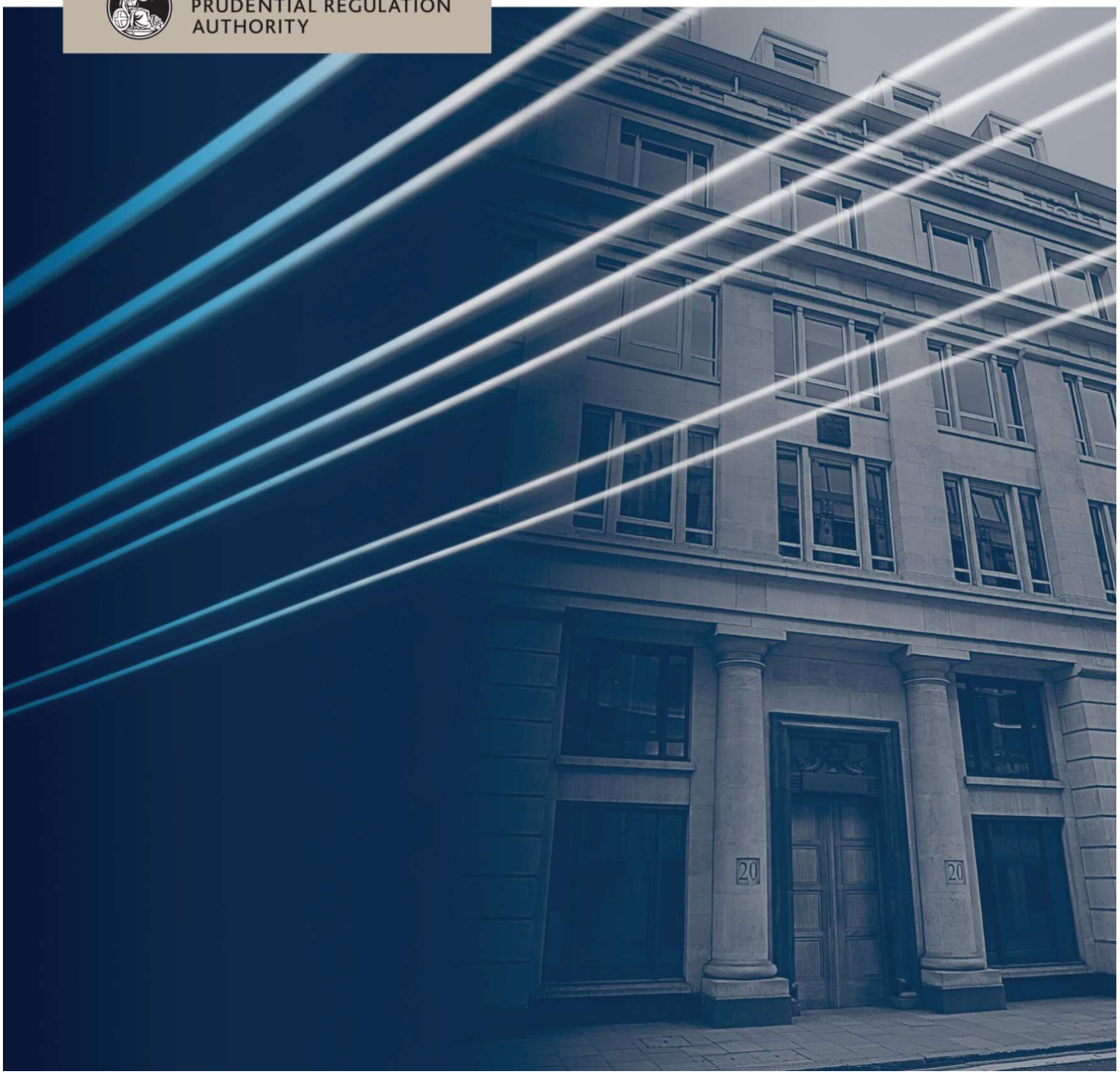
Supervisory Statement | SS4/17

Cyber insurance underwriting risk

November 2024

(Updating July 2017)



Prudential Regulation Authority
20 Moorgate
London EC2R 6DA

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Supervisory Statement | SS4/17

Cyber insurance underwriting risk

November 2024

(Updating July 2017)

Contents

1 Introduction

1.1 This supervisory statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations of firms regarding cyber insurance underwriting risk. For the purposes of this SS cyber insurance underwriting risk is defined as the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (eg cyber attack, infection of an IT system with malicious code) and non-malicious acts (eg loss of data, accidental acts or omissions) involving both tangible and intangible assets.

1.2 This statement follows a cross-industry review conducted between October 2015 and June 2016. The key findings were published in a letter to firms on 14 November 2016.[1]

1.3 This SS is relevant to all UK non-life insurance and reinsurance firms and groups within the scope of Solvency II including the Society of Lloyd's and managing agents ('Solvency II firms').

1.4 This SS should be read in conjunction with:

- the PRA's rules in the Solvency II sector of the PRA Rulebook, in particular rule 3.1 of the Conditions Governing Business Part, and the Insurance Senior Management Functions and Technical Provisions Parts;
- the PRA's approach to insurance supervision;[2]
- the European Insurance and Occupational Pensions Authority (EIOPA) Guidelines, particularly Guidelines 3, 17, 19, 20, 46, 47, 50, 56 and 61 on Systems of Governance and Valuation of Technical Provisions;[3] and
- Valuation 5, 7, and Technical Provision: Further requirements 2, 3 of the PRA Rulebook.

1.5 This SS expands on the PRA's general approach as set out in its insurance approach document. By clearly and consistently explaining its expectations of firms in relation to the particular areas addressed, the PRA seeks to advance its statutory objectives of ensuring the safety and soundness of the firms it regulates, and contributing to securing an appropriate degree of protection for policyholders.

1.6 The PRA expects firms to be able to identify, quantify and manage cyber insurance underwriting risk. This includes both of the following sources of cyber insurance underwriting risk:

(a) affirmative cyber risk, ie insurance policies that explicitly include coverage for cyber risk; and

(b) non-affirmative cyber risk, ie insurance policies that do not explicitly include or exclude coverage for cyber risk . This latter type of cyber risk is sometimes referred to as 'silent' cyber risk by insurance professionals.

1 'Cyber underwriting risk': www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf.
2 Available at: www.bankofengland.co.uk/publications/Pages/other/pra/supervisoryapproach.aspx.
3 https://eiopa.europa.eu/Publications/Guidelines/TP_Final_document_EN.pdf.

1.7 The PRA's expectations are split into three broad areas:

- non-affirmative cyber risk (Chapter 2);
- cyber risk strategy and risk appetite (Chapter 3); and
- cyber expertise (Chapter 4).

2 Non-affirmative cyber risk

2.1 The PRA expects that all Solvency II firms robustly assess and actively manage their insurance products with specific consideration to non-affirmative cyber risk exposures. This includes all property and casualty (P&C) covers which could give rise to cyber risk exposure from physical and non-physical damage. Such firms are expected to introduce measures that reduce the unintended exposure to this risk with a view to aligning the residual risk with the risk appetite and strategy that has been agreed by the board. To achieve this, besides making adequate capital provisions that clearly link with this risk, as they would for any other risk type, firms could consider any of the following (the list is not exhaustive):

- adjusting the premium to reflect the additional risk and offer explicit cover;
- introducing robust wording exclusions; and/or
- attaching specific limits of cover.

2.2 Should a firm decide to offer cyber cover at no extra premium for a specific product or line of business, the PRA would expect to see that the board has confirmed that a comprehensive assessment of the potential resulting losses has been carried out, and that the overall non-affirmative cyber exposure falls within the stated risk appetite. In this case the contract may be reworded to clarify that cyber cover is offered as part of this product or line of business.

2.3 The PRA is not a pricing regulator and does not look to design products. The short-to-medium term aim is to enhance the ability of firms to monitor, manage and mitigate non-affirmative cyber risk and to increase contract certainty for policyholders as to the level and type of coverage they hold. The PRA expects firms to adopt a proportionate approach when assessing their non-affirmative exposures. The firm's underwriting and risk management functions should play a key role in leading this effort.

3 Cyber risk strategy and risk appetite

3.1 Cyber underwriting is a key area of risk and it is important that this is reflected in the firm's strategy and risk appetite statements.

3.2 The PRA expects that all Solvency II firms that underwrite affirmative cyber insurance policies and/or those that are exposed to non-affirmative cyber risk will have clear strategies on the management of the associated risks, which are owned by the board. The cyber strategy should include clearly articulated risk appetite statements with both quantitative and qualitative elements, for example defining target industries to focus on, strategy for managing non-affirmative cyber risk, specifying rules for line sizes, aggregate limits for industries, splits between direct and reinsurance, etc. (this list is not exhaustive).

3.3 The overall cyber strategy, associated risk appetite statements and relevant management information (MI) should be reviewed on a periodic basis by the board. The strategy and overall exposure levels of non-affirmative cyber risk should be reviewed by the board at least on an annual basis. For affirmative cyber risk the review should be more regular. The MI should include as a minimum:

- clear articulations of the risk appetite statements and measurements against these;
- aggregate cyber underwriting exposure metrics for both affirmative and non-affirmative cyber risk; and
- cyber insurance underwriting risk stress tests that explicitly consider the potential for loss aggregation (eg via the cloud or cross-product exposures) at extreme return periods (up to 1 in 200 years) and are consistent with the general insurance stress tests carried out periodically by the PRA.

3.4 By articulating these issues boards will understand and own the overall strategy for cyber risk and the associated prudential risks.

4 Cyber expertise

4.1 Both affirmative and non-affirmative cyber risk elements present significant challenges and are underpinned by technological development. Firms active in this space are faced with the necessity of investment in knowledge and expertise.

4.2 The PRA expects that all Solvency II firms that are materially exposed to these risks understand the continuously evolving cyber landscape and demonstrate a continued commitment to developing their knowledge of cyber insurance underwriting risk. This extends to both affirmative and non-affirmative elements of cyber risk. The PRA expects that this knowledge and understanding should be fully aligned to the level of risk and any growth targets in this field, and should cover all three lines of defence (business, risk management, and audit).

4.3 Regardless of any external input or advice obtained in relation to such risks, responsibility and accountability for this risk remains with the firm. The firm will be responsible for the appropriate management of these risks. The PRA expects the board to have oversight of the effectiveness of the firm’s risk management and controls in this area.

4.4 In this way, firms will have sufficient expertise to understand the risks associated with cyber insurance underwriting.

Appendix: SS4/17 updates

This appendix details the changes that were made to this SS following its initial publication.

15 November 2024

This SS has been updated alongside the publication of Policy Statement (PS) 15/24 - Review of Solvency II: Restatement of assimilated law.[4] This includes updating all previous references to the Commission Delegated Regulation (EU) 2015/35 so as to now refer to the relevant rule(s) in the PRA Rulebook.

4 www.bankofengland.co.uk/error/404.html?item=%2fprudential-regulation%2fpublication%2f2024%2fnovember%2freview-of-solvency-ii-restatement-of-assimilated-law-policy-statement