



Prudential Standard APS 115

Capital Adequacy: Advanced Measurement Approaches to Operational Risk

Objective and key requirements of this Prudential Standard

This Prudential Standard sets out the requirements that an authorised deposit-taking institution that has approval to use an advanced measurement approach to operational risk must meet both at the time of initial implementation and on an ongoing basis for regulatory capital purposes.

The key requirements of this Prudential Standard are that an authorised deposit-taking institution must have:

- a framework to manage, measure and monitor operational risk commensurate with the nature, scale and complexity of its operations; and
- approval from APRA to use a measurement model for determining the institution's operational risk capital requirement.

Table of contents

Prudential Standard

Authority	3
Application	3
Scope	3
Defintitions	3
Key principles	4
Approval process	4
Adoption of the advanced measurement aproach	5
Operational risk management framework	6
Operational risk measurement system	7
Allocation of operational risk regulatory capital.....	8
Significant locally incorporated subsidiaries of foreign ADIs.....	9

Attachments

Attachment A - Governance and the operational risk management framework	10
Responsibilities of the Board of directors and senior management	10
Sufficient resources	11
Operational risk management function	11
Documentation of the operational risk management framework.....	11
Internal reporting of the ADI's operational risk profile	12
Integration of the operational risk measurement system into day-to-day operational risk management	13
Independent review of the operational risk management framework.....	13
Attachment B - Operational risk measurement system and data management	15
Operational risk measurement system track record.....	15
Detailed criteria.....	15
Data	16
Risk mitigation	20
Sensitivity analysis.....	22
Validation	22
Attachment C - Allocation mechanisms	23
Attachment D - Mapping of business lines.....	24
Attachment E - Loss event categories	26

Authority

1. This Prudential Standard is made under section 11AF of the *Banking Act 1959* (**Banking Act**).

Application

2. This Prudential Standard applies to authorised deposit-taking institutions (**ADIs**) that are seeking or have been given approval to use an advanced measurement approach (**AMA**) to operational risk for the purpose of determining regulatory capital.
3. A reference to an ADI in this Prudential Standard shall be taken as a reference to:
 - (a) an ADI on a **Level 1** basis; and
 - (b) a group of which an ADI is a member on a **Level 2** basis.

Level 1 and Level 2 have the meaning in *Prudential Standard APS 110 Capital Adequacy* (**APS 110**).

Where an ADI to which this Prudential Standard applies is a subsidiary of an authorised non-operating holding company (**authorised NOHC**), the authorised NOHC must ensure that the requirements in this Prudential Standard are met on a Level 2 basis, where applicable.

Scope

4. This Prudential Standard applies to all operations and activities of an ADI that has APRA's approval to use an AMA for operational risk.

Definitions

5. The following definitions are used in this Prudential Standard:
 - (a) **AMA** - an advanced approach used to measure an ADI's regulatory capital for operational risk that has been approved by APRA;
 - (b) **allocation mechanism** - an APRA-approved process by which a banking group allocates or distributes regulatory capital for operational risk to legal entities within the group, with the ADI determining its operational risk regulatory capital (**ORRC**) by reference to the ORRC allocated to it as a member of the group;

- (c) **operational risk** - the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risk,¹ but excludes strategic and reputational risks;
- (d) **ORRC** - the regulatory capital that an ADI is required to hold against its exposure to operational risk in accordance with this Prudential Standard;
- (e) **operational risk management framework** - the organisational structures, processes and systems used in identifying, assessing, measuring, monitoring, controlling and mitigating operational risk;
- (f) **operational risk measurement system** - the systems and data of the operational risk management framework used to measure operational risk;
- (g) **operational risk measurement model** - the model central to the operational risk measurement system that is used by the ADI to quantify its ORRC;
- (h) **related body corporate** - a body corporate that is related to another body corporate within the meaning of section 50 of the *Corporations Act 2001*; and
- (i) **third party** - an entity that is not the ADI or a related body corporate of the ADI.

Key principles

6. An ADI that has received approval from APRA to use an AMA must:
 - (a) have in place a robust operational risk management framework and a conceptually sound operational risk measurement system; and
 - (b) hold regulatory capital commensurate with its exposure to operational risk.

Approval process

7. An ADI may apply for written approval from APRA to use an AMA for capital adequacy purposes.
8. In its application, the ADI must, unless exempted in writing by APRA, seek approval to use:
 - (a) the internal ratings-based approach to credit risk for the purpose of determining the ADI's regulatory capital for credit risk (refer to *Prudential Standard APS 113 Capital Adequacy: Internal Ratings-based Approach to Credit Risk (APS 113)*); and

¹ Legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as ordinary damages in civil litigation, related legal costs and private settlements.

- (b) an internal risk measurement model for the purpose of determining the ADI's regulatory capital for interest rate risk in the banking book (refer to *Prudential Standard APS 117 Capital Adequacy: Interest Rate Risk in the Banking Book*)

unless APRA has previously approved the ADI's use of the approach or model.

9. APRA may, in writing, approve the use of an AMA by an ADI. The AMA approval may specify how the AMA is to apply in relation to the ADI, including approvals under other paragraphs of this Prudential Standard. APRA's prior written approval is required for any material changes to the operational risk measurement model. Prior notification to APRA is required for material changes to other components of the operational risk management framework. APRA may impose conditions on the AMA approval.
10. Once an ADI has obtained AMA approval, it must continue to employ the AMA on an ongoing basis unless, or except to the extent that, the AMA approval is revoked or suspended for some or all of the ADI's operations. A return, at the ADI's request, to the standardised approach to operational risk will generally only be permitted in exceptional circumstances.
11. APRA may, at any time in writing to the ADI, vary or revoke an AMA approval, or impose additional conditions on the AMA approval if it determines that:
 - (a) the ADI does not comply with this Prudential Standard; or
 - (b) it is appropriate, having regard to the particular circumstances of the ADI, to impose the additional conditions or make the variation or revocation.
12. Where an AMA approval for an ADI has been varied or revoked, APRA may, in writing, require the ADI to revert to the standardised approach to operational risk (refer to *Prudential Standard APS 114 Capital Adequacy: Standardised Approach to Operational Risk (APS 114)*) for some or all of its operations, until it meets the conditions specified by APRA for returning to the AMA.
13. An ADI that has received AMA approval from APRA may rely on its own internal estimate (based on the approved operational risk measurement model) of operational risk for determining its ORRC. That estimate must be fundamentally sound and consistent with the scope of operational risk defined in paragraph 5(c) of this Prudential Standard.
14. APRA may, in writing, require an ADI with AMA approval to reduce its level of operational risk or increase its capital if APRA considers that the ADI's ORRC is not commensurate with the ADI's operational risk profile.

Adoption of the advanced measurement approach

15. APRA will generally require an ADI that has AMA approval to apply the AMA across all business activities of the ADI. APRA recognises, however, that for many ADIs it may not be practical to implement the AMA across all of their

business activities. This may be the case, for instance, where an ADI moves from the standardised approach to operational risk (refer to APS 114), undertakes a new business activity, has acquired a new business through merger or acquisition or has certain immaterial business activities (refer to paragraph 20 of this Prudential Standard). In such circumstances, APRA's approval of the AMA may permit the ADI to use a combination of the AMA and the standardised approach to operational risk for measuring its ORRC. This approach is referred to as **partial use**.

16. An ADI must provide APRA with appropriate written information, both at the time of the ADI's initial application for AMA approval and subsequent to the ADI obtaining AMA approval, on the business activities for which the ADI proposes to use the standardised approach to operational risk.
17. Approval for partial use of an AMA will, at a minimum, require that:
 - (a) all material operational risks across the ADI are captured (by the combined AMA and standardised approach) within the ADI's total amount of regulatory capital for operational risk; and
 - (b) a substantial majority of the ADI's operational risks are captured by the AMA.

In the case of partial use of an AMA, diversification benefits for any part of the ADI's operations that is excluded from the operational risk measurement system will not be recognised.

18. APRA may approve partial use of an ADI's AMA on a short-term basis. In this case, the ADI will be required to adopt a phased roll-out of the AMA across all material business activities of the ADI. A phased roll-out may include (but need not be limited to) adoption of the AMA, in accordance with a specified timetable, across business activities within a particular legal entity or legal entities within the consolidated banking group.
19. An ADI that has received approval to adopt a phased roll-out of the AMA must have a written APRA-approved implementation plan in place that specifies the extent and timing of roll-out of the AMA across all material business activities.
20. Permanent partial use of an AMA will be approved only in exceptional circumstances and where the ADI is able to demonstrate that those business activities to which the AMA does not apply are immaterial in terms of size and perceived risk profile. The calculated ORRC for such business activities, if considered necessary by APRA, may be subject to additional regulatory capital.

Operational risk management framework

21. An ADI with AMA approval must have in place an operational risk management framework that is sufficiently robust to facilitate quantitative estimates of the ADI's ORRC that are sound, relevant and verifiable. APRA must be satisfied that the ADI's operational risk management framework is suitably rigorous and consistent with the complexity of the ADI's business.

Where industry risk modelling practices evolve and improve over time, the ADI must consider these developments in assessing its own practices. Furthermore, the AMA must play an integral role in the ADI's risk management and decision-making processes and meet the requirements detailed in Attachment A, including requirements relating to the Board of directors (**Board**) and senior management responsibilities.

22. An ADI seeking AMA approval must demonstrate the processes it has undertaken to establish an operational risk management framework. The ADI will also be required to demonstrate the processes that are undertaken to ensure the operational risk management framework has continued relevance to the ADI's operations.

Operational risk measurement system

23. An ADI's operational risk measurement system must be:
- conceptually sound, comprehensive, consistently implemented, transparent and capable of independent review and validation; and
 - sufficiently comprehensive to capture all material sources of operational risk across the ADI, including those events that can lead to rare and severe operational risk losses.
24. As part of the AMA approval process, an ADI will be required to demonstrate the appropriateness of the ORRC determined by the ADI's operational risk measurement system and commensurate with its operational risk profile. An ADI must justify to APRA any changes in the calculated ORRC as part of its ongoing use of an AMA.
25. An ADI must be able to demonstrate to APRA that its ORRC, 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 (the **soundness standard**). This soundness standard 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. Given the subjectivity and uncertainty of operational risk measurement modelling, an ADI must be conservative in the modelling choices and assumptions used in its operational risk measurement model, including the assessment and incorporation of severe loss events. In adopting a conservative modelling approach, the ADI must consider the results of sensitivity analysis referred to in paragraph 51 of Attachment B.
26. An ADI's ORRC must cover expected losses (**EL**) and unexpected losses (**UL**) unless the ADI can demonstrate to APRA that it has adequately measured and accounted for EL in its business practices by way of **EL offsets**. For operational risk EL to be measured and accounted for to the satisfaction of APRA, the ADI must be able to demonstrate that the EL offsets are:
- highly predictable, routine and reasonably stable over time;

- (b) estimated using a process that is conceptually sound, implemented with integrity and consistently applied over time;
- (c) available to cover EL with a high degree of certainty over a one-year time horizon;
- (d) used to support the management of the business including being systematically budgeted and considered in pricing of related products and services; and
- (e) subject to regular review by the ADI for reasonableness given comparisons with subsequent outcomes.

Accounting provisions or reserves for operational risk loss events that have already occurred do not qualify as allowable EL offsets. The ADI must clearly document how its operational risk EL is measured and accounted for, including how any offsets for EL meet the conditions above.

27. An ADI's operational risk measurement system must reasonably estimate the ORRC based on the combined use of internal and relevant external operational risk loss data, scenario analysis and factors reflecting the ADI's business environment and internal control systems. The ADI must have in place a process for systematically tracking operational risk loss data.
28. Data sources and methodologies utilised for the purposes of determining an ADI's economic capital estimate for operational risk must be consistent with the operational risk measurement system used to determine the ORRC. Where there are differences, the ADI will be required to explain to APRA's satisfaction the reasonableness of those differences.
29. Subject to meeting the criteria detailed in Attachment B, and written approval from APRA, an ADI may recognise the risk-mitigating effect of insurance in determining its ORRC. The recognition of insurance will be limited to 20 per cent of the total ORRC calculated using the ADI's operational risk measurement model.
30. The ORRC must be calculated on at least an annual basis or when there is a material change in the ADI's operational risk profile or a material change is made to the operational risk management framework. In addition, the ADI must review the ORRC on at least a half-yearly basis to ensure that it continues to reflect the ADI's operational risk profile.
31. An ADI with AMA approval must meet the quantitative standards for measuring ORRC detailed in Attachment B.

Allocation of operational risk regulatory capital

32. If approved in writing by APRA an ADI:
 - (a) that is part of a consolidated banking group (refer to paragraph 3 of this Prudential Standard); or

- (b) in the case of an ADI that is a locally incorporated subsidiary of a foreign ADI (other than a subsidiary that APRA has determined in writing to be significant), that is part of a banking group in general

may determine its ORRC on the basis of an allocation of the group's ORRC. In this case, the ORRC of the ADI is determined by an allocation mechanism rather than a stand-alone operational risk measurement model. Approval by APRA will only be granted if, at a minimum, the ADI meets the requirements detailed in Attachment C.

Significant locally incorporated subsidiaries of foreign ADIs

- 33. An ADI that is a locally incorporated subsidiary of a foreign ADI, being a subsidiary that APRA has determined in writing to be significant, must calculate its ORRC based on a stand-alone operational risk measurement model. In this case, the ORRC of the ADI must comply with the requirements of this Prudential Standard with the exception that the calculation cannot incorporate group-wide diversification benefits. The ORRC for the ADI may, however, incorporate diversification benefits from its own operations including those that arise from its own subsidiaries.
- 34. In making its determination as to whether an ADI that is a locally incorporated subsidiary of a foreign ADI is significant or not, APRA will liaise, as appropriate, with the home supervisor of the parent entity of the ADI. An ADI that is a locally incorporated subsidiary of a foreign ADI must provide APRA with appropriate information to assist APRA in making its determination.

Attachment A

Governance and the operational risk management framework

Responsibilities of the Board of directors and senior management

1. An ADI's Board is responsible for the overall operational risk profile of the ADI and the ADI's operational risk management framework. Accordingly, the Board must make clear its appetite for operational risk, including operational risk loss reporting thresholds. The Board or a Board committee must be actively involved in the oversight of the ADI's approach to managing and measuring operational risk.
2. An ADI's operational risk management framework must be approved by the Board, or a Board committee. In the latter case, the committee must have clearly defined responsibilities, operational risk loss thresholds for reporting to the Board and performance obligations. The approved framework must clearly articulate respective responsibilities and reporting relationships.
3. To ensure the continued effectiveness of the operational risk management framework, the Board, or Board committee, must ensure that the framework is subject to periodic validation and review (refer to paragraphs 19 and 20 of this Attachment) by a suitable independent party.
4. An ADI's Board, or Board committee, must review operational risk management reports (refer to paragraphs 13 to 16 of this Attachment) on a regular basis and satisfy itself that this risk is appropriately managed.
5. Senior management must have a thorough understanding of the ADI's operational risk management framework (to the extent that it relates to risk areas within their responsibilities), be actively involved in its implementation and ensure its effective operation over time. To facilitate this, the ADI must have in place an executive committee, with appropriate representation from across the ADI, which focuses on the management and measurement of operational risk. The executive committee must hold regular meetings to discuss matters including the performance of the framework, areas requiring improvement and the status of efforts to address previously identified deficiencies.
6. The ADI must have an independent operational risk management function that complies with the requirements in this Attachment. This function must have a suitable independent reporting line, providing access to the executive committee referred to in paragraph 5 of this Attachment.
7. Senior management must, in conjunction with the operational risk management function referred to in paragraph 6 of this Attachment, develop appropriate policies relating to the operational risk management framework. Management is responsible for translating these policies into specific procedures and processes to facilitate implementation and verification within the ADI's business

operations. Senior management must provide notice to the Board, or Board committee, of material changes or exceptions from established policies that could have an impact on the operation of the operational risk management framework, including the operational risk capital requirement.

Sufficient resources

8. An ADI must have sufficient numbers of personnel skilled in the management and measurement of operational risk to ensure that its operational risk management framework continues to operate effectively.

Operational risk management function

9. An ADI must have an independent specialist operational risk management function (**function**) that complies with the requirements set out in this Attachment. This function must:
 - (a) have reporting lines and responsibilities that are functionally independent of the operational risk generating business units;
 - (b) have all roles and responsibilities of people and functions involved in operational risk management clearly defined and documented, particularly where staff with operational risk management responsibility and dual reporting lines to the function and business unit management are embedded in the business units;
 - (c) have responsibility for the design, maintenance and ongoing development of the operational risk management framework, inclusive of the operational risk measurement system and reporting process, and for ensuring its consistent implementation across all business units (in conjunction with senior management and management in general (refer to paragraph 7 of this Attachment)); and
 - (d) continuously monitor the ADI's compliance with the operational risk management framework.

Documentation of the operational risk management framework

10. An ADI's operational risk management framework must be clearly documented. Documentation must include the ADI's definition of operational risk, consistent with this Prudential Standard.
11. Documentation relating to an operational risk measurement system must be comprehensive and provide a level of detail sufficient to ensure that an ADI's approach to determining its ORRC is transparent and capable of independent review and validation.
12. An ADI's technical documentation relating to its operational risk measurement system must include the following information:

- (a) the rationale for all assumptions and specifications underpinning the operational risk measurement system;
- (b) the analytics and relevant theory behind all calculations;
- (c) details of the parameters and assumptions of the operational risk measurement model including the ADI's justification for their use and the process undertaken for checking and validating those assumptions;
- (d) an explanation of how the ADI ensures that the required soundness standard (refer to paragraph 25 of this Prudential Standard) is achieved;
- (e) details of any explicit and implicit dependence structures utilised in the operational risk measurement model, including evidence supporting their use;
- (f) details of the proposed methodology for measuring and accounting for expected loss; and
- (g) details of the methodology relating to the use of insurance for risk mitigation, including how the level of insurance mitigation is derived and the types of insurance contracts utilised.

Internal reporting of the operational risk profile

13. An ADI must implement a process to regularly monitor its operational risk profile. To support the proactive management of operational risk, there must be regular reporting of relevant information to the Board, or Board committee, and senior management.
14. In developing an appropriate internal reporting framework, an ADI must consider the nature of its operational risk and the strategy adopted for managing and measuring it. Management reports must be produced and reviewed regularly and include information on the output of the ADI's operational risk measurement model and operational risk loss reporting thresholds. The reviews must be conducted by a level of management with sufficient seniority and authority to enforce, where necessary, mitigation of the ADI's operational risk.
15. An ADI must have in place a process for ensuring that the ADI's Board, or Board committee, and senior management are able to respond appropriately to the information contained in operational risk management reports. This process should include escalation procedures for key operational risk issues to facilitate appropriate action between formal reporting cycles.
16. In addition to monitoring internal and external operational risk loss events, the ADI must identify, and include in its reporting framework, appropriate indicators that provide early warnings of potential operational risk-related losses. Use of these indicators within the AMA is detailed in Attachment B.

Integration of the operational risk measurement system into day-to-day operational risk management

17. An ADI's operational risk measurement system must be closely integrated into the ADI's risk management processes. This requires that the inputs and outputs of the ADI's operational risk measurement system, as relevant, play an integral role in the ADI's decision-making, corporate governance, risk management and internal capital allocation processes.
18. An ADI's operational risk measurement system must be capable of allocating economic capital for operational risk to internal business lines. The process for allocating capital must be consistent across the ADI and sufficiently granular such that it creates incentives to improve business line operational risk management. Consistent with the ADI's economic capital allocation methodology, the drivers of operational risk capital, as one of the key mechanisms for influencing operational risk management behaviour, must be sufficiently understood by business lines. Moreover, each business line must be able to clearly articulate the drivers of its operational risk profile and demonstrate how it utilises the outputs of the operational risk measurement system to supplement its day-to-day management processes.

Independent review of the operational risk management framework

19. An ADI's operational risk management framework must be subject to effective and comprehensive independent review both initially at the time that AMA approval is sought, and thereafter on an ongoing basis, to ensure the continued integrity of the framework. Such reviews must be conducted by functionally independent, appropriately trained and competent personnel, must take place at least once every three years or when a material change is made to the framework and must cover:
 - (a) the scope of operational risks captured by the operational risk management framework, including an assessment of whether the framework captures all material activities and operational risk exposures from all relevant geographic locations;
 - (b) the accuracy of the analytics underlying the calculation of the ORRC, the outputs of the operational risk measurement model and the consistency of this methodology across the ADI's business areas;
 - (c) assessment of the reasonableness of any assumptions made in the operational risk measurement model;
 - (d) the accuracy and adequacy of documentation supporting the quantitative aspects of the operational risk measurement system; and
 - (e) the continuing appropriateness and adequacy of the risk modelling approach given industry developments in the modelling of operational risk.

20. For the purposes of paragraph 19 of this Attachment, ‘functionally independent’ means that:
- (a) the relationship between the party or parties conducting the reviews and the ADI’s business areas is such that opportunities for the independent party or parties to improperly influence the operational risk management framework are minimised; and
 - (b) the party or parties conducting the reviews must not be involved in the development, implementation or operation of the operational risk measurement system, or be part of, or report to the operational risk management function referred to in paragraph 6 of this Attachment.

It is not necessary that the same party undertake all aspects of the review.²

² In most cases, the independent reviews could be facilitated by an ADI’s internal audit function but may require the engagement of independent parties outside of this function.

Attachment B

Operational risk measurement system and data management

Operational risk measurement system track record

1. An ADI's operational risk measurement system must have a reasonable track record in measuring operational risk. Accordingly, before the ADI receives an AMA approval, 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 ORRC. The length of this monitoring period will depend upon the performance of the ADI's operational risk management framework and its track record in managing and measuring operational risk.

Detailed criteria

2. An ADI's operational risk measurement system must be consistent with the scope of operational risk as defined in paragraph 5(c) of this Prudential Standard and the loss event categories detailed in Attachment E.
3. In order to meet the soundness standard detailed in paragraph 25 of this Prudential Standard, 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 ORRC, the ADI's operational risk measurement system must take into account 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 this Attachment.
4. An ADI must have a reliable, transparent and verifiable approach for incorporating data inputs into its operational risk measurement system. The inputs must be combined in a manner that most effectively enables the ADI to quantify its operational risk profile. The ADI's approach for incorporating these inputs should be internally consistent and avoid the double-counting of qualitative assessments or risk mitigants already recognised in other elements of the operational risk management framework.
5. Irrespective of an ADI's operational risk measurement approach, the ADI will be expected to calculate its ORRC through the use of probability distributions of its operational losses. The ADI must demonstrate that it has considered a reasonably comprehensive set of alternative probability distributions and operational risk classifications and that the selected probability distributions most appropriately represent the operational risks in each class.
6. An ADI may use internal estimates of dependence among operational risk losses across operational risk classes if it can demonstrate that its systems for

estimating dependence are sound (particularly for extreme losses), robust under a variety of scenarios (particularly stress scenarios), implemented with integrity and appropriately take into account the level of uncertainty surrounding the estimates. The ADI must validate its dependence assumptions using appropriate quantitative and qualitative techniques. The ADI must sum the risk measures across its operational risk classes to calculate its total ORRC, unless it has received written approval from APRA allowing it to incorporate its dependence assumptions in the calculation.

7. In relation to paragraphs 5 and 6 of this Attachment, to the extent that the choice of distributions or dependence levels and structures is difficult to verify empirically, or is uncertain, the ADI must conduct sensitivity analysis of its ORRC over the considered distributions and over a reasonably comprehensive range of dependence levels and structures. Where the variation in the ORRC over the considered loss distributions or dependence levels and structures is found to be material, the ADI must demonstrate that its estimation procedures are appropriate.
8. An ADI must collect and retain the output of its operational risk measurement system in electronic form for a minimum of five years.
9. An ADI must map its ORRC to the Category 1 business lines detailed in Attachment D. Where the ADI's own internal classification of business activities differs to those detailed in that table, the ADI may map the ORRC to its own business activities, which in turn must be mapped to those defined in this Prudential Standard. This mapping process must be clearly documented.

Data

10. An ADI must have in place policies (as part of its operational risk management framework) relating to its AMA data requirements. These policies must be clearly documented and may vary by types of data. Specifically, the policies must address data quality and align with the corporate data management framework.
11. An ADI must have transparent and verifiable processes for collecting relevant data inputs (refer to paragraph 3 of this Attachment) on an ongoing basis, with associated review and approval processes. These processes must be consistent, timely and comprehensive across the ADI.
12. Assessments of the appropriateness and relevance of data are to be undertaken on a regular basis and must form the basis of any justification for the exclusion of data from the operational risk measurement system. These assessments must be transparent and clearly documented.
13. To maintain data integrity, an ADI must have transparent and verifiable processes to review and approve data adjustments as circumstances require. Such adjustments must be well documented. Where the ADI makes material 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 better reflects the environment in which the ADI operates.

14. The operational risk data inputs used by an ADI in the calculation of its ORRC must be subject to independent review both initially (that is, at the time that AMA approval is sought) and at least annually, to ensure the continued quality of the data and the effectiveness of internal controls. Reviews must include an assessment of the controls surrounding the data collection and maintenance processes, as well as data inspection.³

Internal data

15. An ADI must identify all material operational risk losses consistent with the definition of operational risk detailed in this Prudential Standard.
16. The collection of internal loss data is considered to be an essential element 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 17 to 30 of this Attachment and must form an integral part of the measurement process for an operational risk measurement system to be credible and sufficiently robust.
17. An ADI must have documented policies and procedures for assessing the ongoing relevance of historical internal loss data. Policies and procedures must detail when an operational risk event becomes an operational risk loss for the purpose of collection within the operational risk loss database.
18. An ADI's internal loss data must be comprehensive in that it captures all material losses from all appropriate business activities and geographic locations. The ADI must be able to justify that any excluded activities or losses, both individually and in aggregate, would not have a material impact on the overall estimate of the ORRC.
19. An ADI's thresholds for the collection of internal loss data must be appropriate. In determining a threshold, the ADI must take into account:
 - (a) its approach to operational risk measurement for regulatory capital purposes;
 - (b) the data necessary to justify the predictability and stability of EL offset amounts;
 - (c) the use of internal loss data for operational risk management; and
 - (d) the administrative requirements placed on the business lines and operational risk resources as a consequence of the data collection and management processes.
20. An ADI must include in its operational risk loss database all operational risk related losses in excess of the ADI's specified loss threshold(s). This includes operational risk losses that have typically been regarded as credit or market risk-related losses (refer to paragraphs 27 to 29 of this Attachment).

³ For the purposes of this requirement, 'independent review' means review by a party or parties who are functionally independent within the meaning of paragraph 20 of Attachment A.

21. An ADI must collect information on the gross loss amounts, 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.
22. 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 related operational risk loss events over time.
23. 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. When an ADI first moves to an AMA, a three-year historical data window may be allowed, subject to written approval by APRA.
24. An ADI must map its historical internal loss data to the relevant Category 1 business activities and Category 1 event type categories detailed in Attachments D and E respectively. The criteria used for the ADI's mapping process must be documented.
25. An ADI must develop specific criteria for allocating loss data arising from an operational risk loss event in a centralised function or an activity that spans more than one business line.
26. An ADI must have a well-defined policy for the classification and regulatory capital treatment of operational risk-related credit risk and market risk losses. This policy should be applied consistently across the ADI.
27. Operational risk losses that are related to providing credit – that is, losses that arise from the purported exercise of a credit delegation – must, consistent with the scope and definition of operational risk (refer to paragraph 5(c) of this Prudential Standard) and loss event types (refer to Attachment E), be flagged within an ADI's internal operational risk loss database. The materiality of these **operational risk-related credit losses** may vary within an ADI across business lines and event types. Materiality thresholds should be set with reference to the ADI's internal credit risk management processes.
28. Operational risk-related credit losses must be treated as credit risk for the purpose of calculating an ADI's minimum capital requirement (refer to APS 113) with the exception of fraud (perpetrated by parties other than the borrower), which must be treated as operational risk for the purpose of calculating an ADI's minimum regulatory capital.
29. Operational risk events that are related to market risk must be reflected in an ADI's operational risk profile at the time of discovery (even if positions remain open) and recorded in the operational risk loss database. An ADI applying *Prudential Standard APS 116 Capital Adequacy: Market Risk* for the calculation of its traded market risk, foreign exchange and commodities capital requirement (**TFC capital requirement**) must include open positions resulting from operational risk events in its TFC capital requirement calculation. Operational risk losses that are related to market risk must be treated as operational risk for the purpose of calculating the ADI's minimum ORRC.

30. 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. If an accounting date is chosen for recognition in the internal operational risk loss database and a material known loss has not yet been recognised for accounting or legal purposes, the loss must be incorporated into the ADI's processes for calculating ORRC.

External data

31. 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.
32. The use of external loss data must include the consideration of infrequent yet potentially severe operational risk loss events.
33. External loss data must include, where available, data on the gross 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.
34. 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.

Scenario analysis

35. 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.
36. The set of developed scenarios should be comprehensive and capture all material sources of operational risk across all the ADI's business activities and geographic locations.
37. An ADI's process for developing scenarios must be robust and applied consistently across the ADI. The ADI must have a process in place for reviewing on an annual cycle (if not more frequently) the developed scenarios to ensure they continue to adequately reflect the operational risk profile of the ADI. Over time, scenarios must be re-assessed through comparison to actual loss experience to assess their reasonableness.

Business environment and internal control factors

38. An ADI's operational risk measurement system must incorporate indicators of the ADI's operational risk profile, as well as other information related to the

assessment of the ADI's internal control framework. These indicators, termed **business environment and internal control factors**, are intended to ensure that an ADI's operational risk measurement system is forward-looking and 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 reflect potential sources of operational risk.

39. An ADI must monitor its business environment and internal control factors. The frequency of such monitoring must 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 the Board, or Board committee, reports.
40. Each business environment and internal control factor must have reporting thresholds to ensure there is an effective process that can identify key material risks in a transparent manner and enable the ADI to react appropriately.
41. An ADI must be able to justify its 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 judgement of relevant business areas.
42. Business environment and internal control factors are required to recognise both improvements and deterioration in the ADI's operational risk profile. The operational risk measurement system 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.
43. An ADI must be able to justify the relationship between changes in its measures of operational risk and changes in its business environment and internal control factors. The ADI must also be able to justify the relative weighting of the various factors within its operational risk measurement system.
44. Where possible, business environment and internal control factors should be translated into quantitative measures that lend themselves to verification. The ADI will be required to compare its estimates of these factors with actual internal operational risk loss experience.

Risk mitigation

45. To recognise insurance as an operational risk mitigant, an ADI must be able to demonstrate that the insurance will cover potential operational risk losses included in the operational risk measurement model in a manner equivalent to holding ORRC. 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 & 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 cancellation period of the insurance policy must not be less than 90 days;
 - (c) the insurance policy must not have any exclusions or limitations of liability for losses or expenses caused by or resulting from:
 - (i) any regulatory or supervisory action taken by a statutory authority except where the ADI has sought and received written approval by APRA of the exclusion to be included in the policy; and
 - (ii) liquidation or receivership proceedings against the ADI unless such losses or expenses are incurred prior to the commencement of any such liquidation or receivership proceedings;
 - (d) notwithstanding paragraph 45(c) of this Attachment, the policy may exclude fines, penalties or punitive damages; and
 - (e) the insurance must be provided by a third party entity regulated by APRA or, with APRA's approval, any other entity.
46. 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 its operational risk measurement model.
47. In addition, an ADI's approach to insurance risk mitigation under the 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 to paragraphs 48 and 49 of this Attachment);
 - (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.
48. 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 to paragraph 49 of this Attachment).

49. 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:

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

Sensitivity analysis

50. An ADI must have in place a comprehensive and rigorous program of sensitivity analysis of its operational risk measurement model. Sensitivity analysis must include consideration of the sensitivity of the ADI's ORRC to changes in modelling choices, assumptions and data inputs (including internal data, external data, scenarios and business environment and internal control factors).
51. The results of sensitivity analysis undertaken must be reflected in an ADI's policies and methodology documentation and be communicated to senior management and the ADI's Board, or Board committee, on a regular basis.

Validation

52. An ADI must have a robust system in place to validate the accuracy and consistency of its operational risk measurement model. This system must be documented. The ADI must demonstrate that its validation process enables it to assess the performance of its operational risk measurement model in a meaningful and consistent manner. As part of the validation of its operational risk measurement model, the ADI must regularly compare actual loss experience against its estimates for those losses to ensure their reasonableness.
53. An ADI must have in place a robust process for validating changes to its operational risk measurement model (including data inputs and information outputs in the model). This would include a systematic process for reviewing the appropriateness of modelling assumptions and for making changes to those assumptions.

Attachment C

Allocation mechanisms

1. Approval from APRA under paragraph 32 of this Prudential Standard for the use of an allocation mechanism is conditional upon the ADI demonstrating that:
 - (a) the allocation mechanism is appropriately risk-sensitive and continues to reflect the operational risk profile of the legal entity and its contribution to the banking group;
 - (b) the allocation mechanism is implemented consistently, is empirically supported and continues to be relevant and stable over time;
 - (c) the amount of ORRC that is allocated to the entity continues to be sufficient given the operational risk profile of that entity; and
 - (d) the Board, or Board committee, and senior management have conducted their own assessment of the entity's risks and controls, and are satisfied that the entity continues to be adequately capitalised in respect of operational risk.

2. In addition to the conditions in paragraph 1 of this Attachment, approval from APRA for the use of an allocation mechanism by an ADI that is a locally incorporated subsidiary of a foreign ADI is conditional upon the ADI being able to demonstrate that:
 - (a) the locally incorporated subsidiary complies with the requirements detailed in Attachment A and paragraphs 10 to 44 of Attachment B;
 - (b) the locally incorporated subsidiary is not significant (refer to paragraphs 33 and 34 of this Prudential Standard);
 - (c) the AMA regime of the home supervisor is sufficiently similar to the regime adopted by APRA; and
 - (d) the group-wide AMA allocation mechanism has been approved by the home supervisor and is acceptable to APRA for the purposes of ORRC.

Attachment D

Mapping of business lines

Table 1: Mapping of business lines

Category 1	Category 2	Example of 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 ⁴	External clients	Payments and collections, funds transfer, clearing and settlement.

⁴ Payment and settlement losses related to an ADI's own activities would be incorporated in the loss experience of the affected business line.

Category 1	Category 2	Example of business activities
Agency services	Custody	Escrow, depository receipts, securities lending (customers) and corporate actions.
	Corporate agency	Issuer and paying agent activity.
	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.

Attachment E

Loss event categories

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

Event-type category (Category 1)	Definition	Categories (Category 2)	Activity examples
			Account take-over/impersonation, etc Tax non-compliance/evasion (intentional) 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 property or circumvent the law.	Theft and fraud	Theft/robbery 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

Event-type category (Category 1)	Definition	Categories (Category 2)	Activity examples
		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 (e. g. 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 Market manipulation Insider trading (on the ADI's account) Unlicensed activity Money laundering
		Product flaws	Product defects (unauthorised, etc) Model errors

Event-type category (Category 1)	Definition	Categories (Category 2)	Activity examples
		Selection, sponsorship and 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 (e.g.terrorism or vandalism)
Business disruption	Losses arising from disruption of business or system failures.	Systems	Hardware Software Telecommunications Utility outage/disruptions
Execution, delivery and process management	Losses arising from failed transactions processing, process management, relations with trade counterparties and vendors.	Transaction capture, execution and 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

Event-type category (Category 1)	Definition	Categories (Category 2)	Activity examples
			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