Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 24 April 2024*

Location: *Held remotely, via MS Teams*

Time: *11:00 to 12:00*

Meeting: *Meeting # 1*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Sameer Bedi, NAB
Darren Booth, RSM Australia
Vincent Cheen, Mastercard
Tilen Chetty, Mastercard
Nick Dawson, Frollo
Olaf Grewe, NAB
Macklin Hartley, WeMoney
Ben Kolera, Biza
Harish Krishnamurthy, ANZ
Stuart Low, Biza
Julian Luton, CBA
Brad McCoy, Basiq
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Nils Berg, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Hemang Rathod, DSB
Christine Williams, DSB
David Franzmann, ACCC
Rio Dose, Excelium
Ross Udemans, Excelium
Elaine Loh, OAIC
Chrisa Chan, Treasury

Apologies

N/A

Chair Introduction

Mark Verstege, the Chair of the Information Security (Info) Consultative Group welcomed everyone to the first InfoSec Consultative Group meeting, acknowledged the traditional owners of the lands, and set out the purpose and expectations of the group.

He provided background that these consultative groups were a new concept and are formal consultative groups which are set up under legislation. The group will trial 6 x meetings to provide feedback and determine if they should continue in a more permanent form.

Purpose and structure of the InfoSec Group

The Chair noted that they have invited ACCC, Treasury and OAIC along with the current security health check supplier Excelium to attend these meetings as observers.

The Chair noted that this is a consultative group, and whilst we'll make decisions about what we're doing within the group, we are not decision makers. Our input will feed into the existing mechanisms for the Data Standards Body (DSB) and the Data Standards Chair and will still need to go out for broader community consultation to make sure that everyone has the opportunity to provide input.

The Chair noted that this group is focussed on the Data Standards and not the broader Rules, however we may discuss issues that the rules create which we could include in the findings report.

Members Introductions

The Chair invited attendees to introduce themselves in the chat due to the number of attendees.

Governance

Terms of Reference & Code of Conduct

The group discussed the proposed Terms of Reference (TOR) and Code of Conduct, which incorporates sensitive information handling, and agreed to provide any additional feedback before approving them at the next meeting.

ACTION: Group to provide any additional feedback on TOR and Code of Conduct prior to next meeting

Ways of Working

The Chair noted that the minutes of the InfoSec Consultancy Group will be published on the Consumer Data Standards website.

Minutes will be prepared and reviewed by the group with feedback incorporated into the published version. Specific comments will not be attributed to individual members as part of the published minutes.

The meetings are also recording for note taking purposes only.

The Chair noted that key outputs from the discussions will be fed back to the Data Standards Advisory Committee (DSAC) and at the weekly Implementation Calls and they will ensure that they share only what is appropriate.

The group discussed and agreed to meet fortnightly for 2 hours on a Wednesday or Thursday. The group would also use GovTEAMS and GitHub for online collaboration and to work on issues and draft standards between meetings.

ACTION: DSB to send out invites to upcoming meetings and GovTeams

Overview of uplift priorities and next steps for authentication uplift

The Chair noted that authentication uplift would be the initial priority and to work through the feedback received from Decision Proposal 327. They should also include other related topics and agreed to further define the scope and priorities of the group.

Decision Proposal 327 consulted on:

- Implementing OTP authenticator recommendations from the 2022 Independent Health Check.
- Support for authenticators beyond OTP by permitting authenticators within TDIF's Credential Levels.
- A risk-based approach to defining baseline Credential Levels for data sharing and action initiation.
- Extending permitted interaction flows beyond 'Redirect with OTP', including supporting:
  - App2App authentication flow; and
  - Decoupled authentication flow using CIBA.
- Restricting credentials that do not satisfy best practice.

The priorities for this consultative group include:

- Defining a practical risk-based framework for data sharing and action initiation
- Balancing Data Holder discretion with a consistent economy-wide consumer experience
- Determining when and how prescription shall be applied including when alternative interaction flows be required
- Determining the pathway for retiring credentials that do not satisfy best practice

Further areas of uplift that have been identified for prioritisation include:

- Authentication Uplift including decoupled and App2App authentication.
- Rich authorisation for data sharing.
- Rich authorisation for action initiation.
- Migration of the Security Profile to the FAPI 2.0 Security Profile + Message Signing Profile.
- A framework for sharing secure event and notifications between participants.
- CDR authorisation receipts.
- Enhanced participant discovery mechanisms.
- A CDR Cyber Threat Scenario Modelling and Attacker Model.
- Interoperability with Digital ID.

One member noted that the differences in how current standards are implemented across banks are affecting consumer experience, security risk, and drop-off rates.

Another member raised concerns about potential impacts on abandonment rates from introducing additional authentication steps, especially for smaller data holders relying on third party platforms.

One member emphasized the importance of not forcing all data holders to take the same approach but allowing flexibility to solve challenges differently based on their capabilities. Another member agreed on avoiding overly prescriptive requirements and focusing more on desired security outcomes rather than exactly how authentication is achieved.

One member suggested alignment to existing customer authentication experiences that already meet required levels, rather than introducing additional CDR-specific friction. They proposed allowing flexibility to organisations without existing authenticators to experiment within CDR while working towards improved security.

The Chair proposed focusing next steps on formulating questions to frame potential solutions, balancing prescription versus discretion, developing a set of problem definition statements and setting minimum security requirements as a baseline.

The group agreed that the next step is to collaborate on defining key questions related to the authentication standards update.

The Chair noted that invites will be sent to the group to join GovTEAMS and we can start that discussion and collaborate there.

Any Other Business

No other business was raised.

Closing and Next Steps

The Chair thanked everyone for attending the first InfoSec meeting and being part of the consultative group.

Meeting closed at 11:58