

DRAFT



Guidance Note AGN 115.2

Advanced Measurement Approaches to Operational Risk: Quantitative Standards

1. This Guidance Note details the requirements that must be met by an authorised deposit-taking institution (ADI) for calculating the **operational risk regulatory capital requirement** under an advanced measurement approach to operational risk (AMA). The requirements detailed in this Guidance Note must be met by the ADI at the time of **AMA approval** (refer paragraph 4 of *Prudential Standard APS 115 Capital Adequacy: Advanced Measurement Approaches to Operational Risk*) and on an on-going basis.
2. APRA recognises that operational risk measurement techniques are evolving and encourages continued evolution and innovation in this area. Accordingly, this Guidance Note specifies a broad set of parameters and modelling inputs that an **operational risk measurement system** would be expected to include in order to be approved for AMA purposes. The requirements in this Guidance Note are intended to be sufficiently objective to ensure consistent regulatory requirements and supervisory assessment across ADIs.
3. Consistent with this approach, the emphasis within this Guidance Note and *Guidance Note AGN 115.1 Advanced Measurement Approaches to Operational Risk: General Requirements* is on ensuring that an ADI's approach to measuring its operational risk regulatory capital requirement is conceptually sound, comprehensive and systematic, transparent and capable of independent review and validation.
4. In line with international regulatory developments, APRA will review the operational risk measurement systems used by ADIs, along with the output of those systems, and may modify the requirements of the AMA to refine the range of acceptable techniques that may be adopted by an ADI for measuring its operational risk regulatory capital requirement.

Soundness standard

5. To obtain AMA approval an ADI will be required to demonstrate to APRA the appropriateness of the operational risk regulatory capital requirement determined by the ADI's operational risk measurement system given its current and planned future operational risk profile. On-going use of an AMA by an

DRAFT

ADI will require that the ADI is able to justify to APRA any changes in the calculated operational risk regulatory capital requirement.

6. An ADI must be able to demonstrate to APRA that its operational risk regulatory capital requirement as determined by the ADI's **operational risk measurement model** meets a **soundness standard** comparable to a one-year holding period and a 99.9 per cent confidence level. In other words, the ADI's operational risk measurement model must capture an appropriately robust set of operational risk-related events that can lead to severe and rare operational risk losses. To do this, the ADI's operational risk measurement model must be sufficiently granular to capture the major drivers of operational risk affecting the shape of the tail of the ADI's operational loss distribution. The ADI's operational risk measurement system must also be sufficiently comprehensive to capture all material sources of operational risk across the ADI.
7. The soundness standard detailed in paragraph 6 above provides significant flexibility for an ADI to develop an operational risk measurement system that best suits the nature and complexity of the ADI's activities. The ADI must have and maintain rigorous procedures surrounding the implementation of the operational risk measurement system including the independent validation of that system (refer paragraphs 73 to 76 below).
8. APRA expects that there will be considerable uncertainty and potential error in an ADI's operational risk measurement system because of the nature and measurement of operational risk. Accordingly, a degree of conservatism will be required to be built into the ADI's approach to reflect the evolutionary status of operational risk and its impact on data capture and modelling.

Operational risk measurement system track record

9. An ADI's operational risk measurement system must have, in APRA's judgement, a reasonable track record in measuring operational risk. Accordingly, the ADI's operational risk measurement system will be subject to a period of initial monitoring by APRA prior to its use for the calculation of the operational risk regulatory capital requirement. The length of this monitoring period will depend upon the performance of the ADI's **operational risk management framework**, including the operational risk measurement system, and the length of that framework's track record in managing and reasonably measuring operational risk. This period of monitoring will assist APRA in determining the credibility and appropriateness of the operational risk measurement system.

Detailed criteria

10. An ADI's operational risk measurement system must be consistent with the scope of operational risk as defined in paragraph 7 of APS 115 and the loss event categories detailed in Table 2 of Attachment A.
11. The operational risk measurement system adopted by an ADI must be implemented consistently across the ADI.

DRAFT

12. In order to meet the soundness standard detailed in paragraph 6 above, an ADI's operational risk measurement system must incorporate key data inputs. These inputs are internal and relevant external operational risk loss data, scenario analysis and factors reflecting the ADI's business environment and internal control systems. In determining its operational risk regulatory capital requirement, the operational risk measurement system must take into account all available information related to these data inputs in a timely and consistent manner. Requirements for the use of these inputs within an operational risk measurement system are detailed in paragraphs 27 to 63 below.
13. An ADI must have a reliable, transparent and verifiable approach for weighting data inputs in its operational risk measurement system. The inputs must be combined in a manner that most effectively enables the ADI to quantify its operational risk exposure. The ADI's approach for weighting these inputs should be such that it does not double count any capital reducing effects arising from the incorporation of these inputs into the operational risk measurement model.
14. An ADI's risk measurement approach must be appropriate for the ADI having regard to the nature, structure and complexity of its operations, historical experience in respect of operational risk-related losses and the assessment of its planned future operational risk profile. Where industry risk modelling practices evolve and improve over time, the ADI should consider these developments in assessing its own practices.
15. Irrespective of the ADI's risk measurement approach, the ADI will be expected to establish a distribution of aggregated potential operational risk losses across the ADI or a set of operational risk loss distributions for sub-parts of the ADI's operations.
16. Where a single distribution is assumed for the purpose of determining the ADI's operational risk regulatory capital requirement, an ADI will be required to demonstrate to APRA, on the basis of quantitative and qualitative considerations, that the distribution is appropriate for all of the ADI's material operational risk exposures. Moreover, the ADI will be required to reasonably justify to APRA that the embedded dependence assumptions across operational risk losses or business lines are appropriate for the ADI, reflect the ADI's current and planned future operational risk environment and take into account the uncertainty surrounding any such estimates (particularly in periods of stress).
17. Where an ADI bases its operational risk measurement model on a number of distributions, the ADI will generally be expected to aggregate the operational risk measures resulting from different distributions for the purpose of calculating the operational risk regulatory capital requirement. Where the ADI's approach assumes a dependence structure across those risk measures, by way of correlation estimates across operational risk losses or business lines, the ADI may be able to incorporate those estimates into its aggregation of individual operational risk measures. Incorporation of correlation estimates will only be permitted if the ADI can demonstrate to APRA, with a reasonable

DRAFT

degree of confidence, that its correlation estimates are appropriate for the ADI, reflect its current and planned future operational risk environment and take into account the uncertainty surrounding any such estimates (particularly in periods of stress).

18. In both cases detailed in paragraphs 16 and 17 above, an ADI must validate its dependence assumptions using appropriate quantitative and qualitative techniques. If dependence assumptions are uncertain, the ADI must be conservative and implement an appropriate adjustment to the operational risk measurement model to take that uncertainty into account.
19. An ADI must be able to verify the accuracy and appropriateness of its operational risk measurement system and the results of its operational risk measurement model. Testing and verification is required to be performed independently of the ADI-wide operational risk management function and the business lines. Validation should include, but is not limited to, the collection and use of data inputs, the operational risk measurement methodology including the regulatory capital results and other outputs of the model.
20. An ADI must collect and retain the output of its operational risk measurement system.
21. An ADI's operational risk measurement model may estimate operational risk regulatory capital at the level of individual business activities or across the ADI. In the latter case, the ADI must be able to allocate its total operational risk regulatory capital requirement to individual business activities.
22. For the purpose of estimating operational risk capital for individual business activities or allocating operational risk capital to those business activities (refer paragraph 27 of AGN 115.1), an ADI may use its own internal classification of business activities. In this case, the ADI must be able to map its business activities, with a reasonable degree of accuracy, to the Category 1 business lines set out in Table 1 of Attachment A.
23. An ADI's mapping process must be clearly documented and include business line definitions that are clear and detailed enough to allow third parties to replicate the business line mapping. Documentation must, among other things, highlight any exceptions or overrides which must also be kept on record. An ADI is required to have in place documented processes for the mapping of new activities or products.
24. An ADI should ensure that the mapping of activities into business lines for operational risk regulatory capital purposes is consistent with the definitions of business lines used for regulatory capital calculations for credit and market risks. If an ADI uses a different scheme of classification for operational risk regulatory capital purposes, the ADI must have documented sound reasons for any difference.
25. Any banking or non-banking activity which cannot be readily mapped into the business line framework set out in Table 1 of Attachment A, but which represents an ancillary function to an activity included in the business line

DRAFT

framework, must be allocated to the business line it supports. If more than one business line is supported through the ancillary activity, an objective mapping criteria should be used to appropriately allocate the ancillary function between business lines.

26. An ADI's mapping process must be subject to independent review.

Data inputs

27. An ADI must have transparent and verifiable processes for collecting relevant data inputs (refer paragraph 12 above) on an on-going basis. These processes should ensure that operational risk data are collected to an appropriate level of integrity and that processes are consistent, timely and comprehensive across the ADI. Assessments on the appropriateness and relevance of data are to be undertaken on a regular basis and at an appropriate level of granularity. The form of these assessments, and the frequency with which they are carried out, will depend on the data in question. Assessments are to form the basis of any justification for the exclusion of data from the operational risk measurement system and must be transparent and clearly documented.
28. An ADI must have in place policies relating to data integrity including capture, completeness, accuracy, validity, consistency and maintenance. These policies must be clearly documented and may vary across type of data depending on the use of the data. Routine tests of integrity for each type of data must form part of the ADI's data validation process (refer paragraph 65 below). Data that are to be used within an operational risk measurement system must meet the ADI's internal policies and procedures which should be applied consistently across the ADI.
29. Where the ADI makes adjustments to data, the ADI must be able to justify to APRA that these adjustments are made for the purpose of ensuring that data utilised within the model more accurately reflects the environment in which the ADI operates. Such adjustments, commonly referred to as scaling, must be undertaken in a consistent and transparent manner with the methodology underlying the adjustments being well documented.

Internal data

30. The collection of internal loss data is considered to be an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal operational risk loss data (**internal loss data**) must be collected in accordance with paragraphs 31 to 45 below and must form an integral part of the measurement process for an operational risk measurement system to be credible and sufficiently robust. Internal loss data is crucial for tying the ADI's operational risk estimates to its actual loss experience.
31. Internal loss data are most relevant when clearly linked to an ADI's current and planned future business activities, internal processes and risk management framework. Therefore, as part of its operational risk management framework, the ADI must have documented policies and procedures for assessing the on-going relevance of historical internal loss data, including those situations in

DRAFT

which judgement overrides, scaling (refer paragraph 29 above) or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions. Policies and procedures should cover when an operational risk event becomes an operational risk loss for the purpose of collection within the operational risk loss database.

32. An ADI must identify all material operational risk losses consistent with the definition of operational risk detailed in paragraph 7 of APS 115.
33. An ADI's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate systems and geographic locations. The ADI must be able to justify that any excluded activities or exposures, both individually and in aggregate, would not have a material impact on the overall estimate of the operational risk regulatory capital requirement.
34. Any thresholds an ADI has for the collection of internal loss data must be appropriate. In determining a threshold, the ADI should take into account its approach to operational risk measurement for regulatory capital purposes, the use of the internal loss data for operational risk management, the capacity of the operational risk loss database and the administrative requirements placed on the business lines and operational risk resources as a consequence of the data collection and management processes. APRA will review the thresholds set by the ADI against the background of these factors and comparisons with relevant external sources including peer ADIs.
35. An ADI should include in its operational risk loss database all operational risk related losses in excess of the ADI's specified threshold(s). This includes operational risk losses that have typically been regarded as credit or market risk-related losses (refer paragraphs 41 to 43 below).
36. Aside from information on the gross operational risk loss amounts, an ADI must collect information about the date of the loss event and any recoveries, as well as descriptive information about the drivers or causes of the loss event. The level of detail of descriptive information should be commensurate with the size of the gross loss amount.
37. An ADI's data procedures must describe how the ADI will treat, for the purpose of its operational risk loss database and operational risk management and modelling, a series of operational loss events that are related events over time.
38. Internally generated measures of operational risk used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data. The exception is when an ADI first moves to an AMA, at which time a three-year historical data window may, subject to written approval by APRA, be acceptable.
39. An ADI must document the criteria it uses to map its historical internal loss data to the relevant Category 1 business activities defined in Table 1 of Attachment A and to the Category 1 event type categories detailed in Table 2 of that Attachment.

DRAFT

40. An ADI must develop specific criteria for allocating losses arising from an operational risk loss event in a centralised function (for example, an information technology department) or an activity that spans more than one business line.
41. Operational risk-related credit risk losses should be flagged separately within an ADI's internal operational risk loss database for the purpose of operational risk management. The materiality of these losses may vary between ADIs and within an ADI across business lines and event types. Materiality thresholds should be set with reference to those used by peer ADIs and with the ADI's internal credit risk management processes.
42. Operational risk losses that have characteristics of credit risk must be treated as credit risk for the purpose of calculating an ADI's minimum regulatory capital requirement. Therefore, such losses will not be subject to an operational risk regulatory capital requirement provided that those losses are subject to the credit risk regulatory capital framework (refer *Prudential Standard APS 113 Capital Adequacy: Internal Ratings-based Approach to Credit Risk*).
43. Operational risk losses that are related to market risk must be treated as operational risk for the purpose of calculating the ADI's minimum regulatory capital requirement for operational risk. An ADI applying *Prudential Standard APS 116 Capital Adequacy: Market Risk* for the calculation of its traded market risk capital requirement must not exclude positions resulting from operational risk events from the traded market risk regulatory capital calculations.
44. An ADI must have a well-defined policy for the classification and regulatory capital treatment of operational, credit and market risk-related losses. This policy should be applied consistently across the ADI.
45. An ADI will be required to implement appropriate processes and controls surrounding the collection of internal loss data so as to ensure that data collected is sufficiently complete and accurate. Reconciliation of individual loss data points with finance records may be one of the techniques utilised to ensure this is achieved.

External data

46. Relevant **external loss data** must be incorporated into an ADI's operational risk measurement system. An ADI must have in place a systematic and robust process for collecting, assessing and incorporating external loss data into the ADI's operational risk measurement system.
47. The use of external loss data should include the consideration of infrequent yet potentially severe operational risk loss events.
48. External loss data should include data on the loss amount and loss event category, information on any recoveries to the extent that these are known, the nature and scale of the operation where the event occurred and any other available information that would assist in assessing the relevance of the loss event to the ADI.

DRAFT

49. An ADI must have a systematic process for determining the situations for which external loss data are used and the methodologies used to incorporate the data. The collection and application of external loss data must be regularly reviewed, documented and subject to periodic independent review.

Scenario analysis

50. Scenario analysis must be incorporated into an ADI's operational risk measurement system to evaluate the ADI's exposure to high-severity loss events. The ADI must collect scenarios that draw upon the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses. This is especially relevant for business activities or types of loss events where internal and external loss data do not provide a sufficiently robust estimate of the ADI's exposure to operational risk.
51. The set of developed scenarios should be comprehensive and capture all material sources of operational risk across all of an ADI's business activities and geographic locations.
52. An ADI's process for building a database of scenario-based events must be robust and methodical and is required to be applied consistently across the ADI. The ADI must have a process in place for regularly reviewing this database to ensure that the developed scenarios continue to adequately reflect the operational risk profile of the ADI. At a minimum, an annual review of all scenarios is required. The ADI must also have in place a process for identifying the need for more frequent reviews of developed scenarios in response to changes in the ADI's operational risk exposure.
53. An ADI's operational risk management framework must include policies and procedures that identify how scenario analysis will be incorporated into the operational risk measurement system.
54. Scenarios and their use in operational risk modelling must be independently reviewed and validated. Over time, scenarios must be re-assessed through comparison to actual loss experience to assess their reasonableness.

Business environment and internal control factors

55. In addition to using operational risk loss data, whether actual or scenario-based, an ADI's operational risk measurement system must incorporate indicators of the ADI's current and planned future operational risk profile, as well as other information related to the assessment of the ADI's internal control framework. This information should assist in aligning the ADI's assessment of the required amount of operational risk capital with the risk management objectives of the ADI.
56. By their nature, these inputs, termed **business environment and internal control factors**, are intended to ensure that an ADI's operational risk measurement system is forward-looking and more closely aligned with the quality of the ADI's control and operating environments. Accordingly, these factors must be responsive to changes in the ADI's operational risk profile and

DRAFT

reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover and system downtime. When reporting thresholds are directly linked to these indicators, an effective monitoring process should identify key material risks in a transparent manner and enable the ADI to react appropriately.

57. An ADI must monitor its business environment and internal control factors. The frequency of such monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring must be an integrated part of an ADI's activities with the results of monitoring activities included in regular senior management and Board reports.
58. An ADI must be able to justify to APRA the choice of each business environment and internal control factor as a relevant driver of operational risk, based on considerations of historical experience and involving the expert judgment of relevant business areas.
59. As noted previously, business environment and internal control factors must be responsive to changes in an ADI's operational risk profile. As such, these factors are required to recognise both improvements and deterioration in the ADI's operational risk profile. This means that the operational risk measurement model must capture potential increases in risk due to greater complexity of activities or increased business volume as well as capturing changes in risk due to improvements in internal controls. Changes in the ADI's internal processes and risk management procedures should be similarly taken into account.
60. An ADI must be able to justify to APRA the relationship between changes in the ADI's operational risk estimates and changes in its business environment and internal control factors. Similarly, APRA will require justification for the relative weighting of the various factors within the ADI's operational risk measurement system.
61. Where possible, business environment and internal control factors should be translated into quantitative measures that lend themselves to verification.
62. An ADI must have in place policies and procedures for the development and use of business environment and internal control factors for the purpose of determining an operational risk regulatory capital requirement. The process for changes in these factors must be documented.
63. Business environment and internal control factors are required to be independently reviewed. Over time, an ADI will be required to compare its estimates of these factors with actual internal operational risk loss experience.

Data management

64. An ADI must have policies and procedures in relation to operational risk data management. These policies and procedures should describe (using if a diagram if appropriate) the data architecture covering the collection of data, data storage, how relevant data is collated for regulatory capital purposes and outline all data

DRAFT

flows between systems, including whether any manual processes are involved in such flows. The ADI should detail the reconciliation process among databases, including between finance and risk data bases, and how unreconciled items are treated.

65. An ADI's operational risk data collection process and historical data set must be subject to initial (that is, at the time that AMA approval is sought) and subsequent independent validation to ensure the continued on-going integrity of the data. The ADI is required to obtain an independent review of:
 - (a) the accuracy and completeness of the data used in the calculation of the operational risk regulatory capital requirement and, to the extent that the data differs, in management reports;
 - (b) the accuracy and completeness of the databases used to validate and redevelop relevant model parameters; and
 - (c) the accuracy and completeness of all flows between data capture systems and other relevant systems such as the operational risk measurement model.
66. For the purposes of paragraph 65 above, the party undertaking the independent review need not be external to the ADI but must be independent of business units and of those areas within the consolidated banking group or, in the case of a locally-incorporated subsidiary of a foreign ADI, the banking group in general, that have played, or will play, a role in the design and implementation of an ADI's operational risk data collection processes.

Risk mitigation

67. Subject to written approval from APRA, an ADI may recognise the risk-mitigating effect of insurance in determining its operational risk regulatory capital requirement. The recognition of insurance will be limited to 20 per cent of the total operational risk regulatory capital requirement calculated using the ADI's operational risk measurement model.
68. To recognise insurance as an operational risk mitigant, an ADI must be able to demonstrate to APRA that the insurance will cover potential operational risk losses included in the operational risk measurement model in a manner equivalent to holding regulatory capital. This will require that the insurance coverage satisfy the following criteria:
 - (a) the provider of the insurance policy must have a minimum claims paying ability rating of A under Standard and Poor's Insurer Financial Strength Ratings, A2 under Moody's Insurance Financial Strength Ratings or A under AM Best's Financial Strength Ratings;
 - (b) the insurance policy must have a minimum notice period for cancellation of 90 days;

DRAFT

- (c) the insurance policy must not have any exclusions or limitations caused by, or resulting from, any regulatory or supervisory action taken by a statutory authority or from any losses or expenses incurred by the ADI prior to the commencement of any liquidation or receivership proceedings against the ADI. Damage or loss which arises from events that occur after such proceedings have been initiated may be excluded or linked;
 - (d) notwithstanding sub-paragraph 68 (c) above, the policy may exclude fines, penalties or punitive damages; and
 - (e) the insurance must be provided by a third-party entity that is regulated by APRA or is subject to regulatory oversight broadly consistent with that applied by APRA. In the case of insurance through captives and affiliates, the exposure must be transferred to an independent third-party entity, for example through reinsurance.
69. An ADI must have in place policies and procedures for determining the risk-mitigating effects of insurance within its operational risk measurement model. The approach adopted by the ADI must reflect its insurance coverage in a manner that is consistent with the actual probability and severity of operational losses assumed within the operational risk measurement model. The approach must be consistently applied and capable of independent validation.
70. In addition, an ADI's approach to insurance risk mitigation under an AMA must capture the following characteristics of the insurance policy through appropriate haircuts to the amount of insurance recognition:
- (a) the residual term of the policy (refer paragraphs 71 to 72 below);
 - (b) the policy's cancellation terms, including the possibility that the policy could be cancelled before the contractual expiration;
 - (c) the uncertainty of payment, including the willingness of the insurer to pay the claim in a timely manner and the legal risk that a claim may be disputed; and
 - (d) any mismatches in the coverage of insurance policies.
71. In order to be eligible as a risk-mitigant for AMA purposes, the insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, an ADI must make appropriate haircuts to reflect the declining residual term of the policy. Haircuts range from zero per cent for policies with a residual term of at least 365 days up to a full 100 per cent haircut for policies with a residual term of 90 days or less (refer paragraph 72).
72. Where an insurance policy has an initial term greater than or equal to one year and the residual term is between 90 and 365 days, the amount of insurance recognition will be subject to the following haircut:

$$(365 - \text{residual term of insurance contract (in days)})/275$$

DRAFT**Independent review and validation of the operational risk measurement system**

73. An independent review and validation of the operational risk measurement system should be carried out on a regular basis. The ADI must ensure that its operational risk measurement system, including its approach to capital modelling, is subject to effective and comprehensive review by operationally independent, appropriately trained and competent staff. (In most cases, this review could be facilitated by an ADI's internal audit function, but may require the engagement of independent parties outside of this function.)
74. For the purpose of paragraph 73 above, independence requires that the party or parties undertaking the review need not be external to the ADI but must not be involved in the development, implementation and use of the operational risk measurement system within the ADI. It is not necessary that the same party undertake all aspects of the review.
75. An independent review of an operational risk measurement system, apart from the approach to capital modelling, should be conducted at least once a year. An independent review of the approach to capital modelling should take place at least once every three years or when a material change is made to that approach.
76. At a minimum, the reviews must address the following:
 - (a) the scope of operational risks captured by the operational risk measurement system and an assessment of whether the system captures all material activities and operational risk exposures from all relevant geographic locations;
 - (b) the consistency of the methodology across the ADI's business areas;
 - (c) compliance with the requirements of this Guidance Note;
 - (d) the accuracy of the analytics underlying the regulatory capital calculation;
 - (e) the accuracy and appropriateness of data flows into the regulatory capital calculation including an assessment of whether relevant data has been omitted from the calculation;
 - (f) assessment of the reasonableness of any assumptions made in the operational risk measurement model, such as those made in relation to implicit or explicit correlation structures;
 - (g) the integrity of the management information system, including the appropriateness and accuracy of management reports;
 - (h) validation of any significant change in the operational risk measurement system;
 - (i) the appropriateness of model validation processes, including the adequacy of procedures and controls over changes in model inputs, assumptions and

DRAFT

calculation methodologies and assessment of the operation of those processes;

- (j) the accuracy and adequacy of technical documentation supporting the quantitative aspects of the operational risk measurement system; and
- (k) the integration of the operational risk measurement system into daily operational risk management processes.

DRAFT**Attachment A****Table 1 - Mapping of business lines**

Category 1	Category 2	Example business activities
Corporate finance	Corporate finance	Mergers and acquisitions, underwriting, privatisations, securitisation, research, syndications, initial public offerings, secondary private placements, holdings of debt (government, high yield) and equity.
	Municipal/government finance	
	Merchant banking	
	Advisory services	
Trading and sales	Sales	Fixed income, equity, foreign exchange, commodities, credit trading, funding, lending and repurchase agreements and brokerage (other than retail brokerage).
	Market making	
	Proprietary positions	
	Treasury	
Retail banking	Retail banking	Retail lending and deposit-taking, banking services, trust and estate management.
	Private banking	Private lending and deposit-taking, banking services, trust and estate management and investment advice.
	Card services	Merchant, commercial and corporate cards.
Commercial banking	Commercial banking	Commercial lending and deposit-taking, project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees and 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) and corporate actions.
	Corporate agency	Issuer and paying agent activity.

¹ Payment and settlement losses related to an ADI's own activities would be incorporated in the loss experience of the affected business line.

DRAFT

	Corporate trust	
Asset management	Discretionary funds management	Pooled, segregated, retail, institutional, closed and open discretionary funds management and private equity.
	Non-discretionary funds management	Pooled, segregated, retail, institutional, closed, and open non-discretionary funds management.
Retail brokerage	Retail brokerage	Execution and full service brokerage services.

DRAFT**Table 2 – Loss event categories**

Event-type category (Category 1)	Definition	Categories (Category 2)	Activity examples
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) Transaction type unauthorised Mismarking of position (intentional)
		Theft and fraud	Fraud/credit fraud/worthless deposits Theft/extortion/embezzlement/robbery Misappropriation of assets Malicious destruction of assets Forgery Cheque kiting Smuggling Account take-over/impersonation etc Tax non-compliance/evasion (wilful) Bribes/kickbacks Insider trading (not on ADI's account)
External fraud	Losses due to acts of a third party that are of a type intended to defraud, misappropriate	Theft and fraud	Theft/robbery

DRAFT

	property or circumvent the law.		Forgery Cheque kiting
		Systems security	Hacking damage Theft of information (with monetary loss)
Employment practices and workplace safety	Losses arising from acts that are 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 and safety rules events Workers compensation
		Diversity and discrimination	All discrimination types
Clients, products and 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 and fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (for example, know your client requirements) Retail customer 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

DRAFT

			<p>Market manipulation</p> <p>Insider trading (on the ADI's account)</p> <p>Unlicensed activity</p> <p>Money laundering</p>
		Product flaws	<p>Product defects (unauthorised etc)</p> <p>Model errors</p>
		Selection, sponsorship and exposure	<p>Failure to investigate client per guidelines</p> <p>Exceeding client exposure limits</p>
		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	<p>Natural disaster losses</p> <p>Human losses from external sources (for example, terrorism or vandalism)</p>
Business disruption	Losses arising from disruption of business or system failures.	Systems	<p>Hardware</p> <p>Software</p> <p>Telecommunications</p> <p>Utility outage/disruptions</p>
Execution, delivery and process management	Losses arising from failed transactions processing, process management, relations with trade counterparties and vendors.	Transaction capture, execution and maintenance	<p>Miscommunication</p> <p>Data entry, maintenance or loading error</p> <p>Missed deadline or responsibility</p> <p>Model/system mis-operation</p> <p>Accounting error/entity attribution error</p> <p>Other task mis-performance</p>

DRAFT

			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 mis-performance Miscellaneous non-client counterparty disputes
		Vendors and suppliers	Outsourcing Vendor disputes