HSBC

7 June 2018

General Manager Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2000

By email: PolicyDevelopment@apra.gov.au

Dear Sir/Madam,

Discussion Paper
Information Security Management: A new cross-industry prudential standard

HSBC Bank Australia Limited and The Hongkong and Shanghai Banking Corporation Sydney Branch (collectively 'HSBC') welcomes the opportunity to provide comments on the Discussion Paper *Information Security management: A new cross-industry prudential standard.*

In relation to the Discussion Paper and the draft *Prudential Standard 234 information Security,* HSBC has participated in the industry discussions led by the Australian Banking Association (ABA) and the Australian Financial Markets Association (AFMA). We support their submissions.

Further, we have undertaken a review of the draft *Prudential Standard CPS 234 Information Security* and wish to provide the following additional comments in regard to the draft Standard.

Materiality, Proportionality and Third Parties

As a member of the global HSBC Group, contracts are executed on our behalf by our parent entity and vice versa. Renegotiation of such international contracts for the benefit of one jurisdiction may create an unintended level of complexity and concerns in other jurisdictions and with offshore regulators. We suggest APRA considers the impact of potential scope and complexity when finalising the implementation timeframe.

We note that the draft wording in general across the Standard does not specifically define any particular scope, size or materiality thresholds. We believe this approach leaves the Standard open to a broad interpretation where entities could adopt different approaches and scope of application across the industry. In particular when negotiating contracts with third parties, many of whom are likely be held in common with our peers, it will be important for a consistent understanding, interpretation and scope of application of regulatory standards to be available.

We suggest APRA consider providing the industry with further guidance on acceptable methods to assess third party assets. For example paragraphs 12 and15 refer to an assessment being 'commensurate with the size and extent of threats to those assets'. To enable an appropriate risk-based approach to be implemented it would be useful to clarify if this

HSBC Bank Australia Limited
ABN 48 006 434 162 AFSL 232595
Level 36 Tower 1, International Towers Sydney,
100 Barangaroo Avenue, Sydney NSW Australia 2000
Tel: (02) 9006 5888 Fax: (02) 9006 5570
www.hsbc.com.au

requirement applies to all third party relationships (including affiliated entities) and further sub-contract arrangements.

We also support the use of cloud technologies and would encourage the Standard to be practically applicable to and inclusive of traditional and new technologies, including those used by third parties, which may be global in nature and external to the Australian regulatory environment.

Notification

We suggest APRA consider the notification requirements and in particular provide a clear definition with respect to the timing and severity expectations under paragraph 34. When experiencing an issue of this nature the initial focus will be on rectification of the issue and any customer impact. We would encourage an approach that provides a reasonable time period to address the triage situation and then provide notification to the regulators, for example, we suggest alignment with notification timelines expressed in CPG 220 *Risk Management* ("as soon as practicable, and no more than 10 business days, after it becomes aware"). Additionally to avoid lack of clarity or duplication of regulatory reporting (both on and offshore), we support the use of a standardised reporting method or template.

We thank APRA for considering our comments and should you have any questions, please do not hesitate to contact Merydith Clark, Head of Security Risk.

Yours sincerely,

Noel McNamara
Chief Risk Officer
HSBC Bank Australia Limited