Australian Government | data standards body

Data Standards Body

Information Security (InfoSec) Consultative Group
Minutes of the Meeting

Date: Wednesday 19 March 2025

Location: Held remotely, via MS Teams

Time: 10:00 to 12:00

Meeting: Meeting # 19

Attendees

Committee Members

Mark Verstege, DSB
Sameer Bedi, NAB
Olaf Grewe, NAB
John Harrison, Mastercard
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Mark Wallis, Skript

Observers

Nils Berge, DSB
Chrisa Chan, TSY
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Matt Shaw, DSB
Abhishek Venkataraman, ACCC
Fiona Walker, TSY
Christine Williams, DSB

Apologies

Darren Booth, RSM
Nick Dawson, Frollo
Macklin Hartley, WeMoney
Kyle Jaculli, ACCC
Michael Palmyre, DSB
Tony Thrassis, Frollo

Chair Introduction

Mark Verstege, the Chair of the Information Security (InfoSec) Consultative Group welcomed everyone to the meeting, acknowledged the traditional custodians of the land and paid respect to elder's past, present and emerging.

The Chair noted that members Darren Booth (RSM), Nick Dawson (Frollo), Macklin Hartley (WeMoney) and Tony Thrassis (Frollo) were apologies for this meeting. A number of observers also sent their apologies.

The Chair outlined the agenda, which included updates on planned consultations, the extension of the consultative group and a follow up on action items.

The Chair noted that prior to the Data Standards Chair Mr Andrew Stevens finishing his term at the end of February 2025, he approved a refresh of the consultative group, which included an expansion to incorporate non-bank lending (NBL) and energy participants. This refresh is currently being considered by the new Chair Dr Ian Opperman who commenced on 1 March 2025, and we hope to provide an update shortly.

The Chair noted that the consultation paper on best practice security was circulated to the Data Standards Advisory Committee (DSAC) for comment and feedback. The feedback along with CDR agency feedback has been incorporated and is for consideration by the new Chair before publishing.

The Chair noted that the redirect to app decision proposal is planned to be published at the same time as the best practice consultation paper. He noted that apart from formatting changes the substance has not change significantly from the draft versions of these papers.

Minutes

Minutes

The Chair thanked members for their comments on the Minutes from the 20 February 2025 meeting. The Minutes will be formally adopted and published on the Consumer Data Standards (CDS) website.

Action items

The Chair noted that there was an outstanding action for the group to continue providing feedback on defining measurable ongoing outcomes and metrics. The plan was to discuss metrics and measurement, both for authentication across redirect to app and for subsequent decision proposals, at the next meeting.

ACTION: Add “defining measurable outcomes and metrics” as an agenda item to next meeting

One member confirmed that he would get back to the group about the list of limitations and differences between the current CDR standards and FAPI 2 compliance for further discussion.

ACTION: Member to provide a list for discussion at next meeting

Recap of Best Practice Security Consultation Paper

One member suggested that it would be good to have pre-reading material distributed before the meeting, including the Miro board link, rather than providing it during the meeting.

The Chair agreed to provide the links in future papers.

ACTION: DSB to include the Miro link and password in future papers

The Chair noted that the paper aims to establish best practice security in authentication by outlining the threat environment, analysing current sector and practices and identifying limitations in current authentication standards within the CDR.

The paper proposes a direction for consulting on the uplift of authentication standards and requests feedback through surveys from the NBL and banking sectors. Key changes from the last version include:

- ADR authentication out of scope
- Moving the risk and threat analysis to an appendix
- Updating privacy safeguard references based on internal feedback
- Incorporating DSAC feedback
- Updating consultation template formats to align with how rules represent a draft Rules package and Explanatory Statement.

It was noted that the intention is to publish the consultation paper as soon as possible after review by the new Chair.

Recap of Minimum Baseline Security Decision Proposal

The Chair noted that the objective is to improve security and consumer experience, reduce authorisation drop-offs, reduce prescription, reduce compliance and maintenance costs, encourage innovation, and ensure security controls are commensurate with the risk of unauthorised data disclosure. This approach involves:

- Define a minimum baseline for authentication security across the CDR
- Remove OTP and single-factor authentication limitations
- Develop a risk-based authentication framework

- Provide data holders (DHs) with the choice to select the appropriate authentication factors

The four models considered for the risk-based framework:

- Option 1: DHs may voluntarily provide stronger authentication
- Option 2: Data standards define credential levels (CL) based on data sensitivity classification
- Option 3: Data Standards prescribe CL2 for all data access
- Option 4: Combination of Option 1 and Option 2 CLs based on the identity proofing requirements of a sector

The preferred approach is to create a framework that allows DHs to adopt alternative authentication factors beyond OTP, commensurate with the risk of the data being disclosed.

Updated risk-based authentication framework

The Chair noted that the risk-based framework provides a principle-based approach to support DHs and Accredited Data Recipients (ADRs) to determine the appropriate authentication level required to authenticate users for accessing consumer data or authorising the disclosure of CDR data.

The purpose is to develop a framework and profiling of NIST around risk management for cybersecurity. The goal is to create a framework that allows DHs to apply an objective risk assessment to determine the level of authentication assurance required. The framework is based on NIST's digital ID guidelines and aims to be adaptable for future datasets and action types beyond data sharing.

Key definitions include:

- **User:** either the individual consumer or a nominated representative on behalf of a non-individual consumer
- **Authenticating entity:** generally, a DH, ADR or accredited person providing the CDR service where the user is authenticating

The framework considers five impact categories from NIST:

- Harm to the authenticating entity or user's interests
- Damage to trust, standing, or reputation
- Unauthorised access to information
- Financial loss or liability
- Loss of life or danger to human safety or health

The framework aims to provide a consistent mechanism for DHs to apply a risk-based approach to authentication, considering the potential harms and likelihood of those harms.

One member raised several queries and concerns regarding the proposed risk-based authentication framework. He pointed out the use of the word "you" in the Terminology and Definitions section, suggesting it should be avoided to align with standards.

The member raised concerns about the practicality and binding nature of the risk-based framework questioning whether the working group had the qualifications to define these rules as they are a technology working group, not a risk working group. He also questioned the suitability of the framework for organisations without established risk and compliance capabilities.

The member also highlighted that the framework might be unachievable for energy companies and non-bank lenders (NBLs), as they may not currently have such risk frameworks in place.

The member noted that the mutual sector, which relies on vendors for compliance, would struggle to meet the requirements of the proposed framework. He emphasised that most organisations do not have a full-time CDR compliance person and depend on technology vendors for solutions.

The Chair acknowledged the members feedback which he found helpful. He suggested considering the feedback in the context of addressing the limitations identified previously with the proposed options. For example, option 2 is only defined on the current data clusters within the standards and how would that work if a DH were to offer a voluntary standard.

One member emphasised that the framework seemed suitable for the big four banks only and would impose significant costs and challenges to other organisations.

One member expressed uncertainty about the practicality of making the risk framework binding and the challenges of attesting to compliance beyond just signing a letter. He emphasised many organisations already have fraud and risk systems in place, and reconciling these with a new risk-based approach might be complicated. He suggested that the biggest achievement through this exercise would be ensuring that existing authentication methods are used and that there is flexibility in the strength of these methods, either through a prescribed level or a risk-based approach.

One member sought to understand whether the proposed risk framework would significantly impact the majority of the ecosystem, particularly smaller DHs.

One member mentioned that his company serves about 50 of the DHs in the ecosystem out of 200 in total. He emphasised that what the big four banks consider ‘normal risk management practices’ are not standard for mutuals and other smaller DHs, who rely on outsourcing and certifications like SoC 2 and ISO for their risk assessments.

The member expressed concern that making the proposed framework binding would impose significant costs and challenges, especially for smaller DHs and sectors like energy and NBL's, which may not have standardised risk management frameworks. He suggested that while a prescriptive standard should be provided, there should also be an option for DHs to propose their own risk-based framework and have it approved by the regulator. This approach would allow organisations that do not want to follow the prescribed standard to present their case and potentially use their own framework, thus providing flexibility while maintaining a baseline standard for others.

One member suggested that the current discussion on risk management might benefit from involving the risk working group to check in on their processes and ensure alignment.

One member raised concerns about the hierarchy of regulations and standards, particularly in the banking sector. He emphasised that higher-level regulations, such as those from APRA would take precedence over the CDR Data Standards. He also mentioned that NIST is a framework, not a standard and expressed caution about turning frameworks into binding standards.

The DSB acknowledged the feedback and concerns raised about the proposed risk-based framework for authentication. He emphasised the original intent of the framework, which was to provide more flexibility for DHs while ensuring strong authentication practices.

One member inquired about approaches taken in other regions specifically the UK, and how they handle risk-based approaches to authentication and whether their methods could inform the current discussion.

One member explained that the structure of banking in the UK and the drivers behind their regulations are different. He noted that the UK had a separate regulation dealing with strong customer authentication with a risk-based approach conditionally applied, depending on the amount.

One member noted that this working group is addressing issues that ideally should have been resolved at the rules level which would have provided a clearer framework for the technical implication.

One member emphasised that if there is any difference between what Australian Prudential Regulation Authority (APRA) says and what the DSB prescribes, APRA's regulations will take precedence.

One member reiterated the idea of an "escape hatch" where organisations that do not want to follow the prescriptive standard can present their own risk framework to the regulator for approval.

This would allow flexibility while ensuring a clear, accepted standard for those who need it. He therefore wondering if it is option 4 plus an “escape hatch” on a case-by-case basis.

One member mentioned that scaling considerations are important, and adding new data each time could create many back-and-forth conversations. He agreed with having both a prescription and a framework which provides guidance on what is acceptable, reducing the need for frequent exemptions.

One member suggested that instead of prescribing a specific framework, the Data Standards could provide a matrix of approved frameworks that are aligned. He emphasised the need for optionality, proposing that the standards could include a mapping of data clusters to CLs across different frameworks like TDIF and NIST. This approach aims to offer flexibility while ensuring consistency and compliance.

The DSB suggested extending the current baseline from OTP to a stronger multi-factor authentication (MFA) which allows DHs to use their existing authentication methods, provided they meet the new baseline or a risk-based approach.

One member commented that TDIF is a standard with very prescriptive role requirements for achieving different CLs. He expressed concern that TIDF does not account for the risk analysis performed during customer authentication flows, such as considering the location or behavior of the user. He emphasised that TDIFs prescriptive nature might introduce unnecessary friction into CDR consent flows, potentially impacting the overall user experience.

The Chair summarised the discussion by emphasising the need to define suitable guardrails for authentication in the CDR, considering the risk to consumers and authenticating entities. He acknowledged the spectrum of security controls across different sectors and the challenge of creating a technically implementable solution that provides clear and specific standards without imposing excessive prescription on DHs. He highlighted the importance of balancing flexibility and consistency to ensure that all DHs implement sufficient controls to protect consumer data.

One member raised concerns about implementing specific authentication standards for app-to-app consent flows could inadvertently dictate how all customers log into their banking apps, not just for CDR purposes. This could lead to unnecessary friction for users who are not engaging with CDR. He emphasised that the current regulatory environment already requires banks to ensure secure authentication methods, and adding another layer of regulation might be redundant and potentially counterproductive. He suggested that the DSB should consider the broader impact of these standards on everyday banking operations and whether it is within their remit to enforce such changes.

One member emphasised that banks have historically resisted taking on liability for CDR, which contrasts with their approach to digital banking where they do assume liability. This resistance impacts the authentication methods and the overall approach to security in CDR.

The Chair highlighted the practical steps moving forward, focusing on the need to create a workable set of technical standards for authentication in the CDR. Key points included:

- To discuss the risk framework internally with CDR agencies to ensure a balanced approach for all sectors
- Progressing with a prescription-based approach considering the feedback and concerns raised during the meeting

One member mentioned the need to discuss Service Level Agreements (SLAs) and the conversation around metadata in the SSA (Service Security Agreement) at a future meeting. He expressed concerns about the complexity and practicality of changing metadata every time it needs to be added or updated, suggesting a more streamlined approach.

The Chair asked the member to provide a list of problems that need to be solved regarding the register and SLAs. This would help anchor the discussion and provide a clear focus for addressing the issues.

ACTION: Member to provide a list of problems that need to be solved regarding the Register

One member suggested a discussion around FAPI 2 should be included in the next meeting. They were interested in understanding what specific changes need to be implemented.

Meeting Schedule

The Chair advised that the next meeting would be held remotely on Wednesday 2 April 2025 from 10am to 12pm.

Any Other Business

No other business was raised.

Closing and Next Steps

The Chair thanked members for attending the meeting.

He noted that the next meeting will include discussions on measuring success metrics, FAPI 2 gap analysis, NBL white labelling and register concerns. Additionally, there will be a standing agenda item for the risk framework topic.

Meeting closed at 11:57