CAO Manual: Annex 4

Review of Potential Breaches and Process Non-Conformances referred to the Commitments Assurance Office by Communications Regulation Compliance

1. PURPOSE

1. This document explains how the Commitments Assurance Office (CAO) reviews cases referred to it by Communications Regulatory Compliance (CRC) as potential breaches of the Commitments or Governance Protocol (hereafter "the Commitments") or non-conformances with policies designed to support the Commitments. Those cases are presented to the BT Compliance Committee (BTCC) for the ultimate decision.

2. CASE CATEGORIES

2. The BTCC considers not only potential breaches of the letter of the Commitments, but also situations in which employees may have failed to observe the spirit of the Commitments, for example by not following relevant policies and processes.

3. The various categories used by the BTCC and the CAO set out below.

2.1. Breaches

4. A breach requires an obligation in the text of the Commitments capable of being breached – either someone failed to do something they were supposed to do, or they did something they were not supposed to do. Breaches can be either trivial or serious (see Section 3 below).

2.2. Non-Conformances with Policy

5. There are circumstances in which behaviours do not meet what BT expects of its people but such behaviours do not constitute a breach. These are sometimes referred to as not meeting the "spirit" of the Commitments. Accordingly, the BTCC also looks at behaviours which do not align with BT policies, for example the rules put in place around Regulatory Compliance Markers to support the rules around information sharing in Section 10 of the Commitments. Non-conformances with policy can also be either trivial or serious (see Section 3 below).

2.3. "Near Misses"

6. "Near misses" occur where CRC has looked at an issue and concluded there has not been a breach of the Commitments or a non-conformance with process, but where there is nevertheless scope for learnings to prevent a future breach arising. For example, this could arise in a case about how Openreach Commercial Information (CI) is being managed. The investigation might identify weaknesses in how that Openreach information was being handled, but it turns out that the information in question was in fact publically-available and hence not CI.

7. Thus the BTCC wants to hear about and track instances of "near misses" as, over time, these may help to identify where proactive action can avoid actual breaches occurring in the future. As such "near misses" can also lead to remedial and consequential action as they still indicate the existence of compliance risk that needs to be adequately managed.

3. CLASSIFICATION OF CASES: TRIVIAL OR SERIOUS?

8. Cases are classified as trivial or serious using the Four-Box Framework adopted by the BTCC in September 2018. This assessment also uses the 7 factors in CAO's Case Serious Diagram to assess whether an issue is more likely to be serious or more likely to be trivial. Both diagrams are set out in Appendix 1.

9. The CAO's general approach is that it is more important to understand whether an issue is serious or trivial than whether it is a breach or a non-conformance with policy. While technically there is a difference in that only breaches need to be reported to Ofcom, in practice the CAO informs Ofcom of all cases decided by the BTCC and includes updates on them in the Bulletin to provide transparency to stakeholders.

4. BACKGROUND: CRC'S PROCESS FOR BRINGING ISSUES TO THE CAO

10. Issues that could result in a breach case or a non-conformance with policy go into CRC via a number of routes, including:

    a. Self-reporting by people involved (e.g. the sender or recipient of information that may not have been shared in line with the Commitments and/or relevant policies);

    b. Issues found during assurance activities by CRC; or

    c. Issues raised by CPs or other third parties.

11. CRC conducts an initial assessment of matters and reviews them on a triage call. At this stage matters are either closed down or proceed for investigation. The CAO periodically observes these calls to understand how CRC runs this process. The CAO will also periodically review CRC's triage log and conduct spot checks to understand CRC's analysis and approach as to why matters were closed down.

12. Once any investigation is concluded and the outcome agreed by the Senior Manager, CRC, each case is written up and sent to the CAO. Simpler cases can be written in a few paragraphs, while more complex or novel cases are more likely to require a fuller report. These are provided to BTCC members as part of the breach reporting and decision process, and thus they should briefly convey the essence of the issue under consideration with sufficient detail to enable the BTCC to reach a decision.

5. CAO REVIEW OF CASES SENT BY CRC

13. Cases sent by CRC are reviewed by the CAO. This review has two objectives:

    a. Is the case write-up sufficiently clear to enable the CAO to properly understand what has happened, and in turn to enable the BTCC to take a decision?; and

    b. Does the CAO agree with the recommendation of the Senior Manager, CRC?

14. As noted above, the CAO uses the 7 factors in the Breach Serious Diagram to consider whether any breach or non-conformance recommended by the Senior Manager, CRC as being trivial should, in fact, be categorised as serious. Set out below is an illustrative list of the themes the CAO considers, but broadly the CAO looks at each case in the round and asks questions as necessary to ensure it has a proper understanding of the matter.

5.1. People

15. The following should be clear:

    a. **What was the context?** Did the issue arise in the normal course of people's work, or was this something atypical? If it was atypical, why was this happening?

    b. **Who was involved?** Does it include sufficient detail about the roles and job titles of the people involved so that the CAO can assess the seniority of those involved?

    c. **Length of service**. How long people have been in their roles is relevant to understanding whether something was a one-off, or an indication of a more fundamental structural issue where a team could be expected to have known what to do.

    d. **Has Commitments training has been provided previously?** If yes, how long ago? If no, why not?

5.2. Facts

16. The case write-up should make it clear what has happened, including dates and times as relevant, and in chronological order. The CAO will look to confirm the following:

    a. For cases concerning the sharing of Openreach CI or Customer Confidential Information (CCI), there should be a high-level description of the relevant information so that it conveys the nature of what the recipient received. This should also list out the products that the information relates to, where relevant.

    b. If it involves Openreach CI, CCI or Commercial Policy there should be clear identification by CRC of which sub-category is relevant per the definitions in the Commitments.

5.3. Is it clear why the issue happened?

17. The case write-up must include an explanation of what outcome the relevant people were seeking to achieve in their actions and their overall purpose. This explanation is essential to assessing the triviality or seriousness of a case. For example:

    a. if someone incorrectly shared CI or CCI, what was the context within which it was shared?

    b. If someone tried to escalate via a non-standard process, what was their motivation for doing so?

5.4. Impact of the issue on CPs

18. The case write-up should consider what the impact has been, or could have been, both for BT CPs as well as non-BT CPs. The CAO looks both at whether some sort of unfair benefit was received by BT CPs, as well as whether there was some form of negative impact on non-BT CPs. In general terms the greater the impact (either way), the more likely the CAO is to consider a matter to be serious rather than trivial.

5.5. Repetition v One-Offs

19. The CAO considers not just the immediate issue presented by CRC, but also whether the same or similar conduct has been observed previously. The CAO will consider:

    a. Has it happened before in that team?

b. Has it happened before elsewhere in BT?

c. Have there been any previous "near misses"?

d. Have there been non-conformances prior to a potential breach?

e. Have there been trivial breaches prior to a potential serious breach?

5.6. Root Cause Analysis

20. The CAO will review the explanation offered about the root cause analysis, and consider whether this properly distinguishes between the between the true root cause and other causal factors.

21. The case write-up should clearly get to the true root case, because if this is not done correctly, there is a risk that the problem will simply keep recurring until the true root cause is dealt with.

6. REMEDIAL AND CONSEQUENTIAL ACTIONS

22. The case write-up should set out both categories:

    a. **Remedial actions** are those taken to correct the immediate breach or non-conformance i.e. verification that an erroneous email has in fact been deleted.

    b. **Consequential actions** are further steps taken to mitigate the risk that the issue in the case does not arise again. This could include additional briefings being sent to relevant teams, or extending planned audits to cover the themes in the case.

23. For each action, the CAO seeks assurance that the remedial and/or consequential actions have been completed. A case will remain open until such assurance is received, and while the actions remain open, the case will feature in each breaches paper to the BTCC. If remedial actions are not completed or there is excessive delay in completing them, the relevant Senior Manager or Director will be invited to the BTCC to provide an update in person on current status and the roadmap to resolution.

7. FINALISING PAPERS FOR THE BTCC

24. All potential breach and non-conformance cases must come to the BTCC for decision with a clear recommendation from the Senior Manager, CRC. The CAO will engage with CRC to ensure that the submissions contain sufficient and relevant information, but authorship of the document and responsibility for the final content remain with CRC.

25. The format of case reports will depend on the case – more straightforward cases may tend to be shorter (a few paragraphs), whereas complex or novel cases may be longer (several pages). Reports for complex or novel cases are appended to the Breaches Paper submitted to the BTCC. These appendices are clearly presented as coming from CRC, so it is vital that any questions about or changes to the paper are sent back to the original author of the paper for their agreement.

8. MANAGING DIFFERING VIEWS BETWEEN THE CAO AND CRC

26. For each BTCC meeting, the CAO include its own Breaches Paper in the BTCC pack, which summarises each case and sets out the CAO's views on each.

27. If the CAO does not agree with a particular case recommendation from BT, it will explain why. The CAO will engage with the Senior Manager, CRC to understand where there are points of agreement, and where there are points of difference. The CAO would not expect differences of opinion on the facts – these should be uncontroversial as between the CAO and CRC. If such a difference of opinion does emerge, this is an indication that the case is not ready to go to the BTCC for decision pending further clarification of the facts.

28. There may be differences of views between the CAO and CRC around the analysis of the issue. Again, the CAO and CRC should work to find common ground to the extent possible – for example, if both parties agree that information was Openreach CI, then this will be stated, and any debate between the CAO and CRC framed around whether the issue is trivial or serious. This helps to ensure that time before the BTCC is used efficiently on the issues of significance. The BTCC will expect to see proper engagement between the CAO and CRC to handle the matter professionally.

APPENDIX 1

(a) The "Four Box Model" to assess issues as Serious or Trivial

The BTCC adopted the framework below in September 2018 to classify the compliance matters referred to it for consideration. This framework was subsequently adopted by the Openreach Board Audit, Risk & Compliance Committee.

Trivial Breach A breach of the letter of the Commitments, but not one that is likely to have caused any CP harm. *e.g. Information sent in error to a person not entitled to see it, and then recovered before it was seen.*	**Serious Breach** A breach of the letter of the Commitments that could well have caused harm. *e.g. BT "interfering with/working on" the Openreach access or backhaul network.*
Trivial Non-Conformance Not a breach of the letter of the Commitments, but individuals have not correctly followed processes, but no real harm done. *e.g. An individual is entitled to see Openreach CI but forgets to turn on their supplier marker before receiving it.*	**Serious Non-Conformance** Not a breach of the letter of the Commitments, but individuals have done something that is seriously wrong, where harm might be done, or where the actions are clearly not in the spirit of the Commitments. *e.g. single individuals act contrary to guidance provided to them in the published Code of Practice.*

(b) The 7 Factor Case Seriousness Diagram