CUSTOMER OWNED BANKING CODE COMPLIANCE COMMITTEE

Completing the 2024 Customer Owned Banking Annual Compliance Statement (ACS)

Your ACS is due on or before ***30 September 2024***.

Before you begin

- Review your internal policy and procedures relating to Code compliance.
- Assess and verify your staff awareness of Code obligations.
- Review your staff training to include compliance with Code obligations.
- Review your Code compliance reporting and monitoring process.
- Assess and verify your Code compliance data.
- Review your internal complaints reporting and monitoring process.
- Assess and verify your internal complaints data.

When completing the ACS

- Record data for the reporting period ***1 July 2023 to 30 June 2024***.
- Provide enough information to address each item in full.
- Highlight any changes to frameworks, processes or procedures in this period.
- Ensure the data you provide is accurate and complete.
- Ensure the data does not include any personal, private or identifiable information.
- Upload any necessary supporting documents.

After you submit

- We recommend you download a copy of your final submission.
- We may contact you if we need more information to assess your compliance with the Code.

Further assistance

- Daniela Kirchlinde, Senior Manager Code Compliance
  dkirchlinde@codecompliance.org.au
- Tania Meadows, Senior Compliance Analyst
  tania.meadows@codecompliance.org.au

Contents

About the Annual Compliance Statement

The 2022 Customer Owned Banking Code of Practice

The *2022 Customer Owned Banking Code of Practice* (2022 Code) became effective 31 October 2022. It replaced the 2018 Code and sets out extensive obligations for subscribers as well as principles and values that underpin the way they promise to deal with customers and the broader community.

It contains a new focus on accessibility and inclusivity with obligations for supporting the needs of customers experiencing vulnerability – an emerging issue that is changing the way customer owned banking institutions approach their relationships with customers.

Following a minor variation to paragraph 91 of the 2022 Code, which was approved by the Australian Competition and Consumer Commission (ACCC), the amended 2022 Code v2.0 is effective 28 October 2023.

Customer Owned Banking Code Compliance Committee

The *Customer Owned Banking Code Compliance Committee* (COBCCC) is the Code's independent compliance monitoring body. In accordance with its Charter and the Code, the COBCCC monitors compliance with the Code, identifies systemic industry-wide issues and promotes good industry practice to improve customer outcomes.

Purpose of the Annual Compliance Statement

The Annual Compliance Statement (ACS) program is a central component of our monitoring work.

It asks for information about your Code compliance frameworks, including breach and complaints reporting and monitoring, as well as your institution's overall compliance culture.

The ACS helps us to:

- benchmark compliance with the Code
- report on current and emerging issues in Code compliance to the industry and wider community, and
- establish the areas of priority for our future monitoring work.

Data collected through the ACS program will be aggregated, de-identified, analysed for trends and patterns, and published in the *COBCCC's Annual Data Report*. We will also provide data to you via individualised Benchmark Reports.

See *previous publications on our website*.

Development of the ACS

We value the feedback you provide when completing the ACS. We have taken on board your feedback and addressed some of your recommendations in our revised 2024 ACS.

In addition, we have worked with COBA and a selection of Code subscribers to consult on our compliance monitoring activities.

Changes to the ACS

The following changes were made to the 2024 ACS:

Table 1: Changes to the 2024 ACS

Part	*Description of the change*	*Reason for the change*
A. Declaration		
A.	Certification of ACS to be completed by CEO or a Senior Executive.	Following feedback, we have updated the certification details to allow for a Senior Executive to sign off on the ACS. You informed us that a CEO may not always be available or the appropriate person to sign off on the ACS.
C. Code Breach reporting		
C.1 Updated columns	The following changes have been made to the requested information: • Rearranging of columns. Column D now asks for *Number of Breaches* and Column F asks for the *Description of Breach(es).* • Removal of Business Unit / Division column. • Columns G & H added for reporting *Number of Incidents and comment*. • Removal of timeframes for immediate and long-term remedial action(s), including comment columns. • Renamed columns. Column S now *Remedial Action(s) for Customer(s)*. Column T now *Remedial Action(s) to Prevent Reoccurrence*.	The changes to the **2024 *Breach Data Report*** were made to optimise the information provided in the report. We use this information as part of our Benchmark Report and Annual Data Report. Based on industry's feedback, strategic directions regarding immediate and long-term remedial action are now captured in question C.2.
C.1 Updated drop-down menu options	• Additional options for multiple product/service types (column I) and identification methods (column K). • Amendment of categories for root cause of breaches (column M). • Amendment of categories for Remedial Action(s) for Customer(s) (column S).	Changes to the drop-down menu have been made based on industry's feedback to consolidate Code breach reporting and/or align with *ASIC Breach Reporting Regulatory Guide 78* (RG 78).

Part	*Description of the change*	*Reason for the change*
	• Amendment of categories for Remedial Action(s) to Prevent Reoccurrence (column T). • Removal of the 'Customer Owned Banking Code Compliance Committee (COBCCC)' as a regulator (column U). • Addition of the Australian Competition and Consumer Commission (ACCC) as a regulator (column U). Information about drop-down menus is provided in *Table 2* and Table 3.	
C.2 Learnings from Code breaches	C.2.1 Learnings or findings from Board or Executive Management for Code breaches and actions taken to address these (C.2.1).	Following feedback, we have introduced this question for subscribers to reflect on self-reported breaches and identify any trends or learnings to improve compliance.
D. Complaint(s) reporting		
D.3	Use the ASIC prescribed form to provide details of all complaints data. For detailed information on ASIC requirements on how to provide internal dispute resolution (IDR) data files please refer to *ASIC's IDR Data Reporting Handbook*.	Following feedback from industry, we now collect complaints data in the same format as ASIC. As ASIC collects data over a six-month period, you will need to provide us with TWO reports: • 1 July to 31 December 2023, and • 1 January to 30 June 2024.
D.4 Learnings from complaints data	Review trends identified in complaints data and provide details of how your institution has addressed this.	Following feedback from industry, we have introduced this question asking subscribers to review and address the importance of complaints data.
Good industry practice		
One example of good industry practice	Removed the request for one good industry practice example.	We have removed this question to focus on a more targeted and direct reflection of subscribers' analysis of Code breaches and complaints, including details of strategic directions taken to improve customer outcomes in C.2 and D.4.

Section A: Declaration

This part of the ACS requests information that will help us understand the size of your institution.

Certification Details

The information provided in the ACS must be certified by the Chief Executive Officer (CEO), Chief Risk Officer (CRO) or relevant Senior Executive of your institution. This supports the accountability of senior management to ensure the data provided is accurate and has been considered by the executive management team.

The ACS is an opportunity for you to review your data for the reporting period and reflect on any learnings to share with us.

Size of your institution

You are required to confirm the following information:

- assets in dollars
- number of members
- number of open accounts
- full-time equivalent staff.

We would like to review our categorisation of Code subscribers based on this information. Depending on the responses, we may recalibrate the current categorisation of subscribers.

We use this information to benchmark data collected from all Code subscribers.

Number of branches

Report the number of branches your institution has across the country.

A branch is considered an office of your institution.

Section B and C: Breach reporting

Recording breaches in the Breach Data Report

This part of the ACS deals with instances of Code non-compliance, asking you to record the number of breaches of each Code section, including specific details of each breach in a separate ***COBCCC Breach Data Report 2024.***

Some *practical examples of how to report Code breaches* are provided below.

Definition of Breach

A failure to comply with the obligations of the Code in relation to the provision of a customer owned banking service and/or product.

Sourcing breach data

Code subscribers typically source breach data from consolidated compliance registers. Where these do not cover all Code breaches, review other sources such as complaints records for breach incidents, internal file audits and external audits.

Breaches can arise across all operational areas, in direct dealings with customers (such as in branches, collections and call centres), and in other areas such as marketing and systems. Your identification of Code breaches should include oversight of all such areas by appropriately trained personnel.

Classification of breaches under specific obligations

Categorise breaches against the primary reason for non-compliance. Classify instances of non-compliance against specific Code obligations. Avoid listing breaches under general obligations (such as 'Key Promises').

The commitments defined in Part A of the 2022 Code underpin all subscriber behaviour and a set of guiding principles that reflect good industry practice. These principles should be reflected in your overall company culture and support the specific obligations set out in Part B of the Code.

Detailed information for each Code breach

Please use the ***COBCCC Breach Data Detail Report 2024*** to specify details for each Code breach. Download this spreadsheet via the online portal or from our website.

Definition of incident

An incident is an event that has occurred that can likely result in a breach. It may be an institution's failure to meet process and procedures or a failure to comply with the Code.

Reporting multiple incidents

If an incident occurs many times and has the same nature, root cause and remedial impact, consolidate this into one row of the table.

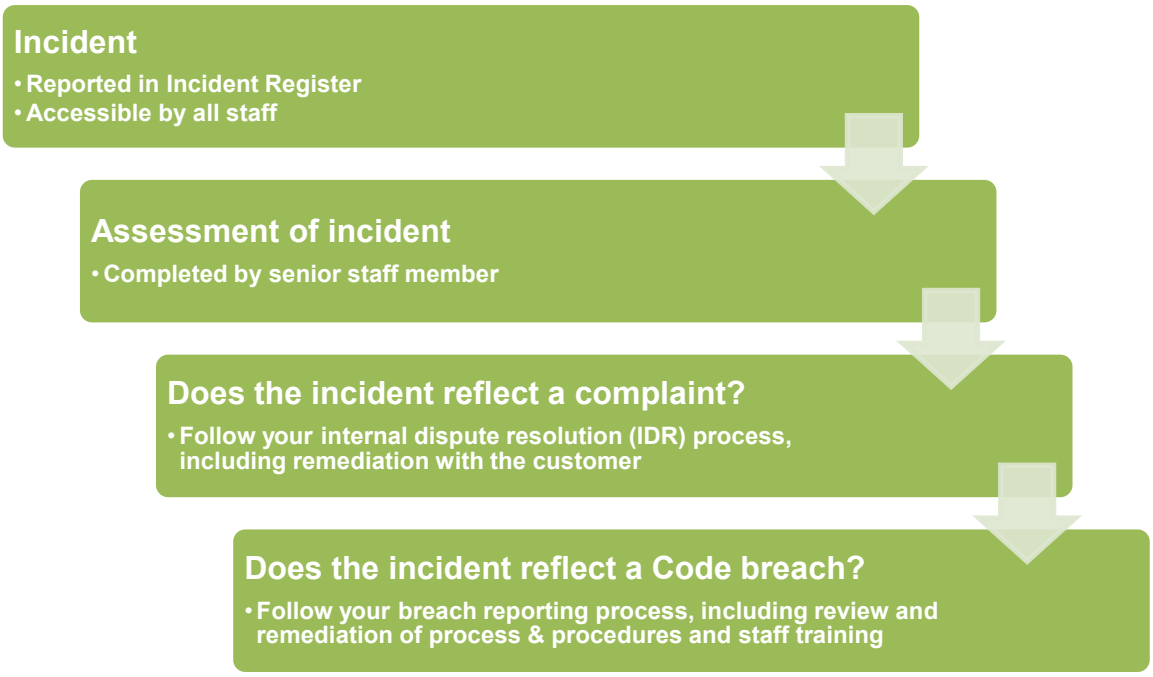
- For a single incident that results in breaches of the same type, count it as a single breach of the relevant Code section.

  Example*: A system error causes a specific mistake to happen 60 times. This is a single breach with the commentary section noting that it occurred 60 times (e.g., 60 incidents and 60 customers were affected).*

- For a single incident that results in breaches of more than one Code section, record the breach only against the primary Code section.

  Example: *A customer's privacy is breached, and their complaint is not dealt with in accordance with internal dispute resolution timeframes. Record the main breach as a privacy breach, noting in the commentary section that there was also a breach of IDR timeframes.*

An example of how an institution might identify a Code breach is as follows:



➢ **Not all incidents are breaches, but all breaches result from incidents.**

Impact of Code breaches

The impact of Code breaches measures how many customers were affected by the breach and the financial impact.

Financial impact is to be considered ***prior*** to remediation activities.

> ***Example:*** *If 100 customers were charged incorrect fees of $100 each due to a system error, the financial impact should be noted as $10,000; even if following identification of the breach and remediation all customers were reimbursed.*

Remedial action

Provide detailed information about your remedial action(s) for each breach. Remedial action is an important step to resolving the Code breach and we encourage subscribers to review these actions to prevent recurring breaches.

Recording breaches reported to regulators

Include regulatory breaches reported to ASIC or another regulator that were also breaches of the Code (*Table 3*).

Grading of breaches

Indicate the grading of a breach according to the severity and management action. The grading factors are detailed in Table 3.

Systemic breaches

Indicate whether a breach was also identified as systemic.

A systemic breach is non-compliance that has implications beyond the immediate actions and affected parties. ASIC's Regulatory Guide 271, paragraph 117 defines a systemic issue as matter that has affected, or is likely to affect, more than one person, and is likely to involve a process, policy or technological issue within your operations.

Drop-Down menu

Use the drop-down menus where applicable. If the drop-down menu does not provide an appropriate option, use the text columns to provide explanatory comments.

Table 2 and Table 3 provide a summary of the drop-down menu options available in the ***COBCCC Breach Data Report 2024.***

Learnings from Code breaches

Based on your feedback, you find it difficult to capture information about remediation activities in the ***Breach Data Report.***

Question C.2 asks you to reflect on the learnings or findings from your self-reported Code breaches and identify any trends - applying to a minimum of 20% of your self-reported breaches. This is a more effective way for you to provide us with detailed information about any strategic remedial directions and how you plan to address this in 2024-25.

Examples of remedial actions can be shared on a de-identified basis as good industry practice for the rest of the industry.

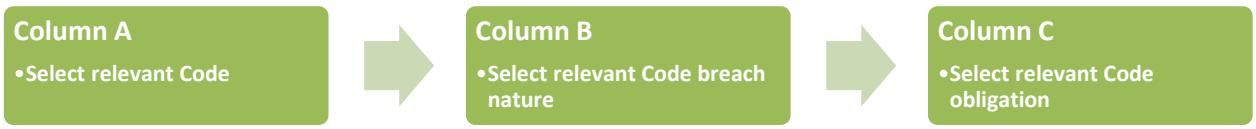
If you did not record any Code breaches

Question C.3 asks you to provide information about your processes and procedures to monitor and review Code compliance. This is an opportunity for you to reflect on your reporting framework and share these examples with us.

Drop-Down Menu Options

Table 2: Drop-down menu options for thematic self-reporting of breaches relating to the 2022 Code

Note: References to the 2018 Code will be removed for the 2024-25 period.



Breach nature	*2022 Code section*	*2018 Code section*
Advertising and promotion	B1-B5	D1
Information about products	B6-B8	D2, D18.1
Fair Terms and Conditions	B9-B12	D4
Training Staff	B13-B14	E2
Communication	B15-B16	D15
Inclusive banking services	B17-B25	No reference
Vulnerable customers	B26-B27	No reference
Complaints resolution	B28-B34	D27, D28, D29
Account statements and balances	B35-B41	D16
Changes to account	B42-B46	D17
Term deposits	B47	No reference
Cheque accounts	B48	No reference
Joint accounts	B49-B50	D9
Subsidiary cards	B51-B52	D10
Closing accounts	B53-B56	D22
Third party products and services	B57-B58	D13, D14
Consumer credit insurance	B59-B64	No reference
Electronic communication	B65-B68	D18
Replacement of documents	B69-B75	D19
Lending	B76-B77	D6

Breach nature	*2022 Code section*	*2018 Code section*
Lending to Small Business	B78-B88	No reference
Credit cards	B89-B94	D7
Safeguards for co-borrowers	B95-B99	D11
Safeguards for loan guarantors	B100-B120	D12
Guarantors' directors	B121	No reference
Lenders mortgage insurance	B122-B125	No reference
Interest rates, fees and charges	B126-B133	D3, D5
Exchange rates and commissions	B134	No reference
Financial difficulty	B135-B143	D24
Working with representative	B144-B145	D25
Debt collection	B146-B156	D26
ePayments Code	B157	B-relationship to other Codes
Direct debit	B158-B162	D20
Chargeback	B163-B167	D21
Privacy	B168-B172	D23
Publicising Code	B173	E1
Compliance responsibilities	C180-C184	E16, E17, E19, E20
Reverse Mortgage loans	n/a	D8
Key Promises [use only in exceptional circumstances]	A1-A7	KP1-KP10

Table 3: Drop-down menu options

Breach detail	*Drop-down options*
Product/Service Type and Description (Column I)	• Business Finance (as per ASIC reference 1 to 8) • Consumer Credit (as per ASIC reference 9 to 22) • Guarantees (as per ASIC reference 23 to 25) • Margin Loans (as per ASIC reference 26) • Current accounts (as per ASIC reference 27 to 32) • Safe custody (as per ASIC reference 33) • Savings accounts (as per ASIC reference 34 to 39) • Domestic insurance (as per ASIC reference 40 to 58) • Extended warranty (as per ASIC reference 59 to 62) • Professional Indemnity insurance (ASIC reference 63 to 64) • Small business/farm insurance (as per ASIC reference 65 to 79) • Derivatives/hedging (as per ASIC reference 80 to 87) • Managed investments (as per ASIC reference 88 to 104) • Real property (as per ASIC reference 105) • Securities (as per ASIC reference 106 to 113) • Life insurance (as per ASIC reference 114 to 125) • Direct transfer (as per ASIC reference 126 to 136) • Non-cash (as per ASIC reference 137 to 142) • Superannuation (as per ASIC reference 143 to 178) • Traditional trustee services (as per ASIC reference 179 to 184) • Financial advice or credit assistance (as per ASIC reference 185 to 187) • Not product/service related (as per ASIC reference 188) • Multiple product/service types • Other (please provide details)
Identification Method (Column K)	• customer query or complaint • staff self-identification • internal quality monitoring/assurance (1st line) • internal governance, process or report (2nd line) • internal audit (3rd line) • external audit • multiple identification methods • other [please provide details]
Root Cause of breach(es) (Column M)	• deficiency in process or procedure • deficiency in product • deficiency in service • inadequate change management • inadequate management controls • inadequate risk management • staff - deficiency in training • staff - fraud/misappropriation • staff - inadequate supervision • staff - misconduct • staff - negligence and/or human error • systems error/failure/issue

	• other [please provide details]
Remedial Action(s) for Customer(s) (Column S)	• customer apology • customer communication/correspondence • customer refund/reimbursement/goodwill payment • data destroyed/deleted/returned • details updated/corrected • liability reduction/repayment arrangement/collections on hold or ceased • ongoing internal investigation • not applicable
Remedial Action(s) to Prevent Reoccurrence (Column T)	• enhanced monitoring and/or controls • ongoing internal investigation • review of and changes to procedures • review of and changes to process • review of and changes to product • review of and changes to service • review of and changes to terms and conditions • staff training/coaching/feedback • system fix/improvement • not applicable
Reported to Regulator (Column U)	• No • *Australian Securities and Investments Commission* (*ASIC*) • *Australian Competition and Consumer Commission* (*ACCC*) • *Australian Financial Complaints Authority* (*AFCA*) • *Australian Prudential Regulation Authority* (*APRA*) • *Australian Transaction Reports and Analysis Centre* (*AUSTRAC*) • *Office of the Australian Information Commissioner* (*OAIC*) • other [please provide details]
Grading of Breach (Column W)	• Grade 1 - Actions/incidents which require management attention, but do not impose a serious risk to the business operations or AFS licence. • Grade 2 - Actions/incidents that require immediate management attention or an accumulation of three Grade 1 actions/incidents. • Grade 3 - Actions which pose a significant risk to the business operations or AFS licence or have resulted in direct financial loss by a client (can be one incident or accumulation of 4 or more Grade 1 incidents or 2 or more Grade 2 incidents. • Grade 4 - Actions/incidents that require urgent management attention and pose a serious risk to the business operations or AFS licence (includes major compliance failures, training inadequacies and/or overall poor performance. • Grade 5 - Actions/incidents that pose a catastrophic risk to the business operations or AFS licence and are not rectifiable.
Systemic Breach (Column Y)	• No • Yes [please provide details] • Other [please provide details]

Examples of Code breaches and how to record them

Example 1

Several staff accidentally sent emails disclosing personal information to other customers. This occurred during the hectic month at the end of the financial year. Each staff reported this mistake in the Incident Register, which all staff can access. The Compliance Manager, who reviews the Incident Register on a weekly basis, saw this mistake was reported 60 times in the past year. In all incidents, staff realised their mistake, and emailed the affected customer, apologised for the mistake and asked them to delete the email. The Compliance Manager is aware that this incident is a common occurrence for staff and is updating procedures for sending out emails, including an automatic delay of one hour before emails are sent by the system. Procedures will be updated and a refresher training program for privacy will be rolled out to all staff over the next three months.

Column	Heading	Example of recording
A - C	Code Breach Nature - Section	2022 Code – Privacy – B168
D - E	Number of Breach(es)	1
	Comment	Combined common incidents to one breach.
F	Description of Incident(s)	Staff accidentally sent emails disclosing personal information to other customers during busy end of financial year period.
G - H	Number of Incident(s)	60
	Comment	Compliance manger identified mistake happened 60 times in the past year.
I - J	Product / Service Type and Description	Multiple Products or Services
	Comment	
K - L	Identification Method(s)	Staff self-identification
	Comment	Staff reported their mistake in the Incident Register and the Compliance Manager identified this as a Code breach.
M - N	Root Cause of Breach(es)	Staff – negligence and/or human error
	Comment	
O - P	Number of Customer(s) Impacted	120
	Comment	Audit revealed 120 customers impacted.
Q - R	Financial Impact to Customer(s)	$0
	Comment	
S	Remedial Action(s) for Customer	Customer Apology
T	Remedial Action(s) to Prevent Reoccurrence	Staff Training/Coaching/Feedback
U – V	Reported to Regulator	No
	Comment	
W – X	Grading of Breach	Grade 1
	Comment	Breach happened 60 times and required management attention. No serious risk.
Y – Z	Systemic Breach(es)	Yes
	Comment	Occurred 60 times to 60 customers. Effectiveness of training and change to procedure need to be reviewed.

Example 2

An audit undertaken revealed a staff member failed to obtain or verify all of the information required to assess a loan approval accurately. These included: not capturing or including expenses; failing to obtain or verify current proof of income; and declaration questions not being verified.

The institution undertook a review of all loan applications approved by the staff member over the past three months. Five customers were identified and contacted to discuss their loan approval and verify their information. None were identified as being at risk.

The institution also undertook a review of process concerning the monitoring of approval of loan applications. The staff member was required to undertake further training.

Column	*Heading*	*Example of recording*
A - C	Code breach nature - Section	2022 Code – Lending – B76
D - E	Number of Breach(es)	5
	Comment	
F	Description of Incident(s)	Staff did not follow process required to assess a loan approval, including not capturing or including expenses; failing to obtain or verify current proof of income; and declaration questions not being verified.
G - H	Number of Incident(s)	5
	Comment	The audit identified five customers affected by the breach.
I - J	Product / Service Type and Description	Consumer Credit (ASIC ref 9 to 22)
	Comment	Personal Loan (ASIC ref 20)
K - L	Identification Method(s)	Internal audit (3rd line)
	Comment	Monthly internal audit of all loan application.
M - N	Root Cause of Breach(es)	Deficiency in process or procedure
	Comment	
O - P	Number of client(s) impacted	5
	Comment	
Q - R	Financial impact to client(s)	$0
	Comment	Affected loan applications were reviewed, information clarified and loans to be considered appropriate.
S	Remedial Action(s) for Customer	Customer communication/correspondence
T	Remedial Action(s) to Prevent Reoccurrence	Review of and changes to process
U – V	Reported to Regulator	No
	Comment	
W – X	Grading of Breach	Grade 2
	Comment	Breach required immediate management attention.
Y - Z	Systemic Breach(es)	No
	Comment	

Section D: Complaints reporting

Self-reported complaints data

This part of the ACS deals with complaints received during the reporting period.

Please use the form prescribed in the *ASIC's IDR Data Reporting Handbook* to provide details of all complaints you identified in the reporting period 1 July 2023 to 30 June 2024.

Definition of Complaint

As per *AS/NZS 10002:2014* and *ASIC RG 271.27*, a complaint is an expression of dissatisfaction made to or about an institution related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.

Please note that *obligations under RG 271* became effective on 5 October 2021.

Report ***all*** complaints, including complaints that are resolved to the customer's complete satisfaction by the end of the fifth business day.

Classification of Complaints

Classify complaints according to the product, issue, outcome and resolution timeframe as follows:

- Product categories are defined as per Tables 7 to 16 in *ASIC's IDR Data Reporting Handbook*.
- Issue categories are defined as per Table 17 in *ASIC'S IDR Data Reporting Handbook*.
- Outcome categories are defined as per Table 18 in *ASIC Data Reporting Handbook*,

Please note that ASIC collects data for a six-month period. Therefore, you will need to **submit TWO reports** to us:

- 1 July to 31 December 2023, and
- 1 January to 30 June 2024.

Please upload your **completed IDR Data Reports** into the online portal under D.3. As long as they conform with the ASIC prescribed format, we can accept them.

Learnings from complaints data

Question D.4 asks you to reflect on your self-reported complaints data and identify any trends. This is an effective way for you to review your overall complaints data and address the root cause of these complaints.

If you did not record any complaints

Question D.5 asks you to provide information about your processes and procedures to monitor and audit the operations and interactions of your institution to ensure good practice was adhered to at all times.

This is an opportunity for you to reflect on your reporting framework for complaints and share these examples with us.

Online portal guidance

The online portal

The online portal is a secure system we use to collect data and receive documents when conducting monitoring activities.

Access to the online portal

Our general approach for monitoring activities is to distribute questionnaires or other information requests in Word and/or Excel format prior to the data collection period. This provides you with more time to gather the relevant information ahead of the submission date.

We will send you an email with a password and a link to the portal. The link is unique for each Code subscriber.

When you click on the link you will be asked to enter the password.

Do not share the link or the password with anyone who should not have access to the portal, or the data being submitted.

Navigating the online portal

You can navigate through the online portal using the 'Save and Next' and 'Back' buttons at the bottom of each page.

Make sure you click 'Save and Next' before navigating backwards. If you do not, you will lose the data you entered.

Saving data and returning later

You can complete part of a questionnaire and return later. Make sure you click the 'Save and Next' button at the bottom of the section to save your progress.

If you return to complete a saved activity, you will not need to enter a password again. The portal will open at the page that was last saved.

Due date

We will email you with information about the ACS and its due date. If you are unable to complete it by the date specified, please contact us as soon as possible.

Loading and saving pages

Sometimes pages may take several minutes to save, especially where there is a large amount of data or multiple attachments. You will see a 'Loading' message with a spinning circle which indicates it is still loading. If the circle stops spinning, please allow a several minutes for the page to update.

There is no specific 'time-out' period, but you should save each page regularly to ensure you do not lose your data.

Copying and pasting into the online portal

You can copy text into most response boxes. However, please note that if you are required to complete data tables you may need to complete fields within a table manually.

Uploading supporting documents

If you are reporting a breach of the Code, you are required to upload a copy of your Breach Data Details Report into the portal. Please click 'Browse,' select the required document from your computer, click 'Open' and then 'Submit.'

If you need to upload more than one document, or the document is not a Word, Excel or PDF file, please create a zip file containing the documents and then upload the zip file.

In most cases, you can create a zip file by selecting the relevant documents, right-clicking and selecting 'Send to' > 'Compressed (zipped) folder.'.

Submitting ACS

At the end of the questionnaire, you will be asked to re-enter your password. On the subsequent page there is a 'Submit final response' button. Clicking on this button will transmit the data to us.

There will be no opportunity for you to amend the data after it has been submitted, so make sure it is correct.

If you think the information, you submitted may be wrong, contact us immediately.

Saving a record of the submission

Once you submit, you will be able to download a PDF copy of your submission.

The PDF will show the filenames of documents you uploaded, but not the contents of those documents.

Online portal security

The portal is a third-party application provided by The Evolved Group. The Evolved Group was formally audited in February 2022 by Best Practice Certification and received ISO 27001:2013 (Information Security Management System Requirements) accreditation.