Response to Consultation Paper on Draft Regulatory Technical Standards (RTS)

EBA/CP/2024/13

Introduction

In June 2006 the Basel Committee on Banking Supervision (BCBS) introduced a regulatory-prescribed taxonomy (the Basel Taxonomy[1]) for operational risk management built around seven event type categories as part of Basel II, formally known as International Convergence of Capital Measurement and Capital Standards, for globally active banks. In the intervening period our understanding of operational risk and its management has increased significantly, and the Basel event type taxonomy has played a crucial role in this.

Almost all banks capture and report operational risk loss event data according to the Basel taxonomy level 1 event types. Some firms supplement this with bespoke categories at a second level for internal management reporting purposes. Furthermore, most firms within the remit of the Single Supervisory Mechanism that use models, applying AMA methodologies, for Pillar 1 AMA or Pillar 2 ICAAP purposes, use the Basel taxonomy as the basis for unit of measure selection.

This response to your consultation paper focuses on Question 1 "*do you think that the granularity of and the distinction between the different Level 2 categories is clear enough? If not, please provide a rationale*". It leverages analysis undertaken on mapping the newly proposed EBA level 2 categorisations to existing Basel level 2 and level 3 categories and my 25+ years of experience working in this area of operational risk management.

A specified objective for the RTS is to "*maintain alignment with the current practices of most institutions, built on level 1 event types and level 2 categories, which retain their quality of being mutually exclusive and collectively exhaustive*". However, my analysis has found causal factors and control failures have been introduced as stand-alone level 2 categories, which will by definition present challenges in meeting this defined objective.

A number of good enhancements have been made the taxonomy. However, there are a few recommendations:

- Remove any EBA2 categories that are either causal factors or control failures. This does not mean these risks are not important. Rather they should be captured through a different taxonomy.
- Simplify and reduce the number of proposed EBA2 categories, but merging some and using flags if it is important to supervisors to capture specific information on those previously identified categories, to identify losses falling in these categories.

Respondent

Jonathan Humphries is the Head of Risk Advisory, Financial Institutions – Europe, at Howden Insurance Broking Limited (part of Howden Group Holdings), and has worked in the fields of operational risk, cyber, risk governance and insurance alignment for over 25 years, using scenario and capital modelling approaches to help firms and their boards better mitigate and manage volatility, and optimise their investment in risk to minimise costs, using risk data analysis (losses, scenarios, risk indicators, …). Jonathan has built, validated or replicated over 50 operational risk capital models globally, including for many systemically important banks. With extensive experience in structured scenario analysis to create a forward-looking view of a firm's risk profile.

Jonathan has also contributed to a number of technical research papers, which include: an investigation of cyber loss data and its links to operational risk, Journal of Operational Risk 14(3), 1–25, March 2019; estimating the probability of insurance recovery in operational risk, Journal of Operational Risk 19(1), 1–15, February 2024; and integrating internal and external loss data via an equivalence principle, Journal of Operational Risk 19(2), 1-24, June 2024.

All views expressed in this response are his own, rather than those of Howden.

[1] https://www.bis.org/publ/bcbs128pdf

OPERATIONAL RISK TAXONOMIES

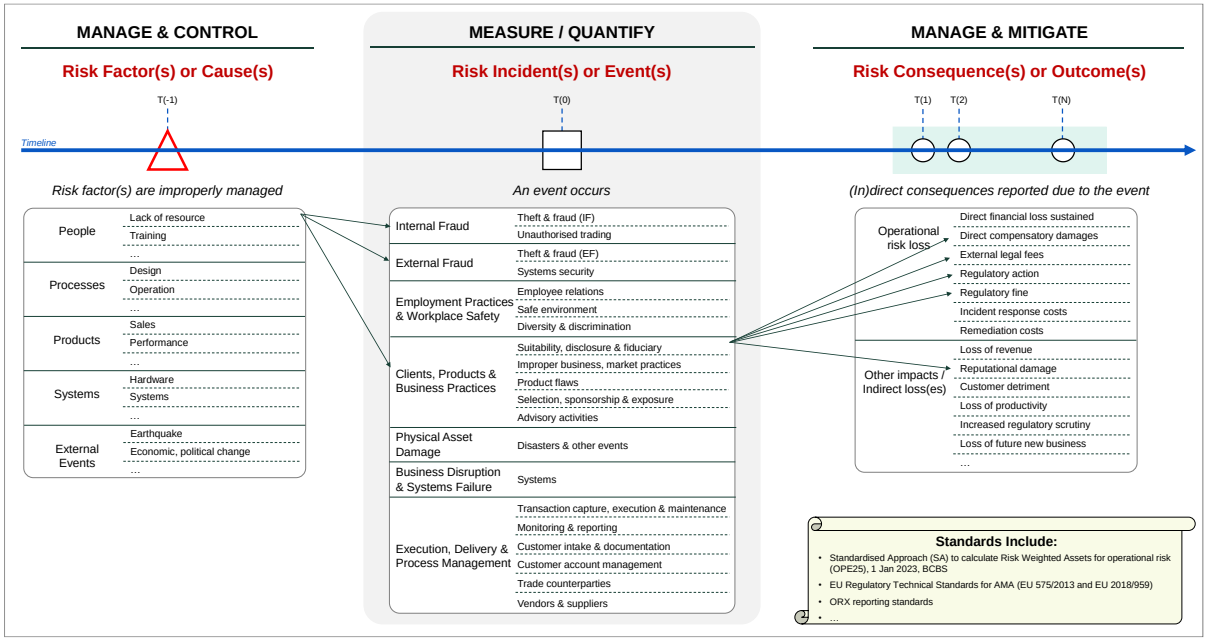
A risk taxonomy, which is a hierarchical classification scheme used to put risks into different buckets, is used for risk reporting, risk analysis, risk quantification and capital modelling. It is typically built around a tree-like structure, whereby high-level risks are decomposed into more specific manifestations. In financial institutions, risks can be broadly categorised into buckets of credit, underwriting / reinsurance (insurance), operational, market, liquidity, investment, pension and business / strategic.

A sound risk taxonomy is an essential starting point for any risk framework. It is the basis for interrelating different datasets, such as historical losses, risk indicators, loss scenarios, and more, … But how should a taxonomy, or taxonomies, be structured? In operational risk management, taxonomies can be applied to event types, processes, controls, products, …

How should these be structured and interact? What role does each have?

Figure 1 uses the Basel taxonomy to illustrate the role of an event type classification taxonomy in a firm's operational risk management framework, providing the vital role of enabling loss quantification.

Figure 1: Bow tie illustrating the inter-relationship between Causes, Events and Outcomes



Before considering specific taxonomies, it is worth noting certain characteristics of operational risks. A single "*Risk Factor or Cause*" can result in multiple "*Risk Incidents or Events*"; and a single "*Risk Incident or Event*" can result in multiple "*Risk Consequences or Outcomes*". Figure 1 shows that: "*Risk Factor(s) or Cause(s)*" can be managed and controlled; "*Risk Incident(s) or Event(s)*" can be quantified and measured through a "*Risk Consequence or Outcome*", typically in the form of a financial loss; and "*Risk Consequence(s) or Outcome(s)*" can be managed and mitigated.

Conversely, it is difficult to measure "*Risk Factor(s) or Cause(s)*" without first capturing and recording a (loss) event. Likewise, "*Risk Consequence(s) or Outcome(s)*" are difficult to quantify without first capturing and recording a (loss) event. These are important considerations to take into account when designing and defining risk taxonomies.

"*Risk Factors and Causes*" also influence the frequency of event occurrence, the severity of individual losses and the (in)effectiveness of controls.

Building an event type taxonomy

A critical building block in a firm's risk framework to enable risk quantification is a "*Risk Event Type Taxonomy*", which does not mix causal, outcomes, control mitigation categories. Whilst there are some challenges with the existing Basel taxonomy (Figure 2), it has proven over time to largely be effective when focussing on event types, which can be measured.

In most jurisdictions these Basel event types have been adopted by banks, and more broadly by the financial services industry, as the foundation for: the collection and reporting of loss events often

applying the level 3 event types; and the design and selection of units of measurement for risk and capital modelling purposes. Although some firms, most notably in the UK, elected to divert from this classification framework and adopt bespoke taxonomies.

Figure 2: The Basel 2 event types

Level 1	Level 2	Level 3
Internal fraud (IF)	Theft and fraud (IF)	Fraud / credit fraud / worthless deposits; Theft / extortion / embezzlement / robbery; Misappropriation of assets; Malicious destruction of assets; Forgery (IF); Check kiting (IF); Smuggling; Account take-over / impersonation / etc.; Tax non-compliance / evasion (wilful); Bribes / kickbacks; Insider trading (not on firm's account).
	Unauthorised activity	Transactions not reported (intentional); Transaction type unauthorised (w/monetary loss); and Mismarking of position (intentional).
External fraud (EF)	Systems security	Hacking damage; and Theft of information (w/monetary loss).
	Theft & fraud (EF)	Theft / Robbery; Forgery (EF); and Check kiting (IF).
Employment practices & workplace safety (EPWS)	Diversity & discrimination	All discrimination types.
	Employee relations	Compensation, benefit, termination issues; and Organised labour activity.
	Safe environment	General liability (slip and fall, etc.); Employee health & safety rules events; and Workers compensation.
Clients, products & business practices (CPBP)	Advisory activities	Disputes over performance of advisory activities
	Improper business or market practices	Antitrust; Improper trade / market practices; Market manipulation; Insider trading (on firm's account); Unlicensed activity; and Money laundering.
	Product flaws	Product defects (unauthorised, etc.); and Model errors.
	Selection, sponsorship & exposure	Failure to investigate client per guidelines; and Exceeding client exposure limits.
	Suitability, disclosure & fiduciary	Fiduciary breaches / guideline violations; Suitability / disclosure issues (KYC, etc.); Retail customer disclosure violations; Breach of privacy; Aggressive sales; Account churning; and Misuse of confidential informationLender liability.
Damage to physical assets (DPA)	Disasters & other events	Natural disaster losses; and Human losses from external sources (terrorism,vandalism).
Business disruption & systems failure (BDSF)	Systems	Hardware; Software; Telecommunications; and Utility outage / disruptions.
Execution, delivery & process management (EDPM)	Customer account management	Unapproved access given to accounts; Incorrect client records (loss incurred); and Negligent loss or damage of client assets.
	Customer intake and documentation	Client permissions / disclaimers missing; and Legal documents missing / incomplete.
	Monitoring and reporting	Failed mandatory reporting obligation; and Inaccurate external report (loss incurred).
	Trade counterparties	Non-client counterparty mis-performance; and Misc. non-client counterparty disputes.
	Transaction capture, execution & maintenance	Miscommunication; Data entry, maintenance or loading error; Missed deadline or responsibility; Model / system mis-operation; Accounting error / entity attribution error; Other task mis-performance; Delivery failure; Collateral management failure; and Reference Data Maintenance.
	Vendors & suppliers	Outsourcing; and Vendor disputes.

In 2007, ORX published its Operational Risk Reporting Standards to describe the standards for the reporting of operational risk losses for consolidation and analysis in the ORX global database by members of ORX. These standards set out in detail how losses contributing to ORX should be classified according to operational risk event type classifications, which map directly to the Basel 2 event types. The exception being "*trade counterparties and vendors/suppliers*", which are both in EDPM, where ORX concluded these categories should not be included within the data. The standards also define taxonomies for products, processes and business lines. It is worth noting that, as at 1 January 2024, the ORX consortia data comprised more than 1.1m loss events totalling €610bn, and with 82 banking

members contributing loss data in 2023. This data is unrivalled in scope, quantity and quality, providing a vital source of reference for risk benchmarking, quantification and modelling for many banking firms and the industry. However, the underlying framework for its categorisation is aligned to the Basel event types and levels 1 and 2. I would anticipate future use of this data to be dependent on being able to feed it into any new taxonomy framework.

The banking industry's proliferation of conduct-related losses, as a result of misbehaviour that led to the global financial crisis of 2007/8. This, coupled with the emergence of cyber, financial crime, ESG and other risks as a real concern, and the BCBS's decision to implement new rules for setting pillar 1 capital for operational risk under Basel 4 (anticipated to be effective from 1 Jan 2025 in most jurisdictions), has led to the emergence of risk categorisations that are often referred to as Management or Non-Financial Risk Categories.

These new risk taxonomies for operational risk have created both opportunities and challenges. The opportunity being that risk information and data can be presented to senior management and stakeholders in a form easier to understand. Challenges include risk overlaps and a failure to achieve the objective of being mutually exclusive – something that, based on my analysis, will also prevail under the EBA's proposed level 2 event types. For example, a model/system mis-operation could be categorised as both "*IT failures related to management of transactions*" and "*model implementation and use*"; or concealing losses could be categorised as both an "*internal fraud committed against other stakeholders*" or an "i*nternal fraud committed against the institution*". These challenges are important factors that need to be overcome for risk reporting, risk governance and Pillar 2 capital calculation.

The EBA operational risk taxonomy

The consultation paper states that the EBA has elected to develop a risk taxonomy "*with the aim of maintaining alignment with the current practices of most institutions, built on level 1 event types and level 2 categories, which retain their quality of being mutually exclusive and collectively exhaustive*". The EBA is planning to retain use of the Basel taxonomy's seven level 1 event types (BET1) but has proposed 38 new level 2 (EBA2) categorisations (see figure 5) to be used instead of those set out in Basel. There is no mention of a third level. It has then identified a list of flags representing risk attributes that cannot be easily captured through the event type dimension (e.g. large loss event; legal risk – misconduct; model risk; ICT risk; governance risk; ...).

Performing an analysis to assess how Basel level 3 event types (BET3) map into the EBA2 categories results in single BET3 categories mapping to multiple EBA2 categories (see Figure 6). Thus, suggesting the new EBA2 are not all "*mutually exclusive and collectively exhaustive*" – see categories highlighted in red in figure 5.

Four EBA2 categories (shown in red font in figure 5) are not realistically event types:

- "*First, second and third-party fraud (EF)*" introduces a causal component into the classification of losses.
- "*Rights/obligation failures in preparation phase (CPBP)*" is most likely a causal factor or control failure, that can sit across multiple other event types
- "*Inadequate business continuity planning/event management (BDSF)*" is a control failure, which occurs after an underlying event.
- "*Improper distribution/marketing (EDPM)*" under Basel 2 would likely be categorised as a CPBP (Suitability, disclosure & fiduciary) and does not logically fit as an EDPM event type.
- "*Third party management failures (EDPM)*" is most likely a causal factor or control failure, that can sit across multiple other event types and is an operational resilience factor.

A more granular analysis has been undertaken on the proposed EBA2 categories to assess how the Basel level 3 event types (BET3), with some additional granularity might map into the EBA2 categories.

Figure 5: EBA proposed event type taxonomy

#	Level 1 (EBA1)	Level 2 (EBA2)
1	IF	(1) Bribery and Corruption; (2) Insider Trading not on institution's account; (3) Intentional mismarking; (4) Intentional money laundering and terrorism financing; (5) Intentional sanctions violation; (6) Internal fraud committed against other stakeholders; (7) Internal fraud committed against the institution; and (8) Malicious physical damage to employees, institution's physical assets and public assets.
2	EF	(1) Cyber-attacks; (2) Data theft and manipulation; (3) First party fraud; (4) Second party fraud; and (5) Third party fraud.
3	EPWS	(1) Inadequate Employment practice; and (2) Inadequate workplace safety
4	CPBP	(1) Accidental money laundering and terrorism financing; (2) Accidental sanctions violations; (3) Anti-trust / anticompetition; (4) Client mistreatment / failure to fulfil duties to customer; (5) Data privacy breach / confidentiality mismanagement; (6) Improper market practices, product and service design or licensing; (7) Insider Trading on institution's account; (8) Model / methodology design error; (9) Rights/obligation failures in preparation phase; and (10) Sale service failure
5	DPA	No categories suggested
6	BDSF	(1) Hardware failure not related to management of transactions; (2) Inadequate business continuity planning/event management; (3) Network failure not related to management of transactions; and (4) Software failure not related to management of transactions.
7	EDPM	(1) Client account mismanagement: (2) Data management; (3) Improper distribution/marketing; (4) IT failures related to management of transactions; (5) Model implementation and use; (6) Processing / execution failures; (7) Regulatory and tax authorities, including reporting; (8) Rights / obligation failures in execution phase; and (9) Third party management failures.

The results of this analysis are presented in Figure 6, where it can be seen that for:

- Mutual exclusivity – BET3 categories falling in multiple EBA2 categories are shown in red:
  - Is achieved for EPWS, DPA and BDSF
  - Is largely achieved for CPBP and EDPM, with the following exceptions: (i) CPBP, where "*guideline violations"* can fall in both "*sale service failure* and *accidental sanctions violations"*; and (iii) EDPM, where "M*odel or system mis-operation"* can fall in both "*IT failures related to management of transactions"* and "M*odel implementation and use"*.
  - In IF, many BET3 categories fall in multiple EBA2 categories.
  - In EF there are significant overlaps between "F*irst and second-party fraud*".
- Granularity of and the distinction between the different EBA2 categories:
  - IF: Certain EBA2 categories are much narrower than current BET2 categories, "*bribery and corruption*" and "*Intentional mismarking*" being good examples. Whilst other categories "*Internal fraud committed against other stakeholders*" and "*Internal fraud committed against the institution*" are much broader.
  - EF: At first glance EBA2 categories appear narrower in scope than BET2. However, the differentiation of "*First, second and third-party fraud*" introduces a causal component, which should be avoided in an event type taxonomy.
  - EPWS: Reduces the level of granularity that exists in BET2
  - CPBP: EBA2 categories are significantly different to BET2, providing greater granularity in certain cases (e.g. "*Accidental money laundering and terrorism financing*" and "*Anti-trust / anticompetition*") and less granularity in others (e.g. "*Client mistreatment / failure to fulfil duties to customer*" and "*Improper market practices, product and service design or licensing*").
- DPA: No EBA2 categories are proposed. This is one category where greater granularity could be considered to address emerging climate and social risks.
- BDSF: EBA2 categories provide greater granularity and broadly align with BET3 categories.
- EDPM: EBA2 categories provide greater granularity in certain cases (e.g. "*IT failures related to management of transactions*") and less granularity in others (e.g. "*Data management*"). The use of "*Third party management failures*" as an EBA2 continues to introduce a causal factor by way of losses caused by third parties.

It should be noted: "*Rights/obligation failures in preparation phase CPBP*" and "*Inadequate business continuity planning / event management (BDSF)*" **could not** be included in the Figure 6 analysis as they are control failures and no BET3 or BET2 categories can be mapped to them.

Figure 6: Mapping BET3 into EBA2 categories according to the EBA hierarchy

EBA1	EBA2	BET3	BET2
IF	Bribery and Corruption	Bribes / kickbacks	Theft and fraud (IF)
	Insider Trading not on institution's account	Insider Trading	
	Intentional sanctions violation	Bribes / kickbacks	
	Malicious physical damage to employees, institution's physical assets and public assets	Malicious destruction of assets	
	Internal fraud committed against other stakeholders	Account take-over / impersonation (IF); Cheque kiting (IF); Credit fraud (IF); Forgery (IF); Fraud (IF); Frontrunning; Misappropriation of assets; Theft / robbery (IF); Wire / electronic fraud; and Worthless deposits (IF)	
		Concealing losses; and Unauthorised fund transfer	Unauthorised activity
	Intentional mismarking	Intentional mismarking of position	
	Internal fraud committed against the institution	Concealing losses; Trading above limits / trading misdeeds; Transaction not reported (intentional); Transaction type unauthorised (with monetary loss); and Unauthorised fund transfer	
		Account take-over / impersonation (IF); Bribes / kickbacks; Cheque kiting (IF); Credit fraud (IF); Credit or debit card fraud (IF); Extortion (IF); Forgery (IF); Fraud (IF); Insider Trading; Misappropriation of assets; Money laundering (IF); Smuggling; Tax non-compliance / evasion (intentional); Theft / robbery (IF); Wire / electronic fraud; and Worthless deposits (IF)	Theft and fraud (IF)
		Manipulation of data; Computer hacking (IF); and Theft of information with monetary loss (IF)	Internal computer crime
EF	Cyber-attacks	Computer hacking (EF)	Systems security
	Data theft and manipulation	Theft of information with monetary loss (EF)	
	First party fraud	Account take-over / impersonation (EF); Cheque kiting (EF); Credit fraud (EF); Credit or debit card fraud (EF); Extortion (EF); Forgery (EF); Money laundering (EF); Theft / robbery (EF); Worthless deposits (EF); and Fraud (EF)	Theft and fraud (EF)
	Second party fraud	Account take-over / impersonation (EF); Cheque kiting (EF); Credit fraud (EF); Credit or debit card fraud (EF); and Forgery (EF)	
	Third party fraud	Fraud (EF)	
EPWS	Inadequate employment practice	All discrimination types; Harassment / hostile environment; and Libel, slander or defamation (EPWS)	Diversity and discrimination
		Breach of non-competition or restrictive trade agreement; Compensation; Employment benefits; Organised labour activity; and Termination issues	Employee relations
	Inadequate workplace safety	Employee health and safety rules event(s); General liability (slips, falls, …); and Workers compensation	Safe environment

EBA1	EBA2	BET3	BET2
CPBP	Accidental money laundering and terrorism financing	Money laundering (CPBP)	Improper business or market practices
	Anti-trust / anticompetition	Antitrust	
	Client mistreatment / failure to fulfil duties to customer	Account churning; Breach of contract	Suitability, disclosure and fiduciary
		Customer service denial; Disputes performance of advisory activities	Advisory activities
		Exceeding client exposure limits	Selection, sponsorship and exposure
		Libel, slander or defamation (CPBP)	Improper business or market practices
		Non-disclosure of sensitive issue	Suitability, disclosure and fiduciary
	Data privacy breach / confidentiality mismanagement	Breach of privacy; Misuse of confidential information; and Misuse of trade secrets	
	Improper market practices, product and service design or licensing	Corporate governance of client of FI; Corporate governance of FI; Improper advertising; Improper trade or market practices; Intellectual property violations; Market manipulation; Problem resulting from a merger or acquisition; and Unlicensed activity	Improper business or market practices
		Product defects (unauthorised, ...)	Product flaws
		Director or officer negligence	Suitability, disclosure and fiduciary
	Insider Trading on institution's account	Insider trading (on firm's account)	Improper business or market practices
	Model / methodology design error	Model errors	Product flaws
	Sale service failure	Failure to investigate client per guidelines	Selection, sponsorship and exposure
		Sales discrimination; and unlicenced activity	Improper business or market practices
		Aggressive sales; Conflict of interest; Errors and omissions; Fiduciary breaches; Lender liability; Retail consumer disclosure violations; Suitability, disclosure issues (e.g. Know Your Customers (KYC), ...); and Guideline violations	Suitability, disclosure and fiduciary
	Accidental sanctions violations	Guideline violations	
DPA	No Classification	Damage to property from intentional acts; Damage to property from terrorism; General property losses; Losses from defects in a building; and Natural disaster losses	Disasters and other events
BDSF	Hardware failure not related to management of transactions	Hardware	Systems
	Network failure not related to management of transactions	Computer virus or glitch; Telecommunications; and Utility outage or disruption	
	Software failure not related to management of transactions	Software	
EDPM	Client account mismanagement	Negligent loss or damage of client assets; Premises losses; and Unapproved access given to account(s)	Client account management

EBA1	EBA2	BET3	BET2
	Data management	Incorrect client records (causing loss)	
		Client permission or disclaimer missing; and Legal document(s) missing or incomplete	Customer intake and documentation
		Date entry, maintenance or loading error; and Reference data maintenance	Transaction capture, execution and maintenance
	Processing / execution failures	Accounting or entry attribution error; Collateral management failure; Delivery failure; Miscommunication; Missed deadline or responsibility; and Other (transaction processing) task mis-performance	
	IT failures related to management of transactions	Model or system mis-operation	
	Model implementation and use	Model or system mis-operation	
	Regulatory and tax authorities, including reporting	Failed mandatory reporting obligation; and Inaccurate external report (causing loss)	Monitoring and reporting
	Third party management failures	Miscellaneous non-client counterparty dispute(s); and Non-client counterparty mis-performance	Trade counterparties
		Outsourcing; and Vendor disputes	Vendors and suppliers

Recommendations

Causal factors and control failures

Remove any EBA2 categories that are either causal factors or control failures. This does not mean these risks are not important. Rather they should be captured through a different taxonomy. The EBA2 categories affected by this are: "*First, second and third-party fraud (EF)*"; "*Rights/obligation failures in preparation phase (CPBP)*"; "*Inadequate business continuity planning/event management (BDSF)*"; "*Improper distribution/marketing (EDPM)*"; and "*Third-party management failures (EDPM)*".

Internal fraud

Use the existing BET2 categories of "*Theft and Fraud*" and "*Unauthorised activity*", but add "*Intentional sanctions violation*", "*Malicious physical damage to employees, institution's physical assets and public assets*" and an additional category called "*Internal computer crime*".

Delete "*Bribery and corruption*", "*Insider Trading not on institution's account*", "*Internal fraud committed against other stakeholders*" and "*Intentional mismarking*". If it is important to supervisors to capture this information, then apply flags to identify losses falling in these categories.

External fraud

Retain the existing BET2 categories of "*Theft and fraud*" and "*Systems Security*"

Delete "*Cyber-attacks*", "*Data theft and manipulation*", "*First party fraud*", "Second party fraud" and "*Third party fraud*". If it is important to supervisors to capture this information, then apply flags to identify losses falling in these categories.

Clients, Products and Business Practices

Incorporate "*Anti-trust / anticompetition*", "*Insider Trading on institution's account*" and "*Accidental money laundering and terrorism financing*" into "*Improper market practices, product and service design or licensing*".

Incorporate "*Accidental sanctions violations" into "Sale service failure*".

If it is important to supervisors to capture specific information on these previously identified categories, then apply flags to identify losses falling in these categories.

Execution, Delivery and Process Management

Incorporate "*IT failures related to management of transactions*" and "*Model implementation and use*" into "*Processing / execution failures*".

Delete "*Third party management failures*".

If it is important to supervisors to capture specific information on these previously identified categories, then apply flags to identify losses falling in these categories.

Business Disruption and Systems Failure

Consider adding a category to capture non-systems related disruptions, such as pandemic, …