BASEL COMMITTEE ON BANKING SUPERVISION

BANK FOR INTERNATIONAL SETTLEMENTS

4 June 2002

Operational Risk Data Collection Exercise - 2002

In May 2001, the Basel Committee on Banking Supervision launched a survey of banks' operational risk data. In a repeat of this exercise, the Committee is now seeking to collect detailed data from the banking sector on operational risk for the most recent financial year (2001). The data collection exercise will include information on banks' operational risk losses and various 'exposure indicators', and will enable the Committee to further refine the calibration of the operational risk charge proposed for the New Basel Accord.

The Committee is providing banks with spreadsheets outlining the operational risk information requested as well as detailed instructions to assist banks in completing the survey. Banks are asked to complete and return the survey, via national supervisors, by 31 August 2002.[1]

Please note that all data received will be treated with complete confidentiality. The Committee intends to provide feedback to the industry on the results of the survey. However, this will be done on a basis that avoids any disclosure of individual bank data.

Background

The Committee's paper *Working Paper on the Regulatory Treatment of Operational Risk* published in September 2001 provides an overview of the proposed framework for the regulatory capital charge for operational risk.[2] In the working paper, the Committee outlines proposals for the development of a capital charge to cover operational risk. In the proposals there are three approaches of increasing sophistication to assess the operational risk charge: the Basic Indicator Approach, the Standardised Approach and the Advanced Measurement Approaches (AMA).

As part of the second quantitative impact survey, the Committee conducted its first survey of operational risk data in May 2001.[3] The data collected in that survey and in this current exercise will allow for the further calibration of the Basic Indicator and Standardised Approaches, and will inform the development of the AMA framework, in particular, resolving issues concerning the qualifying criteria for the AMA. The Committee envisages that these surveys will be part of an on-going data programme undertaken over the next few years to further refine the calibration of the operational risk charge.

---

1 Some national supervisors may request data to be submitted to them in advance of the 31 August deadline.

2 The September 2001 Working Paper on operational risk updated proposals set out in the Committee's second consultative package on the New Basel Capital Accord, published in January 2001.

3 See http://www.bis.org/bcbs/qisoprisk.htm. The results of this survey were published in the paper *The Quantitative Impact Survey for Operational Risk: Overview of Individual Loss Data and Lessons Learned.*

The 2002 survey

The primary purpose of this survey is to collect granular (event-by-event) operational risk loss data to help the Committee determine the appropriate form and structure of the AMA. To facilitate the collection of comparable loss data at both the granular and aggregate levels across banks, the Committee is again using its detailed framework for classifying losses. In the framework, losses are classified in terms of a matrix comprising *eight standard business lines* and *seven loss event categories.* These seven event categories are then further divided into 20 sub-categories and the Committee would like to receive data on individual loss events classified at this second level of detail if available.

The Committee is also collecting information on six “exposure indicators” such as number of employees or total assets. The exposure indicator data serve two purposes. First, they are critical to the Committee’s effort to aggregate loss data across banking institutions to arrive at an industry loss distribution. Second, the exposure indicators are necessary for banks and supervisors to relate historical loss experience to the current level of business activity. This information also enables banks and supervisors to determine separate frequency and severity distributions for the operational risk loss experience. Although indicators other than gross income are included in this survey, the Committee does not envision revisiting the use of gross income as the base for the Basic Indicator and Standardised Approaches.

The survey aims to collect data for the financial year 2001 and banks are asked to complete as much of the survey as possible on a best endeavours basis.

Changes to the previous survey

Although this survey is a repeat of an exercise carried out last year, there are a number of important changes to the scope and content of this year’s survey. These include:

- Banks are no longer asked to provide operational risk loss data by ‘effect types’,
- Banks are no longer asked to provide quarterly aggregated loss data,
- Banks are asked to provide data on *expected* as well as *received* recoveries,
- Banks are asked to indicate the internal threshold used for collecting loss data,
- Banks are asked to identify those losses arising from a ‘corporate centre’ business,
- Banks are no longer asked to provide data on the value of transactions/deals/trades, the number of transactions/deals/trades, the standard deviation of transactions/deals/ trades, the number of accounts and the average balance of accounts,
- Banks are asked to provide component information on gross income,
- Simplified, structured Excel spreadsheets have been developed for completing this year’s survey. These spreadsheets include a number of tests to check the consistency of data submitted and thus reduce the need for further enquiries after data are submitted. It is therefore important that banks do not change the design or structure of the questionnaire and check the messages of these tests.

The Committee appreciates that this exercise is a burden on banks. However, it believes, that its proposals will have increased accuracy and risk sensitivity where they are based on a sound quantitative foundation. The data requested are of fundamental importance to the development of the operational risk charge and the calibration of the overall capital framework, and to the extent that more accurate and complete data are received then the need for buffers or adjustments for uncertainty is reduced.

Operational Risk Data Collection Exercise –Annexes

Annex 1: Example mapping of business lines

Business Unit	Business lines		Activity Groups
	Level 1	Level 2	
INVESTMENT BANKING	Corporate Finance	Corporate Finance	Mergers and Acquisitions, Underwriting, Privatisations, Securitisation, Research, Debt (Government, High Yield) Equity, Syndications, IPO, Secondary Private Placements
		Municipal/Government Finance	
		Merchant Banking	
		Advisory Services	
	Trading & Sales	Sales	Fixed Income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
		Market Making	
		Proprietary Positions	
		Treasury	
BANKING	Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
		Private Banking	Private lending and deposits, banking services, trust and estates, investment advice
		Card Services	Merchant/Commercial/Corporate cards, private labels and retail
	Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lends, guarantees, bills of exchange
	Payment and Settlement[1]	External Clients	Payments and collections, funds transfer, clearing and settlement
	Agency Services	Custody	Escrow, Depository Receipts, Securities lending (Customers) Corporate actions
		Corporate Agency	Issuer and paying agents
		Corporate Trust	
OTHERS	Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
		Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
	Retail Brokerage	Retail Brokerage	Execution and full service

[1] Payment and settlement losses related to a bank's own activities would be incorporated in the loss experience of the affected business line.

Annex 2: Loss event type classification

Operational risk event: Any occurrence specified in Table 1 below, which gives rise to one or more of the loss effects set out above and explained in Table 2 below. Every individual event shall be separately reported, subject to the guidance specified below:

‘Internal fraud’: multiple dishonest/fraudulent acts committed by the same employee and categorised in the same level 2 category shall be counted as a single event.

‘External fraud’: multiple criminal acts committed by the same person/party and categorised in the same level 2 category shall be counted as a single event. A series of losses involving unidentified person/party but arising from the same method of operation shall be deemed to involve the same person/party.

‘Employment Practices and Workplace safety’ and ‘Clients, Products & Business practices’: claims, litigation and payments of restitution arising from the same cause shall be counted as a single event.

‘Damage to physical assets’: two or more natural hazards (i.e. earthquake, typhoon, hurricane, windstorm, flood etc) which occurred within 72 hours, shall be deemed as a single event except in the case where the affected areas do not coincide entirely.

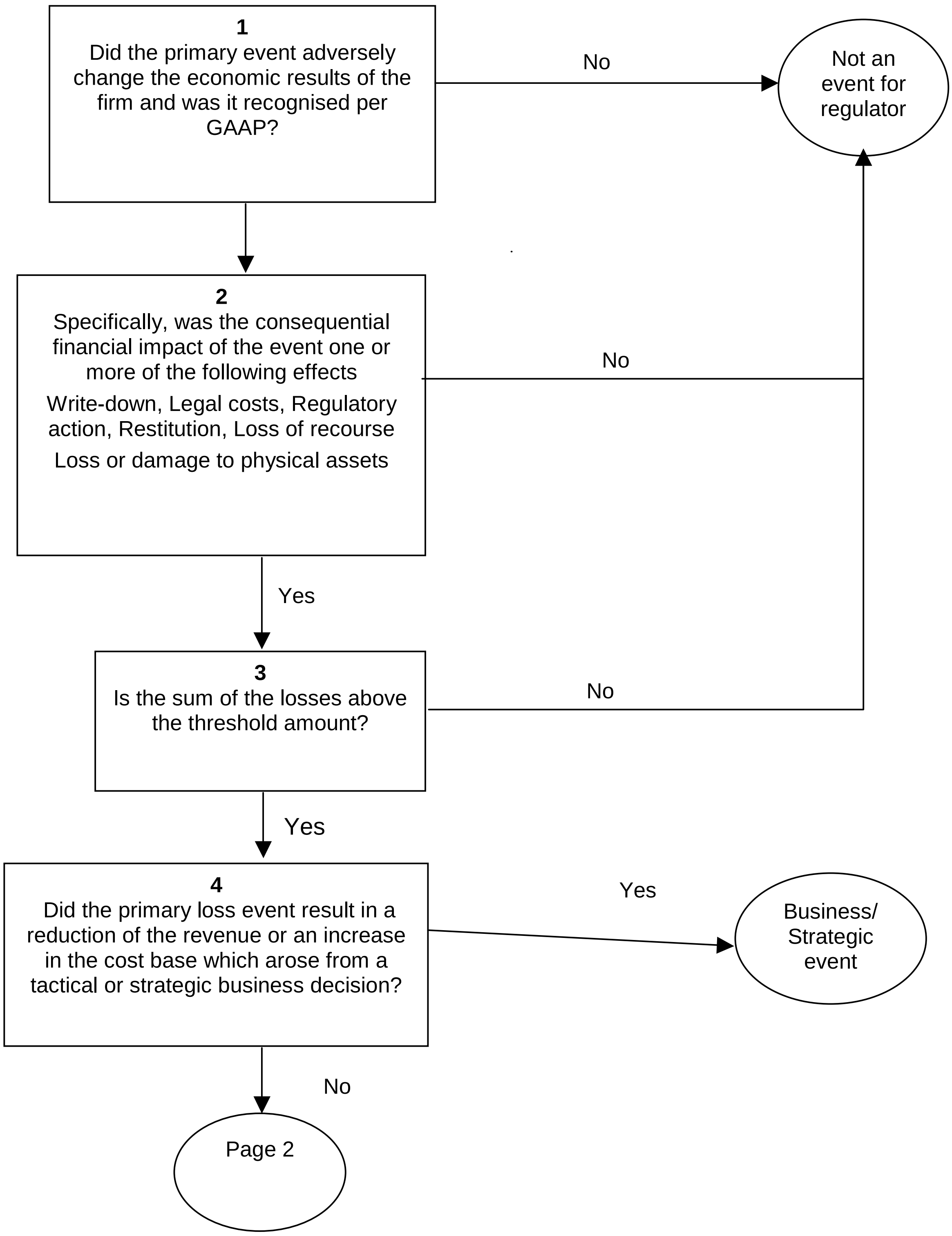
‘Business disruption and system failure’: any one event or a series of event resulting from the same cause (e.g. mechanical breakdown of the same parts, error in the specific program) shall be deemed as a single event.

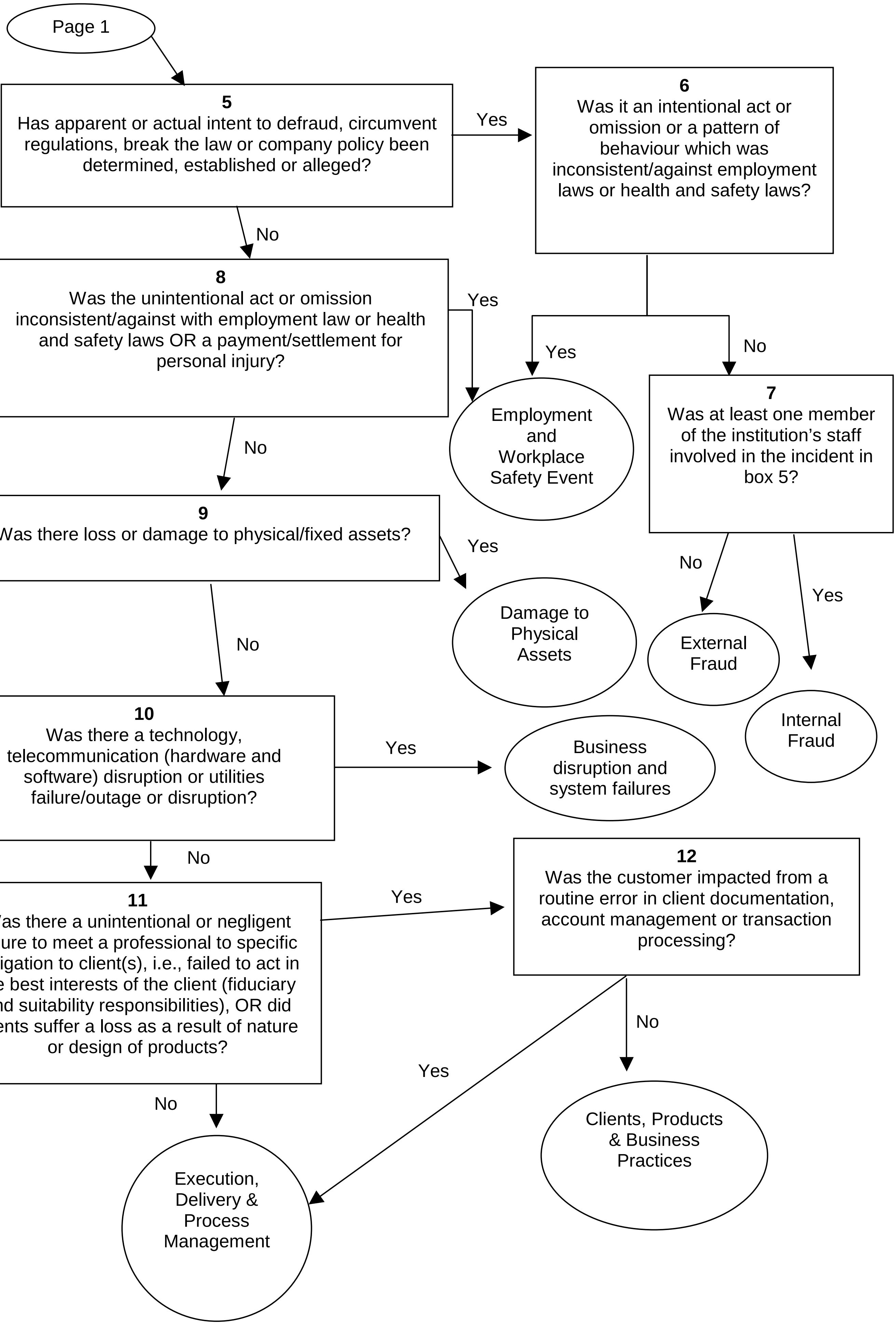
Table 1: Loss event type classification

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	Unauthorised Activity	Transactions not reported (intentional) Trans type unauthorised (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (wilful) Bribes / kickbacks Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail consumer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender Liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorised, etc.) Model errors

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing Vendor disputes

Table 2: Decision trees to determine event categorisation




Page 1
5
Has apparent or actual intent to defraud, circumvent regulations, break the law or company policy been determined, established or alleged?
Yes
6
Was it an intentional act or omission or a pattern of behaviour which was inconsistent/against employment laws or health and safety laws?
No
8
Was the unintentional act or omission inconsistent/against with employment law or health and safety laws OR a payment/settlement for personal injury?
Yes
Yes
No
Employment and Workplace Safety Event
7
Was at least one member of the institution's staff involved in the incident in box 5?
No
9
Was there loss or damage to physical/fixed assets?
Yes
No
Yes
Damage to Physical Assets
External Fraud
No
Internal Fraud
10
Was there a technology, telecommunication (hardware and software) disruption or utilities failure/outage or disruption?
Yes
Business disruption and system failures
No
11
Was there a unintentional or negligent failure to meet a professional to specific obligation to client(s), i.e., failed to act in the best interests of the client (fiduciary and suitability responsibilities), OR did clients suffer a loss as a result of nature or design of products?
Yes
12
Was the customer impacted from a routine error in client documentation, account management or transaction processing?
No
Yes
Clients, Products & Business Practices
No
Execution, Delivery & Process Management