Prudential Standard GOI 3.2

Business Continuity Management (BCM)

Objectives and Key Requirements of this Prudential Standard

This Standard requires insurers to implement an enterprise-wide approach to business continuity management, designed to minimise the impact on critical business operations that could arise from a business disruption.

The key requirements of the Standard are that an insurer must:

- *Have a board-approved policy and related procedures for its objectives and approach in relation to BCM;*
- *Conduct a regular Business Impact Analysis that identifies all its critical business operations and assesses the impact of a material disruption on each of these;*
- *A Business Continuity Plan that includes crisis management and recovery plans; and*
- *A programme for regular review and testing of the Business Continuity Plan.*

Table of Contents

1. Application 1
2. Roles and Responsibilities 2
3. Commencement and Transition Provisions 2
4. Principles 2
5. Minimum Requirements for Business Continuity Management Framework 2
6. Business Impact Analysis 3
7. Recovery Objectives and Strategies 3
8. Business Continuity Planning 3
9. Review and Testing of the Business Continuity Plan 4
10. Notification Requirements 4

1. Application

1.1. This Standard applies to all insurers licensed under the Insurance Act, 2017, other than microinsurers, Lloyd's and branches of foreign reinsurers. The application of these Standards to insurance groups that have been designated as such by the Prudential Authority, under Section 10 of the Insurance Act, 2017, is addressed in a separate standard, GOG 1 (Governance and Operational Standard for Groups).

1.2. Unless otherwise indicated, all references to "insurer" in this Standard can be read as a reference to life insurers, non-life insurers and reinsurers.

2. Roles and Responsibilities

2.1. An insurer's board of directors is ultimately responsible for ensuring that the insurer complies with the principles and requirements of this Standard.

2.2. An insurer's internal audit function, or an external expert, must periodically review the insurer's Business Continuity Plan and provide assurance to the board of directors that the Plan is consistent with the insurer's Business Continuity Management Policy and addresses the risks it is designed to control, and that testing procedures are adequate and have been conducted satisfactorily.

2.3. An insurer's auditor must provide assurance to the insurer and the Prudential Authority, if requested, that the insurer complies with the requirements of this Standard.

3. Commencement and Transition Provisions

3.1. This Standard commences on [XX].

3.2. The final version of this Standard reflects feedback and comments provided to the Prudential Authority in relation to the following draft versions released for consultation:

Draft versions of this Standard released for consultation

Version Number	Release Date	Description
1	26 April 2017	Initial draft of GOI 3.2 released for consultation

4. Principles

4.1. BCM is an enterprise-wide approach that includes policies, standards and procedures for ensuring that critical business operations can be maintained or recovered in a timely fashion, in the event of a disruption. Its purpose is to minimise the financial, legal, regulatory, reputational and other material consequences arising from a disruption.

4.2. Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on an insurer's business functions, reputation, profitability, or policyholders.

4.3. The Prudential Authority requires insurers to have, and to implement, a board-approved policy and related procedures for its objectives and approach in relation to BCM. The policy must address the matters provided for in this Standard.

4.4. The board of directors must ensure that the insurer's business continuity risks and controls are taken into account as part of its overall risk management strategy and when completing a risk management declaration required to be provided to the Prudential Authority under section 8 of GOI 3.1 (Own Risk and Solvency Assessment).

5. Minimum Requirements for Business Continuity Management Framework

5.1. An insurer's BCM framework must, at a minimum, include:

a) a BCM Policy in accordance with section 4.3 above;

b) a regular Business Impact Analysis, including a risk assessment in accordance with section 6 below;
c) recovery objectives and strategies, in accordance with section 7 below;
d) a Business Continuity Plan that includes crisis management and recovery plans in accordance with section 8 below; and
e) programs for:
    i. review and testing of the Business Continuity Plan in accordance with section 9 below; and
    ii. training and ensuring awareness of staff in relation to BCM.

6. Business Impact Analysis

6.1. A Business Impact Analysis involves an insurer identifying all its critical business operations (functions, resources and infrastructure) and assessing the impact of a material disruption on each of these. The Business Impact Analysis should pay attention to potential disruption arising from all material risks, but with special attention to risks related to information technology and cyber attacks (see GOI 3 (Risk Management and Internal Controls)).

6.2. A Business Impact Analysis must be conducted at least annually, or more frequently if there are material changes to business operations, or when so directed by the Prudential Authority.

6.3. When conducting the Business Impact Analysis, an insurer must consider:

a) plausible disruption scenarios over varying periods of time;
b) the period of time for which the insurer could not operate without each of its critical business operations;
c) the extent to which a disruption to the critical business operations might have a material impact on the interests of the insurer's policyholders; and
d) the financial, legal, regulatory and reputational impact of a disruption on the insurer's critical business operations over varying periods of time.

7. Recovery Objectives and Strategies

7.1. Recovery objectives are pre-defined goals for recovering critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.

7.2. An insurer must identify and document appropriate recovery objectives and implementation strategies based on the results of the Business Impact Analysis and the size and complexity of the insurer.

8. Business Continuity Planning

8.1. An insurer must maintain at all times a documented Business Continuity Plan that meets the objectives of the Business Continuity Policy.

8.2. The Business Continuity Plan must document procedures and information that enable the insurer to:

a) manage an initial business disruption (crisis management); and
b) recover critical business operations.

8.3. The Business Continuity Plan must reflect the specific operational requirements of the insurer and must identify:

a) critical business operations;
b) recovery levels and time targets for each critical business operation;
c) recovery strategies for each critical business operation;
d) infrastructure and resources required to implement the Business Continuity Plan;
e) roles, responsibilities and authorities to act in relation to the Business Continuity Plan; and
f) communication plans with staff and external stakeholders.

9. Review and Testing of the Business Continuity Plan

9.1. An insurer must review and test its Business Continuity Plan at least annually, or more frequently if there are material changes to business operations, to ensure that the Business Continuity Plan can meet the Business Continuity Management objectives. The results of the testing must be formally reported to the board of directors.

9.2. The Business Continuity Plan must be updated if shortcomings are identified as a result of the review and testing required above.

10. Notification Requirements

10.1. An insurer must notify the Prudential Authority as soon as possible, but no later than 24 hours, after experiencing a major disruption that has the potential to have a material impact on the insurer's risk profile, or affect its financial soundness. The insurer must explain to the Prudential Authority the nature of the disruption, the action being taken, the likely effect and the timeframe for returning to normal operations. The insurer must notify the Prudential Authority when normal operations resume.

10.2. The information or notifications required by this Prudential Standard must be given in such form, if any, and by such procedures, if any, as the Prudential Authority determines and publishes on its website from time to time.