IBCCC Information Document: Completing the 2024 Insurance Brokers Code of Practice Annual Compliance Statement

Your Annual Compliance Statement (ACS) is due on or before **31 March 2025.**

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 January 2024 to 31 December 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.
- The Insurance Brokers Code Compliance Committee (IBCCC) does not require personal client or employee data to be provided in the ACS. Subscribers must ensure any personal information is removed before reporting to the IBCCC.

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

- Carli Kidd (Senior Compliance Analyst), ckidd@codecompliance.org.au.
- info@codecompliance.org.au

Contents

About the ACS 3
Changes to the 2024 Annual Compliance Statement 4
Part A: Declaration 5
Part B and C: Breach reporting 6
Drop-down menu options 9
Examples of Code breaches 14
Part D: Complaints reporting 18
Online portal guidance 19

About the ACS

The Insurance Brokers Code of Practice

The Insurance Brokers Code of Practice (the Code) became effective on 1 November 2022. The Code replaced the 2014 Code and includes new obligations concerning clients experiencing vulnerability, remuneration disclosure, policy renewals and claims management.

Insurance Brokers Code Compliance Committee

The Insurance Brokers Code Compliance Committee (the IBCCC) is the Code's independent compliance monitoring body. In accordance with its Charter and the Code, the IBCCC monitors compliance with the Code, identifies systemic industry-wide issues and promotes good industry practice to improve consumer outcomes.

Purpose of the ACS

The 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 you to:

- benchmark your compliance with the Code
- report on current and emerging issues in Code compliance as part of your risk and regulatory framework, and
- establish the areas of priority for your future monitoring work to improve business and maintain clients.

Data collected through the ACS program will be aggregated, de-identified, analysed for trends and patterns, and published in the *IBCCC'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.

Changes to the 2024 Annual Compliance Statement

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*
C. IBCCC Breach Data Report 2024		
Updated drop-down menu options	Addition of "not product/service related (ASIC reference 188)" for Product/Service Category. Information about drop-down menus is provided in Table 2, Table 3 and Table 4.	Changes to the drop-down menu have been made to reflect subscriber feedback.
New column added	Column I added for reporting specific Product/Service Type. Information about drop-down menu for Product/ Service Category and Type is provided in Table 3.	Changes made to optimise information provided in the report and reflect ASIC's IDR Data Reporting Handbook.
Mandatory columns	Columns highlighted in yellow must be completed.	Ensuring these columns are completed will assist in maintaining consistency and integrity of the data provided by all subscribers.
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 January to 30 June 2024, and • 1 July 2024 to 31 December 2024.

Part A: Declaration

This part of the ACS requests information that helps us understand the size of your organisation.

Certification details

The information provided in the ACS must be certified by the Chief Executive Officer (CEO) or relevant Senior Executive of your organisation. 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 organisation

You are required to confirm how many full-time equivalent staff and authorised representatives you have.

We would like to review our categorisation of Code subscribers based on the number of staff members. 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 written insurance policies and clients

Reporting the approximate number of written insurance policies and clients assists us in understanding the size of the organisation.

We use this information as a common denominator for benchmarking purposes.

If you are unable to provide accurate information, please list the approximate numbers.

Number of branches

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

A branch is considered an office of your organisation or any authorised representative.

Offices overseas

Advise us if you have any offices overseas.

We use this information to understand the size of your organisation.

Member of a Network

Responses to this question assist us to target our communication to specific networks as part of our multi-channel communication strategy. Our objective is to tap into existing networks to share information and insights with a wide range of audiences in the most effective and efficient manner.

Consent to share information in Part A with NIBA

Only information in Part A of this ACS will be shared with NIBA.

NIBA has requested the IBCCC ask subscribers to share this information on an identified basis to assist NIBA in understanding the business operations of all Code subscribers.

Part B and C: Breach reporting

Recording breaches in the Breach Data Report

This part of the ACS deals with instances of non-compliance with the Code, asking you to record the number of breaches of each Code section, including specific details of each breach in a separate ***IBCCC 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 an insurance broking service.

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 clients (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 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.

The commitments defined in Section 3 of the 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 the rest of the Code. For these reasons Sections 1 to 3 of the Code are not included in the ***IBCCC Breach Data Report 2024***.

Detailed information for each Code breach

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

Users of Steadfast's CCX360 system can upload the 'IBCCC Incident Breach Register' in EXCEL format for Code breaches recorded in 2024.

Definition of incident

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

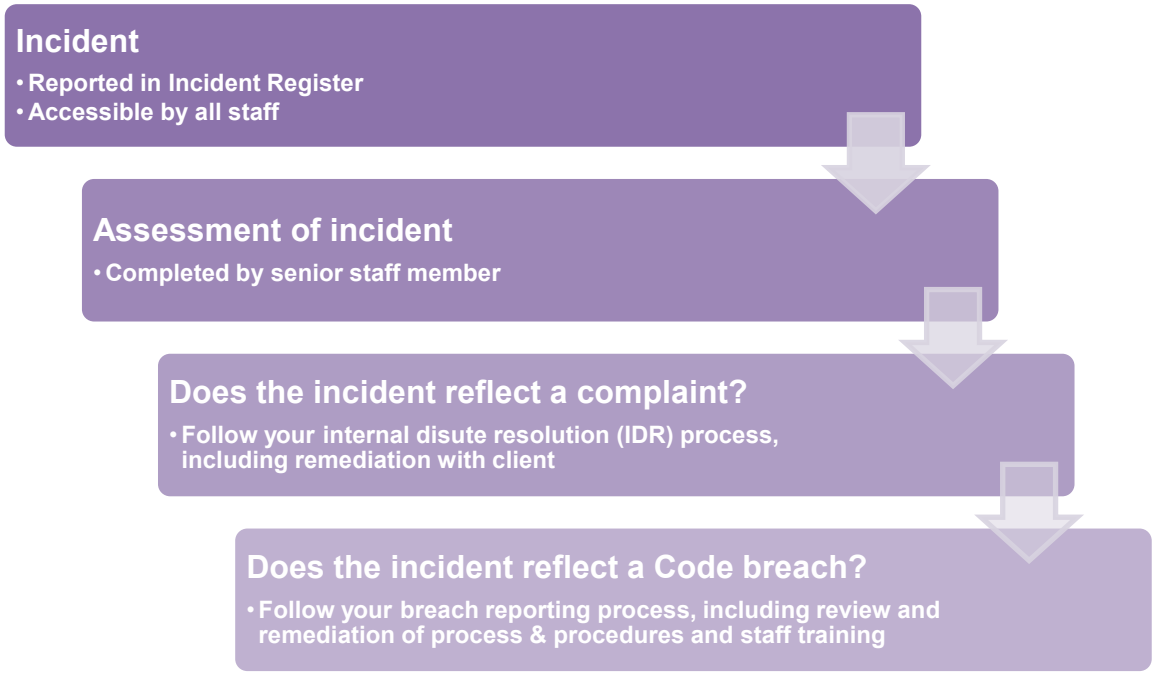
Reporting multiple incidents

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

> ***Example:*** *10 system errors caused Terms of Engagement letters to exclude required information throughout the year. Record this as 1 Code breach, that occurred in 10 instances.*

The number of times this event occurred can be recorded in Column F "Number of Incidents".

An example of how an organisation 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 clients were impacted by the breach and the financial impact.

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

> ***Example:*** if 100 clients 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 clients were reimbursed.

Remedial action

Select the relevant drop-down for immediate and long-term remedial action relevant to the Code breach (Table 4). Remedial action is an important step to resolving the Code breach and we encourage subscribers to review these actions to prevent recurring breaches.

We consider immediate remedial action to be completed within six months of the breach.

Long-term remedial action is an action that has taken more than six months to complete.

Recording breaches reported to regulators

Include any regulatory breaches reported to the Australian Securities and Investments Commission (ASIC) or other regulators, that were also breaches of the Code (Table 4).

Grading of breaches

Indicate the grading of a breach according to the severity and management action. The grading factors are detailed in Table 4.

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 3 and Table 4 provide a summary of the drop-down menu options available in the ***IBCCC Breach Data Report 2024.***

Learnings from Code breaches

Based on your feedback, you find it difficult to capture information in the ***IBCCC 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. This is a more effective way for you to provide us with detailed information about any short or long-term remedial action and how you plan to address this in 2025.

These examples 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 self-reporting of breaches relating to the Code

Column A
- Select relevant Code breach nature

Column B
- Select relevant Code section

Breach nature	*Code section*
Understanding Our Role	4.1(a)
Terms of Engagement	4.2(a)-(c)
Communications	5.1(a)-(b)
Behaviour	5.2(a)-(c)
Who We Act For	5.3(a)-(e)
Disclosing Remuneration	6.1(a)-(d)
Contingent Remuneration	6.2(a)-(c)
Non-Monetary Benefits	6.3(a)-(b)
Service Provided to Insurers and others	6.4(a)-(c)
Remuneration Review	6.5
Claims Management	7.1(a)-(g)
Policy Renewal	7.2(a)-(b)
Our Responsibility (Training)	8.1
Promoting Code compliance	8.2(a)(i)-(v)
Making a Complaint	9.1(a)-(b)
Handling Complaints	9.2(a)-(c)
Responding to Complaints	9.3(a)-(c)
Timeframes for handling your Complaints	9.4(a)-(c)
Identifying vulnerable clients	10.1(a)-(c)
Supporting vulnerable clients	10.2(a)-(d)
Working with the IBCCC	11.4(a)-(b)
Promoting the Code	12.1(a)-(c)

Table 3: Drop-down menu options for product / service

Product/Service Category (Column H)	*Product/Service Type (Column I)*
Domestic Insurance (ASIC 40 to 58)	Consumer credit insurance (ASIC reference 40)
	Home building (ASIC reference 41)
	Home contents (ASIC reference 42)
	Landlord insurance (ASIC reference 43)
	Motor vehicle — Comprehensive (ASIC reference 44)
	Motor vehicle — Third-party (fire and theft) (ASIC reference 45)
	Motor vehicle — Third-party (ASIC reference 46)
	Motor vehicle — Uninsured third-party (ASIC reference 47)
	Personal and domestic property — Mobile phone (ASIC reference 48)
	Personal and domestic property — Domestic pet/horse (ASIC reference 49)
	Personal and domestic property — Caravan/trailer (ASIC reference 50)
	Personal and domestic property — Pleasure craft (ASIC reference 51)
	Personal and domestic property — Valuables/other moveable property (ASIC reference 52)
	Residential strata title (ASIC reference 53)
	Sickness and accident insurance (ASIC reference 54)
	Ticket insurance (ASIC reference 55)
	Travel insurance (ASIC reference 56)
	Trust bond (ASIC reference 57)
	Other domestic insurance (ASIC reference 58)
Extended Warranty (ASIC 59 to 62)	Brown goods (ASIC reference 59)

	Motor vehicles (ASIC reference 60)
	White goods (ASIC reference 61)
	Other extended warranty (ASIC reference 62)
Professional Indemnity (ASIC 63 to 64)	Medical indemnity insurance (ASIC reference 63)
	Other professional indemnity (ASIC reference 64)
Small business/farm insurance (ASIC 65 to 79)	Commercial property (ASIC reference 65)
	Commercial vehicle (ASIC reference 66)
	Computer and electronic breakdown (ASIC reference 67)
	Contractors all risk (ASIC reference 68)
	Fire or accident damage (ASIC reference 69)
	Glass (ASIC reference 70)
	Industrial special risk (ASIC reference 71)
	Land transit (ASIC reference 72)
	Livestock (ASIC reference 73)
	Loss of profits/business interruption (ASIC reference 74)
	Machinery breakdowns (ASIC reference 75)
	Money (ASIC reference 76)
	Public liability (ASIC reference 77)
	Thefts (ASIC reference 78)
	Other small business/farm insurance (ASIC reference 79)
Multiple Products or Services	
Not product/service-related (ASIC reference 188)	
Other [please provide additional details]	

Table 4: Other Drop-down menu options

Breach detail	*Drop-down options*
Identification Method(s) **(Column K)**	• internal process or report • random internal audit • external compliance audit • staff self-identification • client query or complaint • multiple identification methods • other [please provide additional details]
Root Cause of breach(es) **(Column M)**	• incorrect process & procedure • insufficient training • mail house error • manual error • process & procedure not followed • staffing/resourcing issues • staff misconduct • system error or failure • other [please provide additional details]
Immediate Remedial Action(s) **(Column S)**	• apology • ex-gratia payment • premium adjustment • refund of premium • refund of fees/charges • review of and changes to procedure • review of and changes to process • review of and changes to terms and conditions • training • undertaking • other [please provide additional details in C.2] • not applicable
Long-Term Remedial Action(s) **(Column T)**	• premium adjustment • review of and changes to procedure • review of and changes to process • review of and changes to terms and conditions • training • undertaking • other [please provide additional details in C.2] • not applicable

Breach detail	*Drop-down options*
Reported to Regulator **(Column U)**	• not applicable • Australian Securities and Investments Commission (ASIC) • Australian Prudential Regulation Authority (APRA) • Office of the Australian Information Commissioner (OAIC) • Australian Financial Complaints Authority (AFCA) • Australian Competition and Consumer Commission (ACCC) • other [please provide additional details]
Grading of Breach **(Column W)**	• Grade 1 - Actions/incidents which require management attention, but do not pose 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(es) **(Column Y)**	• No • Yes [please provide additional details] • Other [please provide additional details]

Examples of Code breaches

Example 1

Several of our authorised representatives (AR) accidentally sent emails disclosing personal information to other clients. This occurred during the hectic end of financial year months when the ARs were issuing renewals to clients in time. Each AR reported this mistake in our Incident Register, which all staff can access. Our 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, the AR realised their mistake, and emailed the affected client, apologised for the mistake and asked them to delete the email. Our Compliance Manager is aware that this incident is a common occurrence for our ARs and is updating procedures for sending renewal notices. We expect it will take 8 months to update our procedures.

Example of how to record this in the Breach Data Report 2024

Column	Heading	Example of recording
A - B	Code breach nature - Section	Our responsibility (training) – 8.1
C - D	Number of Breach(es)	1
E	Description of Breach(es)	ARs accidentally sent emails disclosing personal information to other clients during busy renewal period at end of year.
F - G	Number of Incidents	60
	Comment	Compliance manger identified mistake happened 60 times in the past year
H - J	Product/Service Category	Multiple Products or Services
	Product/Service Type	-
K - L	Identification Method(s)	Staff self-identification
	Comment	ARs reported their mistake in the Incident Register and the Compliance Manager identified this as a Code breach.
M - N	Root Cause of Breach(es)	Process & procedure not followed
O - P	Number of client(s) impacted	60
Q - R	Financial impact to client(s)	$0
S	Immediate Remedial Action(s)	Apology
T	Long-Term Remedial Action(s)	Review of and changes to procedure
U - V	Reported to Regulator	Not applicable
W - X	Grading of Breach	Grade 1
	Comment	Breach happened 60 times and required management attention.
Y - Z	Systemic Breach(es)	Yes
	Comment	ARs did not follow process & procedure

Example 2

John called us to lodge a claim under his motor vehicle policy. We lodged this claim on his behalf with the insurer. The insurer denied the claim, as John's policy had lapsed more than 2 weeks ago.

We reviewed our records and realized that we did not renew John's policy. Upon further investigation we discovered that there was no record of any renewal notices being sent to John. Our staff had deleted an email reminding them to check upcoming policy renewals.

We immediately called John, explained that his policy had lapsed due to our error, and his claim was denied by the insurer. We apologized for this and informed him that we would cover his claim of $950 as we did not renew his policy on time.

Following this incident, we have committed to an overhaul of our current processes and are implementing an automated system which will send out renewal notices 30 days prior to expiry. We have also rolled out a training program to our staff about the automated system and how to check renewals on a weekly basis.

Example of how to record this in the Breach Data Report 2024

Column	Heading	Example of recording
A - B	Code breach nature - Section	Policy Renewal – 7.2 (a)
C - D	Number of Breach(es)	1
E	Description of Breach(es)	Discovered client's policy was not renewed on time after insurer denied the client's claim.
F - G	Number of Incidents	1
H - J	Product/Service Category	Domestic Insurance (ASIC 40 to 58)
	Product/Service Type	Motor vehicle — Comprehensive (ASIC reference 44)
K – L	Identification Method(s)	Client query or complaint
	Comment	We lodged the claim on behalf of the client.
M – N	Root Cause of Breach(es)	Manual Error
	Comment	Staff member deleted an email reminding them to check upcoming policy renewals.
O – P	Number of client(s) impacted	1
Q – R	Financial impact to client(s)	$950
S	Immediate Remedial Action(s)	Ex-gratia payment
T	Long-Term Remedial Action(s)	Review of and changes to process
U- V	Reported to Regulator	Not applicable
W – X	Grading of Breach	Grade 2
	Comment	Incident required immediate management attention.
Y - Z	Systemic Breach(es)	No
	Comment	Isolated incident

Example 3

Jane held an insurance policy for her car, organised by us. Jane has low literacy skills and finds it difficult to make sense of written documents. She has informed us of this and asked to receive an additional phone call to pass on any information.

Jane lodged a claim under her policy after a car accident. The insurer denied the claim, and informed Jane that her policy had lapsed more than four weeks before the accident.

We reviewed Jane's file and confirmed that a renewal notice was emailed to her four weeks before the renewal date, but she did not respond, and the policy lapsed.

We acknowledge that we were aware of Jane's low literacy skills and had noted this as a vulnerability on our data base. We should have provided Jane with additional support to help her renew her policy.

We paid Jane's claim of $5,000 as we should have helped her with the policy renewal. We also undertook an entire staff training program to help understand and recognise vulnerabilities.

Example of how to record this in the Breach Data Report 2024

Column	Heading	Example of recording
A - B	Code breach nature - Section	Supporting vulnerable clients – 10.2 (a)
C - D	Number of Breach(es)	1
E	Description of Breach(es)	Client identified their vulnerability to us and requested they receive a phone call to pass on any information. The broker emailed the client a renewal notice but did not follow up via phone call. As a result, when the client made a claim, after a car accident, it was denied.
F - G	Number of Incidents	1
H - J	Product/Service Category	Domestic Insurance (ASIC 40 to 58)
	Product/Service Type	Motor vehicle — Comprehensive (ASIC reference 44)
K – L	Identification Method(s)	Client query or complaint
	Comment	Identified after client's claim was denied.
M – N	Root Cause of Breach(es)	Process & procedure not followed
O – P	Number of client(s) impacted	1
Q – R	Financial impact to client(s)	$5,000
S	Immediate Remedial Action(s)	Ex-gratia payment
T	Long-Term Remedial Action(s)	Training
U – V	Reported to Regulator	Not applicable
W – X	Grading of Breach	Grade 1
Y – Z	Systemic Breach(es)	No

Example 4

Our half-yearly external audit identified that a software glitch caused 30 Terms of Engagement letters to be printed with the incorrect remuneration information. As a result of this error, client invoices were overcharged by $100 each. We immediately refunded the $100 to each of the affected clients and updated their Terms of Engagement to reflect accurate disclosure of remuneration. We are working with our software provider to fix this glitch, but they have suggested it may take 8 months to fix. In the meantime, we have directed all staff to manually verify the remuneration information in new Terms of Engagement letters.

Example of how to record this in the Breach Data Report 2024

Column	Heading	Example of recording
A - B	Code breach nature - Section	Terms of engagement – 4.2 (b)
C - D	Number of Breach(es)	1
E	Description of Breach(es)	Software glitch caused 30 Terms of Engagement letters to be printed with the incorrect remuneration information.
F - G	Number of Incidents	1
	Comment	It was 1 print run of Terms of Engagement letters for 30 clients.
H - J	Product/Service Category	Small business/farm insurance (ASIC 65 to 79)
	Product/Service Type	Commercial property (ASIC reference 65)
K – L	Identification Method(s)	External compliance audit
M – N	Root Cause of Breach(es)	System error or failure
O – P	Number of client(s) impacted	30
Q – R	Financial impact to client(s)	$3,000
	Comment	30 clients were overcharged $100 each.
S	Immediate Remedial Action(s)	Refund of fees / charges
T	Long-Term Remedial Action(s)	Review of and changes to process
U – V	Reported to Regulator	Not applicable
W – X	Grading of Breach	Grade 3
	Comment	The software glitch has not been fixed yet. We have refunded clients $3,000 and this issue is still a significant risk to the business.
Y – Z	Systemic Breach(es)	Yes
	Comment	The software glitch (system error) has affected 30 clients.

Part D: Complaints reporting

Self-reported complaints data

This part of the ACS deals with complaints received during the reporting period. The following tables show how we classify complaint products, issues and outcomes.

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 organisation 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.

Classify complaints according to the product, issue, outcome and resolution timeframe as per ASIC's IDR Data Reporting Handbook.

Classification of Complaints

Classify complaints according to the product, issue, outcome and resolution timeframe in ASIC's IDR Data Reporting Handbook as follows:

- Product categories are defined as per Tables 7 to 16
- Issue categories are defined as per Table 17
- Outcome categories are defined as per Table 18.

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

- 1 January to 30 June 2024, and
- 1 July 2024 to 31 December 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 organisation 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 used by the IBCCC for collecting data or the submission of 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 urge you to prioritise the completion of the ACS program prior to deadline **31 March 2025**.

If you are unable to complete the ACS by this deadline, please contact us as soon as possible.

The IBCCC will likely apply sanctions if you continue to provide late ACS submissions.

Failure to provide ACS by due date 31 March

The Code sets out your obligations for interacting with the IBCCC, including to take reasonable steps to cooperate with us in our review of compliance with the Code (section 11.4(b)).

We consider the three months to prepare and submit your ACS as adequate time for you to meet your reporting obligation.

A failure to cooperate with the IBCCC's reasonable request for information, may be considered a breach of the Code.

If the IBCCC determines you have breached section 11.4(b) of the Code, it has the right to impose a sanction which includes:

- publishing the fact that a named subscriber has breached the Code, or
- referring the matter to NIBA to be dealt.

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 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 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.