



# IBCCC 2022 ACS Information Document

## ***Completing the 2022 Insurance Brokers Code of Practice Annual Compliance Statement (ACS)***

Your ACS is due on or before **31 March 2023**.

### **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 2022 to 31 December 2022**.
- 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.
- If we need more information to assess your compliance with the Code, we may contact you to ask for further information and/or to arrange a video conference.

### **Further assistance**

- Daniela Kirchlinde (Code Compliance and Operations Manager),  
[dkirchlinde@codecompliance.org.au](mailto:dkirchlinde@codecompliance.org.au)
- Amanda Rosario (Senior Compliance Analyst),  
[ARosario@codecompliance.org.au](mailto:ARosario@codecompliance.org.au)
- Email: [info@codecompliance.org.au](mailto:info@codecompliance.org.au)

## Contents

---

|  |           |
|--|-----------|
| <b>Introduction</b> .....  | <b>4</b>  |
| The Insurance Brokers Code of Practice .....   | 4         |
| Insurance Brokers Code Compliance Committee .....  | 4         |
| Purpose of the Annual Compliance Statement .....   | 4         |
| <b>Changes to the 2022 Annual Compliance Statement</b> .....   | <b>5</b>  |
| Table 1: Changes to the 2022 ACS.....  | 5         |
| <b>Completing Part A: Declaration</b> .....  | <b>7</b>  |
| Certification Details.....   | 7         |
| Size of your organisation .....  | 7         |
| Number of written insurance policies and clients .....   | 7         |
| Number of branches .....   | 7         |
| Offices overseas.....  | 7         |
| <b>Completing Part B and C: Breach reporting</b> .....   | <b>8</b>  |
| Definition of Breach .....   | 8         |
| Sourcing breach data .....   | 8         |
| Classification of breaches under specific obligations .....  | 8         |
| Detailed information for each Code breach.....   | 8         |
| Recording incidents involving multiple breaches.....   | 8         |
| Impact of Code breaches.....   | 9         |
| Recording breaches reported to regulators.....   | 9         |
| Grading of breaches .....  | 9         |
| Systemic breaches .....  | 9         |
| Drop-Down Menu .....   | 9         |
| Table 2: Drop-down menu options for thematic self-reporting of breaches relating to the<br>2022 Code and the 2014 Code ..... | 10        |
| Table 3: Drop-down menu options .....  | 11        |
| <b>Completing Part D: Complaints reporting</b> .....   | <b>13</b> |
| Definition of Complaint .....  | 13        |
| Recording complaints involving multiple products, issues.....  | 13        |
| Products .....   | 13        |
| Issues.....  | 14        |
| Outcomes.....  | 14        |
| Resolution timeframes.....   | 15        |
| Complaints not resolved within 30 days.....  | 15        |

|   |           |
|---|-----------|
| <b>Completing Part E: Good industry practice .....</b>                        | <b>16</b> |
| <b>Completing Part F: Code Transition and Implementation.....</b>             | <b>16</b> |
| <b>Completing Part G: Supporting clients experiencing vulnerability .....</b> | <b>16</b> |
| <b>Online portal guidance .....</b>   | <b>17</b> |
| <b>Contact us .....</b>   | <b>19</b> |

## Introduction

---

### The Insurance Brokers Code of Practice

#### [2014 Code](#)

The 2014 Insurance Brokers Code of Practice (the Code) became effective on 1 January 2014. The 2014 Code sets standards of good industry practice for insurance brokers when dealing with current and prospective individual and small business clients.

It includes a set of service standards that guide insurance brokers who subscribe to the Code how to act when providing insurance broking services to consumers. These service standards form the basis for the Code's specific obligations.

#### [2022 Code](#)

Following a review of the 2014 Code, the National Insurance Brokers Association ([NIBA](#)) released the new Code in March 2022. The 2022 Code becomes effective from 1 November 2022. The 2022 Code includes new obligations to support clients experiencing vulnerability, banning preferential remuneration and increased disclosure requirements.

NIBA has delayed the implementation of section 6.1 (disclosing remuneration) of the 2022 Code until 1 November 2023.

#### Transition period

The 2022 ACS requests Code subscribers to self-report breach and complaints data referring to a period where the 2014 Code applies (from 1 January – 31 October 2021), as well as the 2022 Code (1 November – 31 December 2021). We used the 2022 ACS to assist Code subscribers with the transition to the 2022 Code by providing references to both, the 2014 Code and the 2022 Code.

#### 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.

#### Purpose of the Annual Compliance Statement

The Annual Compliance Statement (ACS) program is a central component of the IBCCC's monitoring work.

The ACS asks for information about your Code compliance frameworks and breach and complaints reporting and monitoring, as well as your organisation's overall culture of compliance.

The ACS helps the IBCCC to:

- benchmark organisations' 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 its future monitoring work.

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, as well as provided to Code subscribers via individualised Benchmark Reports.

Previous publications of the IBCCC can be downloaded [here](#).

## Changes to the 2022 Annual Compliance Statement

Table 1 provides an overview of some changes to the 2022 ACS compared to previous reporting periods. These changes have been carefully considered by the IBCCC based on current compliance monitoring requirements and consultation with NIBA and industry.

**Table 1: Changes to the 2022 ACS**

| <b>Part</b>                            | <b>What</b>  | <b>Reason</b>  |
|--|--|--|
| <b>A. Declaration</b>                  |  |  |
| <b>A.2 Written Client Policies</b>     | Provide the approximate number of written insurance policies and clients. This is the overall policies and clients for your insurance broking business.  | These numbers will be used to provide a common denominator for benchmark reporting purposes.<br>For example, number of breaches per 1,000 clients.   |
| <b>B. and C. Code Breach reporting</b> |  |  |
| <b>Breach reporting</b>                | Confirmation if Code breaches have been identified during the reporting period.<br>Depending on the response, you will need to: <ul style="list-style-type: none"> <li>• YES, provide a Breach Data Detail Report (see C.1).</li> <li>• NO, provide additional information regarding your reporting and monitoring framework (see C.2).</li> </ul>   | Detailed information regarding self-reported breaches is only requested once as per the Breach Data Detail Report (C.1). This avoids previous years' duplication to report the same data in the ACS as well as in the excel spreadsheet.<br><br>Code subscribers who self-report nil breaches are requested to provide further information (C.2).  |
| <b>C.1 Detailed Breach reporting</b>   | Improved detailed breach reporting via the Breach Data Detail Report in the form of a provided excel spreadsheet.<br><br>Information about options listed in the drop-down menu are provided in <a href="#">Table 2</a> and <a href="#">Table 3</a> .<br><br>We acknowledge this information might not be readily available for the 2022 ACS data from all Code subscribers but should be used as guidance document to transition to the 2022 Code.<br><br>The document has been developed to provide guidance to Code subscribers in the transitioning to the revised Code.<br><br>It also allows early adopters to already report under the 2022 Code. | The Breach Data Detail Report refers to both, the 2014 Code and the 2022 Code, in a thematic structure referencing the specific obligations in each Code (see <a href="#">Table 2</a> for details).<br><br>An overview of the other drop-down options is provided in <a href="#">Table 3</a> , including: <ul style="list-style-type: none"> <li>• categorisation of: <ul style="list-style-type: none"> <li>○ product/service type and description (column D)</li> <li>○ identification Method(s) (Column J).</li> </ul> </li> <li>• Additional information regarding: <ul style="list-style-type: none"> <li>○ grading of breaches according to severity and management action (Column AB), and</li> <li>○ identification of systemic breaches (Column AD).</li> </ul> </li> </ul> |

| <b>Part</b>   | <b>What</b>   | <b>Reason</b>  |
|---|---|--|
| <b>C.2 Reporting nil breaches</b>   | Request to provide detailed information about process, procedures, monitoring and training in place to ensure a positive breach reporting culture.  | Provide the IBCCC with background information to provide additional information when self-reporting nil breaches.  |
| <b>D. Complaint reporting</b>   |   |  |
| <b>D.8 Reporting nil complaints</b>   | Request to provide detailed information about process, procedures, monitoring and training in place to ensure a positive complaint reporting culture.   | Provide the IBCCC with background information to provide additional information when self-reporting nil complaints.  |
| <b>F. Code Transition and Implementation</b>  |   |  |
| <b>Conduct targeted inquiry into how Code subscribers have transitioned to the 2022 Code and monitoring of Code compliance.</b> |   |  |
| <b>F. 1 Transition to the 2022 Code</b>   | Request to provide information regarding activities undertaken or scheduled to be undertaken to transition to the 2022 Code and main areas that required change.<br>F.1.1 – Activities your organisation has completed.<br>F.1.2 – Activities your organisation is planning to initiate.<br>F.1.3 – Areas that require change<br>F.1.4 – Additional comments. | Provide the IBCCC with background information to develop guidance for transitioning to the 2022 Code and identify any gaps.<br><br>The IBCCC wish to understand activities taken to support transition to the 2022 Code. F.1.1 and F.1.2 distinguish between activities completed and activities planning to initiate. |
| <b>F.2 Governance Processes</b>   | Request to provide information about processes in place to report on Code compliance to the Board or Executive Management and how often these reports are made.   | Provide the IBCCC with background information to share good industry practice about reporting on Code compliance to Board or Executive Management.   |
| <b>F.3 Post Implementation Review</b>   | Request to provide information regarding post implementation reviews, who undertook them, and the scope and timeframes of any reviews.  | Provide the IBCCC with background information and examples of good industry practice to be shared with the industry.   |
| <b>F.4 Resource requirements</b>  | Request to provide information of time/resources needed to implement the 2022 Code.   | Provide the IBCCC with background information to better understand what impact the 2022 Code has on industry.  |
| <b>G. Supporting clients experiencing vulnerability</b>   |   |  |
| <b>Conduct targeted inquiry into compliance with section 10 of the 2022 Code.</b>   |   |  |
| <b><i>'We are committed to supporting clients who may be experiencing vulnerability.'</i></b>                                   |   |  |
| <b>Supporting clients experiencing vulnerability</b>  | Conduct targeted inquiry into compliance with section 10 of the 2022 Code, including additional questions relating to the definition of vulnerability, identification of vulnerability and support provided to clients and staff.   | Responses will inform the IBCCC on what policies/processes and training you have in place to deal with these issues.<br><br>Provide the IBCCC with background information and examples of good industry practice to be shared with the industry.   |

## Completing Part A: Declaration

---

This part of the ACS requests identification information that will assist the IBCCC in understanding the size of your organisation.

### **Certification Details**

The information provided in the ACS must be certified by the Chief Executive Office of your organisation.

It is important that data and responses provided is accurate.

The ACS is an opportunity for organisations to review their data for the reporting period and reflect on any learnings to share with the IBCCC.

### **Size of your organisation**

Code subscribers are required to confirm how many full-time equivalent staff and authorised representatives they have.

The IBCCC uses 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 will assist the IBCCC in understanding the size of the organisation.

The IBCCC will 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**

You are required to report the number of branches your organisation has across the country.

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

### **Offices overseas**

Please advise the IBCCC if you have any offices overseas.

The IBCCC uses this information to understand the size of your organisation.

## Completing Part B and C: Breach reporting

---

This part of the ACS deals with instances of Code non-compliance, asking you to record the number of breaches of each Code section in a table, including providing specific details of each breach in a separate **IBCCC Breach Data Detail Report 2022**.

### Definition of Breach

A failure to comply with the obligations of the Code in relation to the provision of an insurance broking service.<sup>1</sup>

### 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, file audit 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 such areas by appropriately trained personnel.

### Classification of breaches under specific obligations

Breaches should be categorised against the primary reason for non-compliance. Avoid listing breaches under the general Code Principles (e.g., Section 3.1 of the 2022 Code) but classify instances of non-compliance against specific Code obligations. This provides the IBCCC with more meaningful information and data to identify areas of concern.

The commitments defined in Section 3.1 of the 2022 Code underpin the Code by a set of guiding principles reflecting good industry practice. These should be reflected in your overall company culture and support the specific obligations set out in the main part of the Code.

### Detailed information for each Code breach

Please use the provided **IBCCC Breach Data Detail Report 2022** to specify details for each Code breach. This excel spreadsheet can be downloaded via the online portal. A sample has also been provided in a prior email to you.

### Recording incidents involving multiple breaches

The IBCCC seeks to avoid duplication in reporting of Code breaches.

Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

For the purposes of compiling breach reporting totals, multiple breaches of the Code should be recorded as follows:

- Where a single incident results in breaches of the same type, count this as a single breach of the relevant Code section.

---

<sup>1</sup> Terms have been defined with reference to the [ASIC Regulatory Guide 78 – Breach Reporting by AFS Licensees](#), the Australian Standard [AS 3806 2006 – Compliance Programs](#), Section 912D of the [Corporations Act 2001](#).



**Example:** A system error causes a specific mistake to happen 60 times, record this as a single breach noting in the commentary section that it occurred 60 times (e.g. 60 clients were affected).

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

**Example:** A client'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.

## 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. For 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.

## Recording breaches reported to regulators

Include in your Breach Data Detail Report any regulatory breaches reported to ASIC or another regulator that also constituted breaches of the Code.

## Grading of breaches

Please indicate the grading of a breach(es) according to the severity and management action. The grading factors are detailed in [Table 3](#) below.

## Systemic breaches

Please include information if any of the breach(es) were also identified as systemic.

A systemic breach is non-compliance that has implications beyond the immediate actions and affected parties. A systemic breaches has affected, or are likely to affect, more than one person.<sup>2</sup> It is likely to involve a process, policy or technological issue within the Code Subscriber's operations.

## Drop-Down Menu

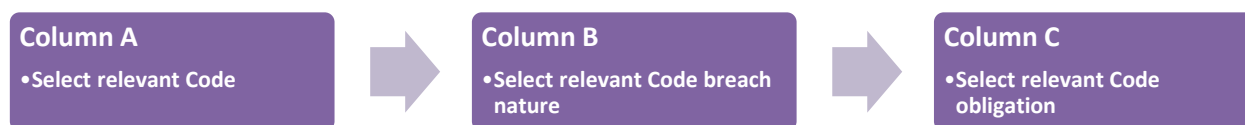
Please use the provided drop-down lists where applicable. If the drop-down list does not provide an appropriate option, please use the text columns to provide further explanatory comments. Please do NOT overwrite the drop-down options.

The following tables ([Table 2](#) and [Table 3](#)) provide a summary of the drop-down menu options available in the Breach Data Detail Report.

---

<sup>2</sup> ASIC's [Regulatory Guide 271](#) *Internal Dispute Resolution*, paragraph 117.

**Table 2: Drop-down menu options for thematic self-reporting of breaches relating to the 2022 Code and the 2014 Code**



| <b>2022 Code</b>                        |                     |
|---|---------------------|
| <i>Breach nature</i>                    | <i>Code section</i> |
| 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                      | 8.1                 |
| Promoting the Code                      | 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)         |

| <b>2014 Code</b>        |                     |
|-------------------------|---------------------|
| <i>Breach nature</i>    | <i>Code section</i> |
| Compliance with the law | St1                 |
| Conflict of Interest    | St2                 |
| Who we act for          | St3                 |
| Covered services        | St4                 |
| Buying insurance        | St5.1               |
| Claims handling         | St5.2               |
| Acting for u/w          | St5.3               |
| Remuneration            | St6                 |
|                         |                     |
| Money handling          | St7                 |
| Training                | St8                 |
| Disasters               | St9                 |
| Complaints handling     | St10                |
| Promotion of the Code   | St11                |
| Professionalism         | St12                |

**Table 3: Drop-down menu options**

| <i>Breach detail</i>                       | <i>Drop-down options</i>   |
|--|--|
| Product/Service Type & Description         | <ul style="list-style-type: none"> <li>• Domestic Insurance (ASIC 40 to 58)</li> <li>• Extended Warranty (ASIC 59 to 62)</li> <li>• Professional Indemnity (ASIC 63 to 64)</li> <li>• Small business/farm insurance (ASIC 65 to 79)</li> <li>• Other [please provide additional details]</li> </ul>  |
| Identification Method(s)                   | <ul style="list-style-type: none"> <li>• internal process or report</li> <li>• random internal audit</li> <li>• external compliance audit</li> <li>• staff self-identification</li> <li>• client query or complaint</li> <li>• other [please provide additional details]</li> </ul>  |
| Root Cause of breach(es)                   | <ul style="list-style-type: none"> <li>• incorrect process &amp; procedure</li> <li>• insufficient training</li> <li>• mail house error</li> <li>• manual error</li> <li>• process &amp; procedure not followed</li> <li>• staffing/resourcing issues</li> <li>• staff misconduct</li> <li>• system error or failure</li> <li>• other [please provide additional details]</li> </ul>   |
| Immediate Remedial Action(s)               | <ul style="list-style-type: none"> <li>• apology</li> <li>• ex-gratia payment</li> <li>• premium adjustment</li> <li>• refund of premium</li> <li>• refund of fees/charges</li> <li>• review of and changes to procedure</li> <li>• review of and changes to process</li> <li>• review of and changes to terms and conditions</li> <li>• training</li> <li>• undertaking</li> <li>• other [please provide additional details]</li> </ul> |
| Timeframe for immediate remedial action(s) | <ul style="list-style-type: none"> <li>• immediate</li> <li>• within 48 hours</li> <li>• within 1 week</li> <li>• within 2 weeks</li> <li>• within 1 month</li> <li>• 1 to 3 months</li> <li>• 3 to 6 months</li> <li>• 6 to 12 months</li> <li>• over 1 year</li> <li>• other [please provide additional details]</li> </ul>  |
| Long Term Remedial Action(s)               | <ul style="list-style-type: none"> <li>• apology</li> <li>• ex-gratia payment</li> <li>• premium adjustment</li> <li>• refund of premium</li> <li>• refund of fees/charges</li> <li>• review of and changes to procedure</li> <li>• review of and changes to process</li> </ul>  |

| <i>Breach detail</i>                       | <i>Drop-down options</i>  |
|--|---|
|  | <ul style="list-style-type: none"> <li>• review of and changes to terms and conditions</li> <li>• training</li> <li>• undertaking</li> <li>• other [please provide additional details]</li> </ul>   |
| Timeframe for long term remedial action(s) | <ul style="list-style-type: none"> <li>• within 1 month</li> <li>• 1 to 3 months</li> <li>• 3 to 6 months</li> <li>• 6 to 12 months</li> <li>• 1 to 2 years</li> <li>• 2 to 5 years</li> <li>• over 5 years</li> <li>• other [please provide additional details]</li> </ul>   |
| Reported to Regulator                      | <ul style="list-style-type: none"> <li>• Australian Securities and Investments Commission (<a href="#">ASIC</a>)</li> <li>• Australian Prudential Regulation Authority (<a href="#">APRA</a>)</li> <li>• Office of the Australian Information Commissioner (<a href="#">OAIC</a>)</li> <li>• Australian Financial Complaints Authority (<a href="#">AFCA</a>)</li> <li>• Insurance Brokers Code Compliance Committee (<a href="#">IBCCC</a>)</li> <li>• other [please provide additional details]</li> </ul>  |
| Grading of Breach                          | <ul style="list-style-type: none"> <li>• Grade 1 - An action or incident that requires management attention but does not impose a serious risk to business operations or the AFS licence.</li> <li>• Grade 2 - An action or incident that requires immediate management attention. It can be an accumulation of three Grade 1 actions or incidents.</li> <li>• Grade 3 - An action or incident that poses a significant risk to business operations or the AFS licence or has resulted in direct financial loss by a client. It can be one action or incident or an accumulation of four or more Grade 1 or two or more Grade 2 actions or incidents.</li> <li>• Grade 4 - An action or incident that requires urgent management attention and poses a serious risk to business operations or the AFS licence (includes major compliance failures, training inadequacies and overall poor performance).</li> <li>• Grade 5 - An action or incident that poses a catastrophic risk to business operations or the AFS licence and cannot be rectified.</li> </ul> |
| Systemic Breach(es)                        | <ul style="list-style-type: none"> <li>• No</li> <li>• Yes [please provide additional details]</li> <li>• Other [please provide additional details]</li> </ul>  |

## Completing Part D: Complaints reporting

---

This part of the ACS deals with complaints<sup>3</sup> received during the reporting period. The following tables show how we classify complaint products, issues and outcomes.

### Definition of Complaint

[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.<sup>4</sup>

Please note obligations under [RG271](#) became effective 5 October 2021.

**All** complaints are to be reported, including complaints that are resolved to the client's complete satisfaction by the end of the fifth business day.

All complaints should also be classified regarding product involved, issue involved, outcome and resolution timeframe as per ASIC's [IDR Data Reporting Handbook](#).

### Recording complaints involving multiple products, issues

Where a complaint involves multiple products and issues, please report all the relevant products or issues related to that complaint.

Example: A client lives in a flood prone area and asks their broker to find a policy that covers both home building and contents, and damages as a result of floods. The broker sets up a policy, which they believe meets the client's needs. A flood affects the client's property causing structural damage and destroying furniture. The client lodges a claim for structural damage and the loss of contents. The insurer denies the claim on the basis that the client's policies did not cover losses suffered from flooding. The client lodges a complaint about the broker's failure to obtain insurance covering their needs, despite them living in a flood prone area.

- This complaint involves the following products:
  - home building (ASIC reference 41) and
  - home contents (ASIC reference 42).
- This complaint involves the following issues:
  - Denial of claim – exclusion/condition (ASIC reference 50)
  - Failure to follow instructions/agreement (ASIC reference 67)

### Products

Product categories are defined as per ASIC's [IDR Data Reporting Handbook](#) Table 9.

If you are not able yet to provide specific categorisation as per the ASIC IDR Data dictionary, please use the main categories:

- *D.3.1 Domestic Insurance (ASIC 40 to 58)*
- *D.3.2 Extended Warranty (ASIC 59 to 62)*
- *D.3.4 Professional Indemnity (ASIC 63 to 64)*

---

<sup>3</sup> Terms have been defined with reference to the ASIC Regulatory Guide 78 – Breach Reporting by AFS Licensees, the Australian Standard AS 3806 2006 – Compliance Programs, Section 912D of the Corporations Act 200.

<sup>4</sup> As per AS/NZS 10002:2014 and ASIC RG 271.27.

- *D.3.5 Small business/farm insurance (ASIC 65 to 79)*
- *D.3.5 Other [please provide additional details]*

Where a complaint involved multiple products, please list all the products related to the complaint.

## Issues

Issue categories are defined as per ASIC's [IDR Data Reporting Handbook](#) Table 17.

If you are not able yet to provide specific categorisation as per the ASIC IDR Data dictionary, please use the main categories:

- *D.4.1 Advice (as per ASIC reference 1 to 3)*
- *D.4.2 Charges (as per ASIC reference 4 to 13)*
- *D.4.3 Consumer Data Right (as per ASIC reference 14 to 20)*
- *D.4.4 Disclosure (as per ASIC reference 26 to 30)*
- *D.4.5 Financial difficulty/debt collection (as per ASIC reference 31 to 40)*
- *D.4.6 Financial firm decision – specific to insurance (as per ASIC reference 45 to 54)*
- *D.4.7 Financial firm decision – general (as per ASIC reference 58 to 65)*
- *D.4.8 Instructions (as per ASIC reference 66 to 68)*
- *D.4.9 Privacy and confidentiality (as per ASIC reference 70 to 72)*
- *D.4.10 Scams/fraud (as per ASIC reference 73 to 76)*
- *D.4.11 Service (as per ASIC reference 77 to 88)*
- *D.4.12 Transactions (as per ASIC reference 89 to 96)*
- *D.4.13 Other (please provide details)*

Where a complaint involved multiple issues, please list all the issues related to the complaint.

## Outcomes

Outcome categories are defined as per ASIC's [IDR Data Reporting Handbook](#) Table 18, including:

- *Service-based remedy (ASIC reference 1)*
- *Monetary remedy, please advise total \$ amount (ASIC reference 2)*
- *Contract/policy variation (ASIC reference 3)*
- *Decision changed (ASIC reference 4)*
- *Other remedy (ASIC reference 5)*
- *Withdrawn/discontinued (ASIC reference 6)*
- *Referred to another financial firm (ASIC reference 7)*
- *No remedy provided/ apology or explanation only (ASIC reference 8)*
- *Unresolved as at 31 December 2022*

Any outcome which does not fit into any of the provided categories should be listed under 'other' and additional information to be provided.

## **Resolution timeframes**

Resolution timeframe categories are pursuant to ASIC Regulatory Guide [RG271](#) Internal Dispute Resolution, Part C and current obligations under Service Standard 10 of the Code, including:

- *Resolved within 30 days*<sup>5</sup>
- *Resolved beyond 30 days*
- Unresolved as at 31 December 2022

Any complaint which does not fit into any of the provided resolution timeframes should be listed under 'other' and additional information to be provided.

## **Complaints not resolved within 30 days**

Please provide primary reasons for any complaints that have not been resolved within 30 days.

---

<sup>5</sup> Pursuant to ASIC Regulatory Guide [RG271](#) Internal Dispute Resolution, Part C and section 9.4(b) of the 2022 Code.

## **Completing Part E: Good industry practice**

---

Responses to Part E.1 provide some insight into how Code subscribers share value and norms to shape behaviours and mindset reflected in the company culture.

## **Completing Part F: Code Transition and Implementation**

---

Responses to Part F will inform the IBCCC's Own Motion Inquiry (OMI) into Code subscribers transition to the 2022 Code.

This OMI will inform the IBCCC's understanding of what steps Code subscribers have taken to work towards compliance with the 2022 Code, including:

- F.1 Transition to the 2022 Code
- F.2 Governance Processes
- F.3 Post Implementation Reviews, and
- F.4 Resource requirements to transition to the 2022 Code.

Code subscribers are required to work towards compliance with the 2022 Code by 1 November 2022. The IBCCC acknowledges that it takes time to implement a new Code within an organisation and is keen to understand steps taken to implement the Code. The IBCCC can draw on good practice examples to be shared with the industry.

The 2022 Code introduces new obligations for Code subscribers including supporting clients experiencing vulnerability, a ban on preferential remuneration and increased disclosure requirements. The IBCCC understands that new processes and procedures may need to be developed to comply with these obligations.

## **Completing Part G: Supporting clients experiencing vulnerability**

---

Responses to Part G will inform the IBCCC's OMI into how Code subscribers support clients experiencing vulnerability and what policies, processes and training is in place to support this.

The purpose of this inquiry is to monitor and encourage good practice compliance with section 10 of the 2022 Code. To do this, the IBCCC will:

- a) establish industry practice concerning section 10 of the 2022 Code
- b) understand work undertaken by Code subscribers to work towards compliance with section 10 of the 2022 Code
- c) identify and share examples of good practice to help Code subscriber improve the ways they support clients, and
- d) make recommendations for industry improvement towards best practice.

The IBCCC is seeking to understand what Code subscribers are currently doing to support clients experiencing vulnerability and sharing examples of good practice.



## 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.

You will then receive an email from the IBCCC containing a hyperlink to the portal and password. This link is unique for each Code subscriber.

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

***It is important you do not share the link or the password with anyone who should not have access to the portal or the data being submitted, either internally or externally.***

### 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.

***If you have answered a question, please make sure you click 'Save and Next' before navigating backwards. If you do not do this, you will lose the data you have entered.***

### Saving data and returning later

The portal has been designed so you can complete part of a questionnaire and return later. Once you have completed the questions you wish to complete in a session, make sure you press the 'Save and Next' button at the bottom of the section. This will ensure that work you have completed is saved.

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

### Due dates for information requests

You will receive emails and documentation from the IBCCC which provides information about when the ACS must be completed. If, for some reason, you are unable to complete it by the date specified, please contact us as soon as possible (see contact details below).

### Loading and saving pages

In some cases, pages may take a few minutes to save, especially where there is a large amount of data or 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 few minutes for the page to update.

There is no specific 'time-out' period, but you are encouraged to 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 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 Detail Report into the portal. Please click 'Browse', select the required document from your computer, click 'Open' and then 'Submit'.

Where 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 your mouse and selecting 'Send to' - 'Compressed (zipped) folder'. Further information on creating a zip file may be available from your IT team or the internet.

## 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.

***Please make sure the data is correct before you submit it. You cannot amend the data after it has been submitted.***

If you consider the information is wrong, you should contact us immediately.

## Saving a record of the submission

On the final page and once the data has been submitted, there will a PDF icon displayed. By clicking and opening this icon you will have the opportunity to download the details of your submission and save a copy to your system.

The details will include the filenames of any uploaded documents, 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.

### *Physical Security*

- All production hosts are located in a Microsoft Azure cloud-based instance. This is Geo-Located in South East Australia and is secured behind their industry leading security controls.
- All data stored in the system is encrypted, including encryption at rest (all data files including backups).
- No data is stored or transmitted off-shore. Back-ups are stored in an Australian Hosted Azure instance.

### *Logical Security*

- All production hosts are protected by Microsoft Security controls, including Azure Sentinel, Azure Guardian and Azure Firewall – these controls include anti-virus, intrusion protection detection, denial of service detection, SPAM blockers, application control, reputation enabled defense and data loss prevention.
- All hosts are monitored and updated for threat protection. Updates are managed directly by Microsoft Engineers.

- All host access is via a strongly encrypted Virtual Protocol Network (VPN) requiring 2-factor authentication.
- All interfaces to admin functions are over Hyper Text Transfer Protocol Secure (HTTPS). No data can be transmitted over an unencrypted link.

### *Testing*

The Evolved Group regularly tests production deployments internally against OWASP Top 10 (utilising Zap tools). In addition, it does external pen tests with an external partner, Indigo IT Labs.

## **Contact us**

---

If you have any difficulties accessing the portal or any queries about completing the IBCCC's request for information, please contact:

- Daniela Kirchlinde (Code Compliance and Operations Manager), [dkirchlinde@codecompliance.org.au](mailto:dkirchlinde@codecompliance.org.au)
- Amanda Rosario (Senior Compliance Analyst), [ARosario@codecompliance.org.au](mailto:ARosario@codecompliance.org.au)
- [info@codecompliance.org.au](mailto:info@codecompliance.org.au)