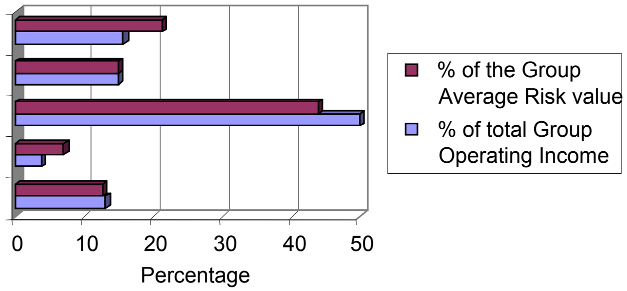


Risk Profile Summary

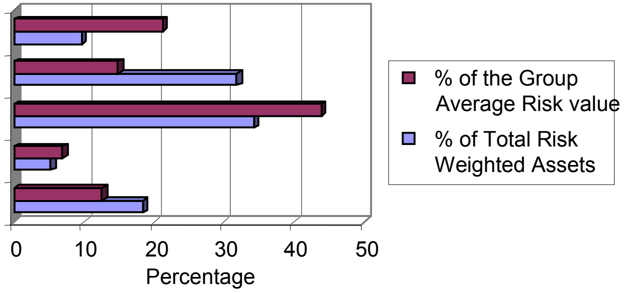
Current Org Unit: Group Operational Risk

Org Unit	Risk No	Title	Ctrl	Residual Score (£M)	Key Risk	Status	Type	Outstanding Challenges?
Group Operational Risk	2	Failure to maintain Corporate Governance and financial reporting standards	G	[illegible]	☑	[illegible]	Own	☑
Group Operational Risk	[illegible]	Unauthorised disclosure of Material Operational Risk Information	A	[illegible]	☑	[illegible]	Own	☐
Group Operational Risk	[illegible]	The risk that [illegible]	A	[illegible]	☑	[illegible]	Own	☐
Group Operational Risk	[illegible]	Staff Pressure/Work Overload	G	[illegible]	☑	No Action Taken	Own	☐
Group Operational Risk	[illegible]	Lack of [illegible] business knowledge and [illegible] Group Operational Risk	G	[illegible]	☐	No Action Taken	Own	☐
Group Operational Risk	[illegible]	Existing operational risk policies written and implemented in the absence of a defined and approved HBOS risk appetite, [illegible]	A	[illegible]	☐	No Action Taken	Own	☐
Group Operational Risk	[illegible]	Operating model not effectively implemented leading to GOR being unable to deliver [illegible]	A	[illegible]	☑	No Action Taken	Own	☐
Group Operational Risk	[illegible]	The risk that [illegible] capacity is diminished due to management [illegible]	A	[illegible]	☐	No Action Taken	Own	☐

Comparison between total average value and total operating income by Division

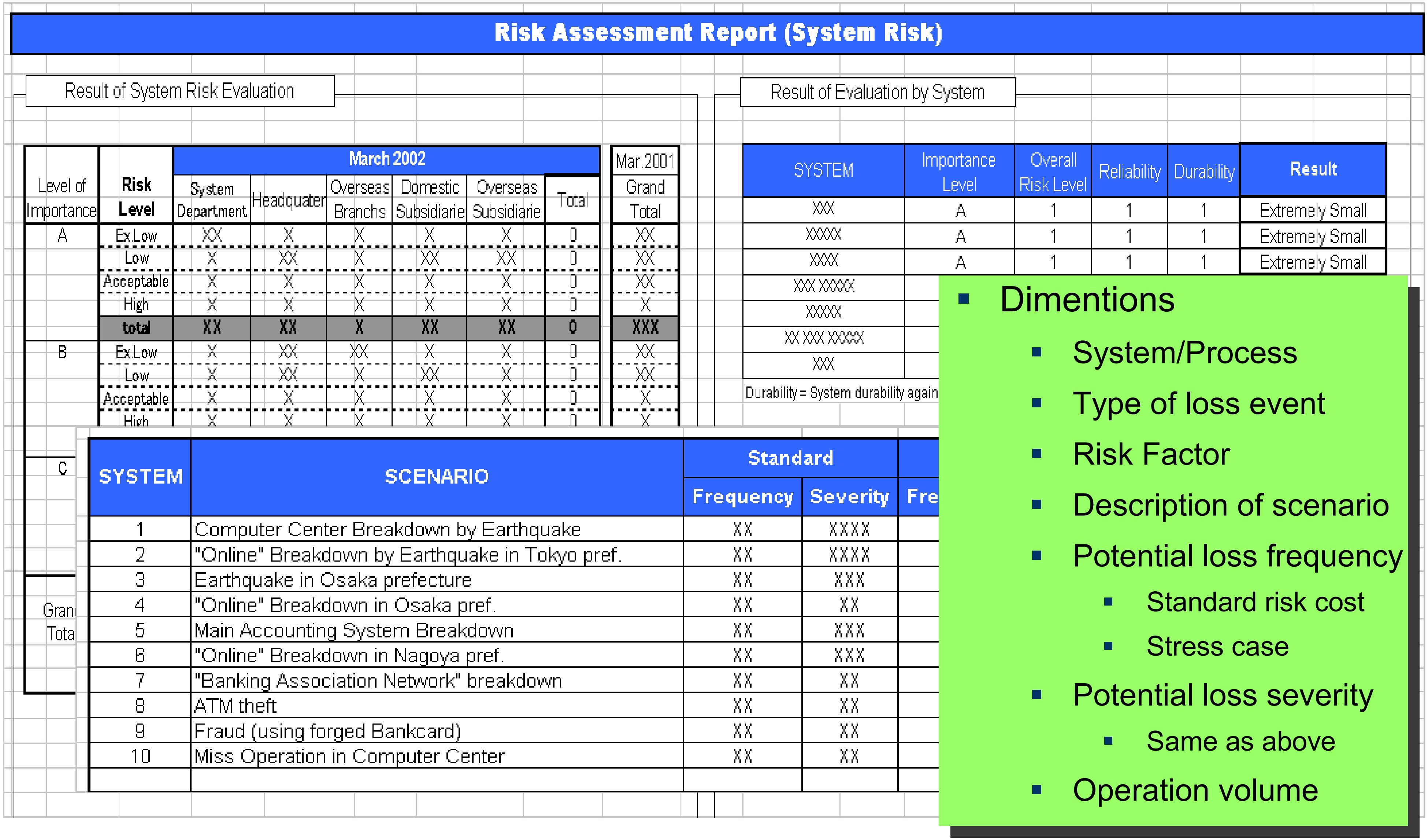


Comparison between total average risk and total risk weighted assets by Division



- A Group-wide operational risk report is produced semi annually for the Board and Audit Committee. Results from the scenario exercise are used with other OR information including losses, project risk data etc.
- Comparisons drawn against other operating measures (dummy example shown above).

UFJ Holdings, Inc.



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								
Gran Tota								

Result of Evaluation by System

SYSTEM	Importance Level	Overall Risk Level	Reliability	Durability	Result
XXX	A	1	1	1	Extremely Small
XXXXX	A	1	1	1	Extremely Small
XXXX	A	1	1	1	Extremely Small
XXX XXXXX					
XXXXX					
XX XXX XXXXX					
XXX					

Durability = System durability again

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

- Dimentions
  - System/Process
  - Type of loss event
  - Risk Factor
  - Description of scenario
  - Potential loss frequency
    - Standard risk cost
    - Stress case
  - Potential loss severity
    - Same as above
  - Operation volume

What distributional assumptions are you making in your risk capital model?

Choice of distributions and qq-plots

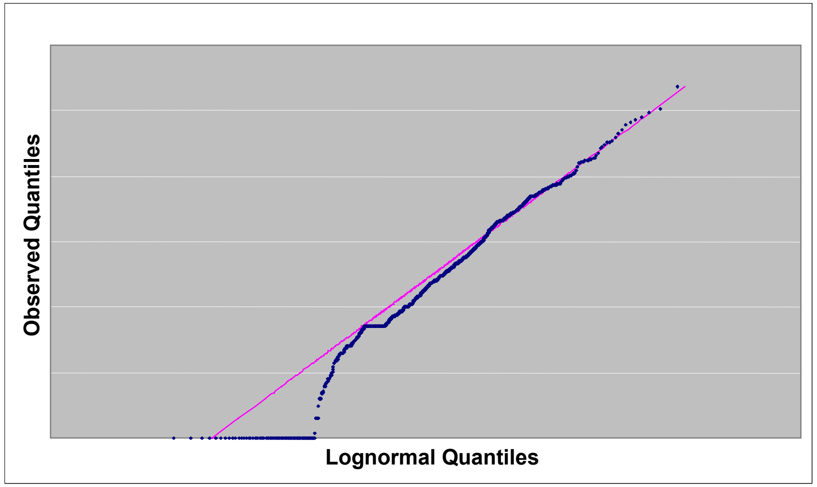
Severity distributions:

- *Lognormal:* Credit Lyonnais, Dresdner Bank HBOS
- *Normal Gamma:* Fortis, Dresdner Bank
- *Others, e.g. Gumbel, Weibull, Frechet:* Banca Intesa, Halifax Bank of Scotland

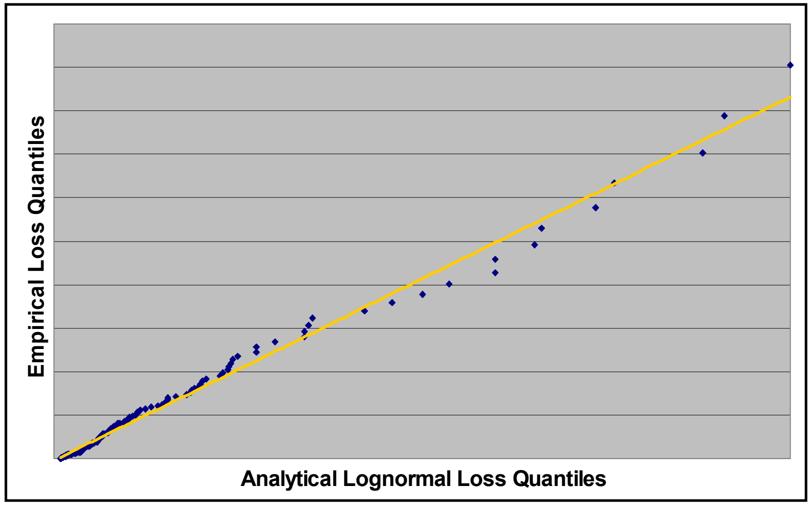
Frequency distributions:

- *(Negative) Binomial distribution:* Dresdner Bank, Fortis
- *Poisson*:* Banca Intesa, Credit Lyonnais, Dresdner Bank, UFJ Holdings

Dresdner Bank: qq-plot for OR losses



HBOS: qq-plot for OR losses > £ 10,000


Empirical Loss Quantiles
Analytical Lognormal Loss Quantiles