ADELARD

CAE MINI-GUIDE 4: CAE CONNECTION RULES

Summary

This document is part of the Declare CAE guidance document set. It contains guidance on the application of the CAE connection rules.

24 Waterside
44–48 Wharf Road
London
N1 7UX

T +44 20 7832 5850
F +44 20 7832 5870
E office@adelard.com
W www.adelard.com

Authors
Robin Bloomfield
Nick Chozos

Distribution
As per Cinif list in
Adelard D1284v10

Contents

Figures

Tables

1 Introduction

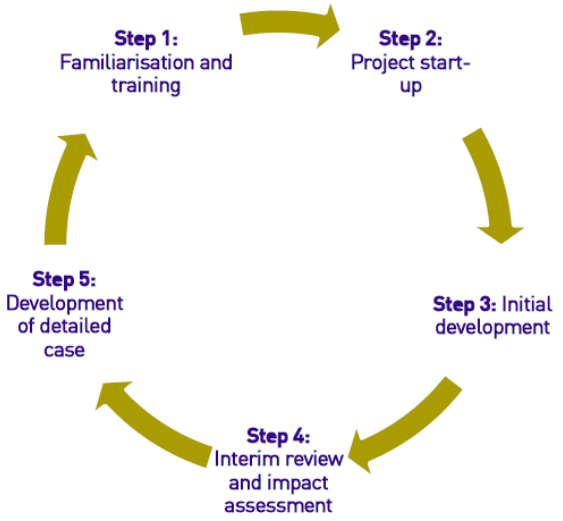
This document is part of the Declare CAE guidance document set. It contains guidance on the application of the CAE connection rules.

2 This mini-guide and the CAE document set

The CAE guidance can be seen as having two main components:

1. **CAE process:** The first component describes an overall process made up of five steps (the "CAE process"), explaining the evolution of a justification within an organisation and the activities involved. The approach is flexible, adaptable, and will apply differently to different scenarios of use.
2. **CAE mini-guides:** The second part provides specific technical guidance on the underlying concepts, their definition and their application. We have compartmentalised the technical guidance into "mini-guides": small, dedicated sets of guidance each focusing on a particular issue. Each mini-guide contains a concise summary with a short list of the key points and risks and challenges that need to be considered, which is then supported by more detailed guidance.

The CAE process, and the supporting mini-guides, are summarised in Figure 1 below. This document is highlighted (mini-guide 4). For a list of all currently available mini-guides, please refer to Section 6.2.



	Mini-guide
1.	One-page guidance
2.	CAE concepts
3.	Formulation of top-level claim
4.	**Connection rules**
5.	The CAE building blocks
6.	Summarising and communication
7.	Review and challenge

Figure 1: Summary of the CAE process and supporting mini-guides

The overall CAE process is described in the main CAE guidance document [1]. The main guide explains the various scenarios of use and how the guidance may apply in different cases. The document also discusses how the mini-guides may be used in different scenarios and at different phases of a project.

Table 1 below illustrates how this mini-guide applies throughout the CAE process.

CAE steps	CAE connection rules
Step 1: Familiarisation and training	Review and preparation
Step 2: Project start-up	-

CAE steps	CAE connection rules
Step 3: Overview and initial development	Application during development of outline case – refinement is expected in next steps
Step 4: Interim review and safety case impact assessment	Full application on all nodes for purposes of review Review upwards as evidence is being linked to claims
Step 5: Development of a more detailed case	Iteration of Step 4 until all evidence has been linked to case Guidance may be used for review and challenge

Table 1: Relationship of this mini-guide to the CAE process

3 CAE connection rules

There are a number of rules that place constraints on the manner in which the components of CAE are linked. These rules are important as they help to achieve consistency in the presentation of a CAE structure, and more importantly help to avoid some of the risks that may arise from a free form approach.

This guidance contains a number of rules (referred to in the rest of the document as the "CAE normal form") that make a CAE structure more consistent and easier to read. These rules place constraints on the way that claims, arguments and evidence may be linked in a CAE structure. The purpose of these rules is to help avoid some issues arising from a free form style of construction, yet recognise that different styles are appropriate. For example, we want to support, especially in the initial stages of case exploration, a more brainstorming and free form approach.

We first propose these rules and then we discuss in a small example how a CAE structure might evolve using the CAE connection rules.

CAE normal form has the following characteristics:

1. Claim nodes may *only* be connected to argument nodes, i.e., evidence cannot support a claim without an intervening argument. Claims cannot be split into subclaims without an argument.
2. Argument nodes may *only* be connected to claim and evidence nodes, i.e., argument nodes are not connected to other argument nodes.
3. Each argument node may *only* have one outbound link to a claim node, i.e., it can only support one claim.
4. Evidence nodes may *only* be connected to argument nodes.
5. Each claim is to be supported *by one and only* one argument. If two arguments appear to be both reinforcing the same claim, consider why this is so and explain the increase in confidence or reduction in assumption doubt that might be brought about. This will involve making the claims more precise and adding an additional argument.
6. Argument nodes must be supported by at least one subclaim or evidence node.
7. Evidence nodes represent the bottom of the safety argument and are not supported; they represent agreed facts.
8. A claim or a subclaim may support more than one argument and similarly, one evidence node may be used by more than one argument.

These connection rules do not apply to context nodes, which can be connected to any type of node.

The table below (Table 2) summarises what is allowed and what is not when linking the various components of the CAE, assuming the direction of links is flowing upwards and towards the top-level claim.

Allowed	Not allowed
Claim to Argument or several Arguments	Claim to Evidence Claim to Claim Unsupported Claims
Argument to single Claim	Argument to Evidence Argument to Argument (needs claim between) Argument to multiple Claims Unsupported Arguments (but might occur in case development)
Evidence to Argument	Evidence to Claim Evidence to Evidence (sometimes used to show structure of evidence)

Table 2: CAE linking rules

The use of the normal form has the effect of encouraging the safety case author to be more precise about the claims being made and more explicit about the supporting arguments for those claims. Furthermore, following the normal form will help to achieve consistency in how CAE is used (developed and read) within an organization.

An example of the application of the rules is shown in Figure 2, where the parts not in normal form are highlighted in red.

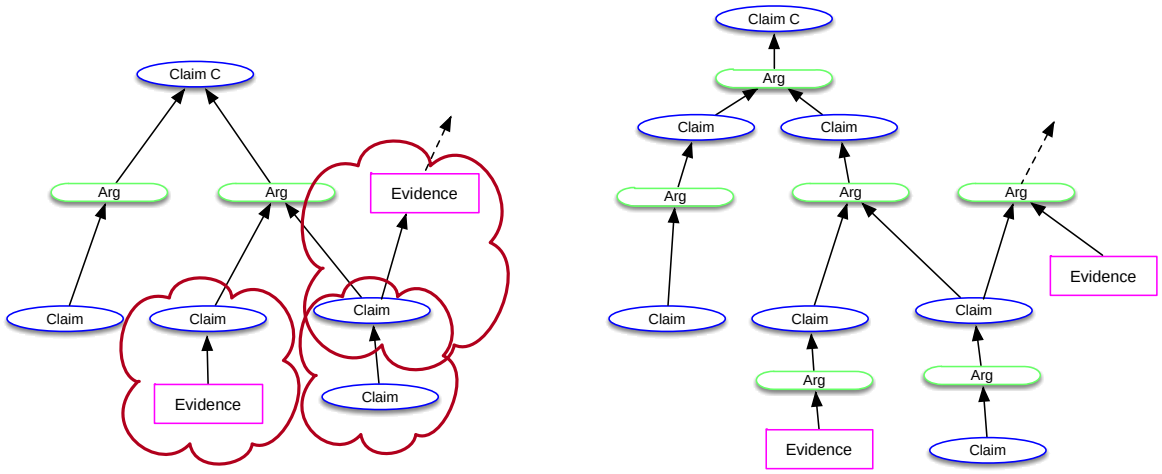


Figure 2: Example of a claim structure before and after normal form

In the example above, we see an evidence node being directly connected to a claim. This goes against the rules suggested by the CAE normal form. An argument is needed between them, explaining how and why the evidence supports the claim, potentially including statements regarding the quality and trustworthiness of the evidence.

A lot of these practices are common in the CAE community, typically because people instinctively wish to "tell the story" as it flows in their minds and naturally in conversation. It can leave room for assumptions to

go unnoticed, positive bias to occur, misunderstanding to take place, or just reduce efficiency by requiring the audience to ask more questions until the argument is eventually rephrased. Normal form helps avoid risks associated with this, and also helps achieve consistency in how an organization uses CAE – something which is an important requirement and driver for the Declare project.

In addition to the restrictions posed by normal form, we require arguments to be conjunctions of the subclaims and evidence. Note that when satisfying a subclaim, it must not be forgotten that the other subclaims are also true: the graphical format may hide significant dependencies. We have found that a disjunctive combination of claims (logical OR) is not normally appropriate: even when there is diversity, both subclaims are usually required to ensure that the parent claim holds with sufficient confidence[1].

3.1 Evolving the topology of the case

In this section we discuss how a CAE structure may evolve as we develop it in light of the above rules. It is based on examples we have seen, but anonymised.

The first stage of developing a case might be a brainstorm that identifies a top-level claim along with the five supporting arguments as shown in Figure 3.

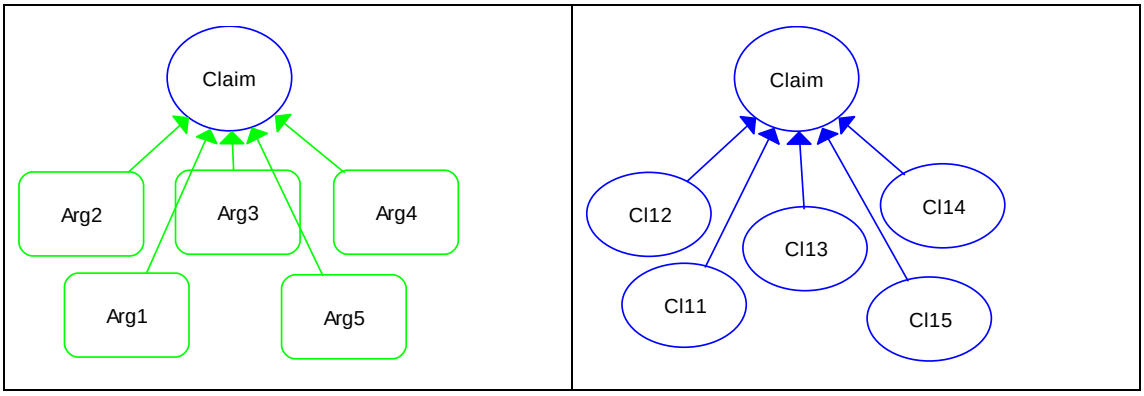


Figure 3: Initial structure

When reviewed it is likely that these are not arguments but actually supporting subclaims. So the first stage of evolving the structure is to redraw this as shown in the right hand side of the figure. If in fact there really were five arguments then, as we suggest in the guidance, more analysis of the claim is probably needed.

In reclassifying the arguments as claims, there will probably be a need to rework and update these new claims.

[1] Of course in classical propositional logic one could move between a conjunctive and disjunctive normal form

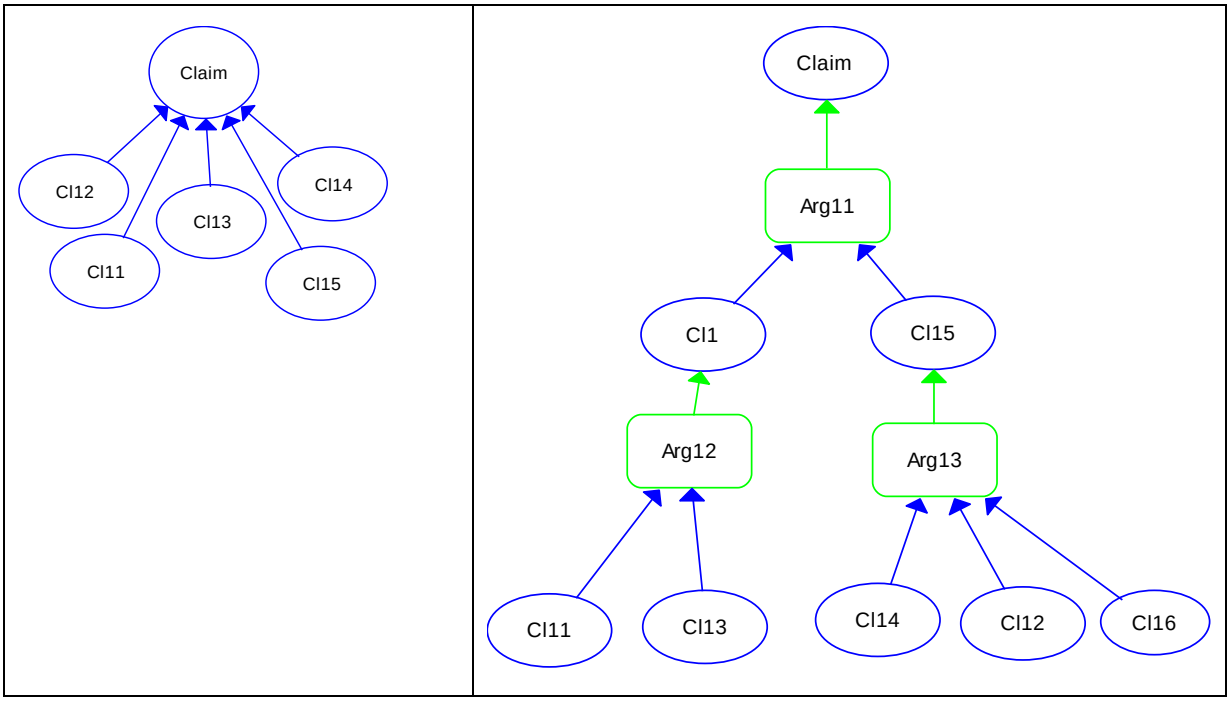


Figure 4: Adding arguments – discovering claims

Having established the top-level claim and some of the subclaims that support it, it is necessary to identify the arguments that give the reasons why these subclaims support the top-level claim. This is where the CAE blocks are helpful, as we can use them either bottom up or top down to arrive at a structure as in the right hand side of Figure 4. In doing so, we have identified intermediary subclaims. Also we find, in this example as we have seen in practice, a claim was missing in Figure 2. We can also now see how the top claim is supported by two main "legs".

The next stage of the CAE evolution is to identify and map the evidence to the subclaims. Here we find that one subclaim is unsupported by evidence and that some evidence supports several claims. This may warrant a further decomposition of the structure to understand in what way the evidence contributes: we may need more precise claims to see the role of the evidence and to assess if it is redundant, as there may be savings from not using it. The resulting structure is shown Figure 5 below.

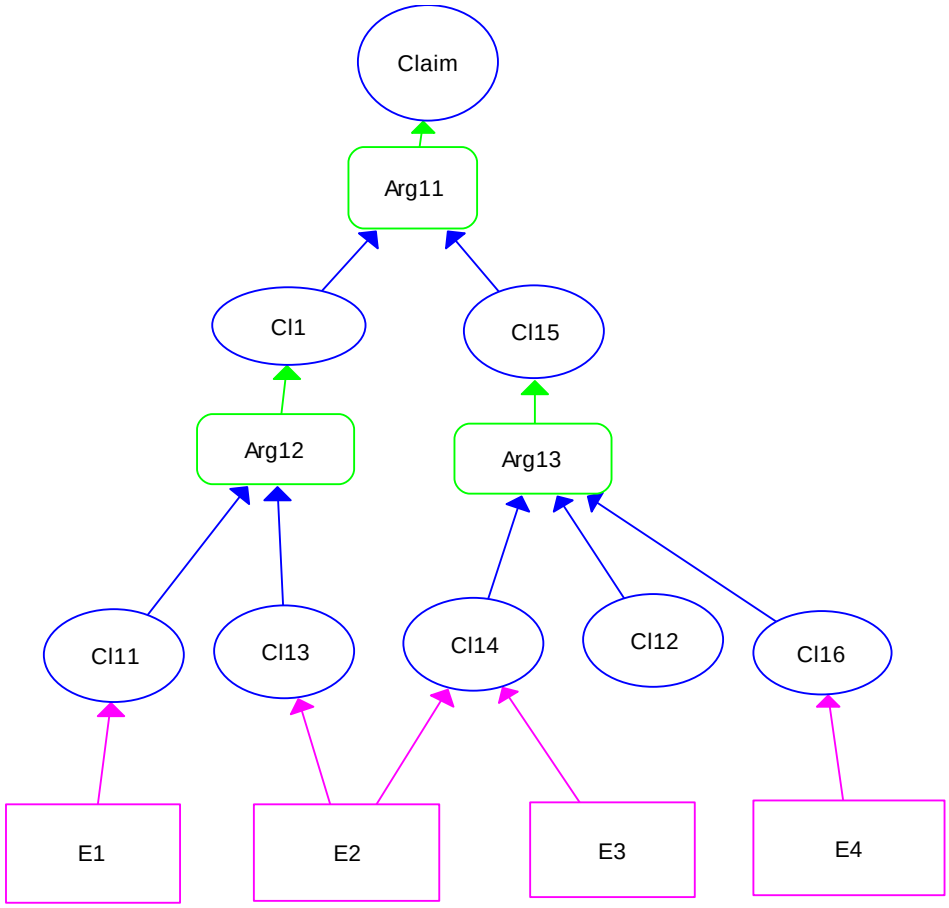
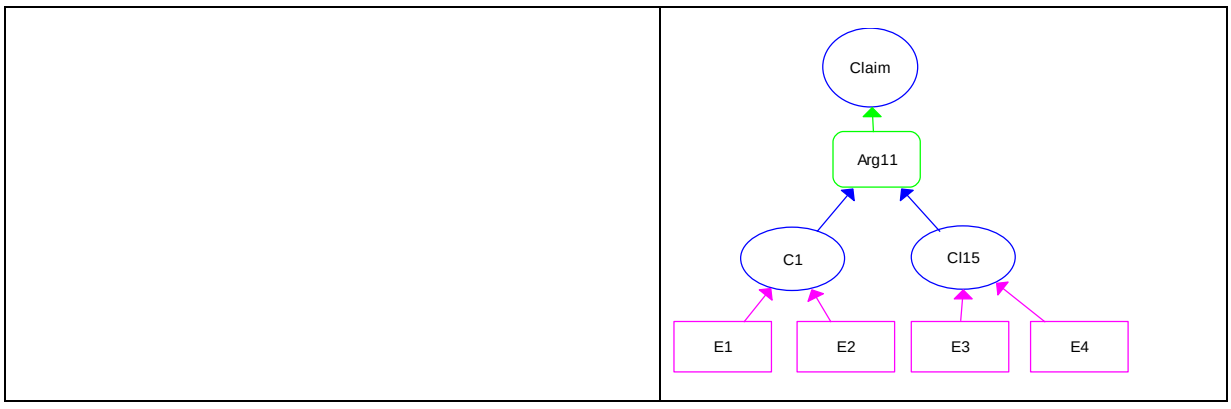


Figure 5: Identifying the role of evidence and gaps

Although Figure 5 is small enough to be readily assimilated, in more complicated CAE structures there may be a need to provide a summary. Figure 6 illustrates two options for summarising. One takes the top of the case, showing the two legs, and provides the main claims and main evidence sources. The second approach is to suppress the arguments and provide a structure that shows all the claims. Of course, summaries by their nature omit things; in the first summary it is not shown that there is an unsupported claim.



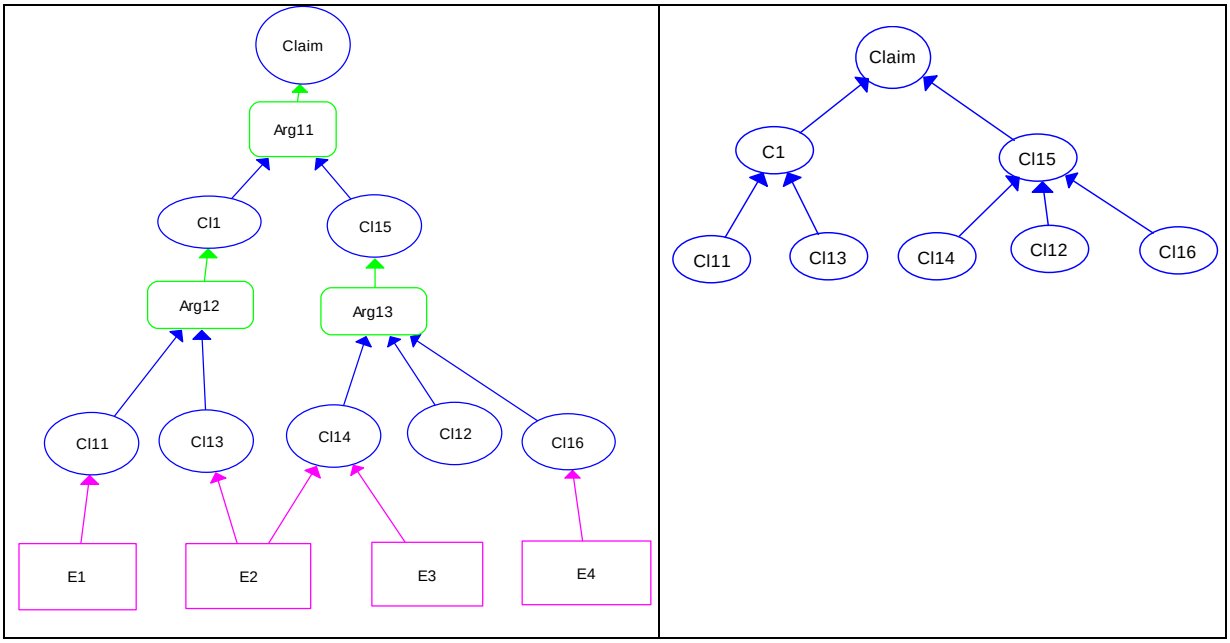


Figure 6: Options for summarising

We have also received feedback from stakeholders that sometimes a mixed graphical and textual or tabular approach is useful. For example, the top set of claims could be defined in the CAE graphical notation as in the bottom of Figure 6, with the subclaims and evidence supporting the claims at the edges of the tree structure, and then expanded in tables within the supporting textual document.

4 Summary guidance

- This document contains a number of connection rules (referred to as "normal form") that help to ensure correct and consistent use of the CAE approach, and the way that Claims, Arguments and Evidence are linked graphically.
- CAE normal form has the following rules:

1. Claim nodes may *only* be connected to argument nodes, i.e., evidence cannot support a claim without an intervening argument. Claims cannot be split into subclaims without an argument.
2. Argument nodes may *only* be connected to claim and evidence nodes, i.e., argument nodes are not connected to other argument nodes.
3. Each argument node may *only* have one outbound link to a claim node, i.e., it can only support one claim.
4. Evidence nodes may *only* be connected to argument nodes.
5. Each claim is to be supported *by one and only* one argument. If two arguments appear to be both reinforcing the same claim, consider why this is so and explain the increase in confidence or reduction in assumption doubt that might be brought about. This will involve making the claims more precise and adding an additional argument.
6. Argument nodes must be supported by at least one subclaim or evidence node.
7. Evidence nodes represent the bottom of the safety argument and are not supported; they represent agreed facts.

8. A claim or a subclaim may support more than one argument and similarly, one evidence node may be used by more than one argument.

5 Acknowledgements

We would like to thank Sellafield Ltd and ONR for their high level of engagement with the project, and particularly Sellafield Ltd for their support and involvement in the project workshops.

This deliverable draws on a number of sources developed in earlier Cinif, SSM and Adelard projects (and in particular.

6 Bibliography

6.1 CAE main-guide

[1] Bloomfield R, Chozos N, Declare: CAE main guidance and process, Adelard document reference D/1284/43195/2, version v1.0, April 2020

6.2 CAE mini-guides

[2] Bloomfield R, Chozos N, CAE mini-guide 1 – One-page guidance, , Adelard document reference W/3104/43195/1, version v1.0, April 2020

[3] Bloomfield R, Chozos N, CAE mini-guide 2 - CAE concepts, Adelard document reference 2, Adelard document reference W/3104/43195/1, version v1.0, April 2020

[4] Bloomfield R, Chozos N, CAE mini-guide 3 – Formulation of top-level claim, Adelard document reference 2, Adelard document reference W/3104/43195/1, version v1.0, April 2020

[5] Bloomfield R, Chozos N, CAE mini-guide 4 - Connection rules, Adelard document reference W/3104/43195/1, version v1.0, April 2020 (this document)

[6] Bloomfield R, Chozos N, CAE mini-guide 5 - The CAE building blocks, Adelard document reference W/3104/43195/1, version v1.0, April 2020

[7] Bloomfield R, Chozos N, CAE mini-guide 6 – Summarising and communication, Adelard document reference W/3104/43195/1, version v1.0, April 2020

[8] Bloomfield R, Chozos N, CAE mini-guide 7 - Review and challenge, Adelard document reference W/3104/43195/1, version v1.0, April 2020