Framework and Process to Understand Software Safety Practice

NOTE: Any suitable modelling notation may be used to instantiate the process to understand and assess safety engineering practice.

Safety Engineering Practice

The Framework employs three elements of safety practice, namely:

- Safety Practice **as-desired**
- Safety Practice **as-required**
- Safety Practice **as-observed.**

All existing (safety) **(<Practice As> <X>)** can be mapped onto these three elements, and whilst it is argued this is necessary, it cannot yet be argued whether this is complete - although further instantiations of the process will reveal the levels of confidence in completeness.

The main elements of safety practice, and their relationships are shown in Figure 1 – with each number representing an activity within the process to understand safety practice.

The Framework:

1. As-desired safety practice model
2. Safety practice as represented by an Open Standard
3. An organisation's safety engineering processes (as-required)
4. Safety practice as carried out (as-observed)
5. Degree of conformance between an organisation's safety engineering processes with safety practice as- desired
6. Degree of conformance between the Open Standard with the safety practice as-desired
7. Degree of conformance between the safety practice (as-observed) and the safety engineering practice (as-required)
8. Degree of conformance between the organisation's safety engineering lifecycle (as-required) and the Open Standard which informed / influenced its development
9. Degree of conformance between the safety practice (as-observed) with the as-desired model
10. Degree of conformance between the safety practice (as-observed) with safety practice (as-required).

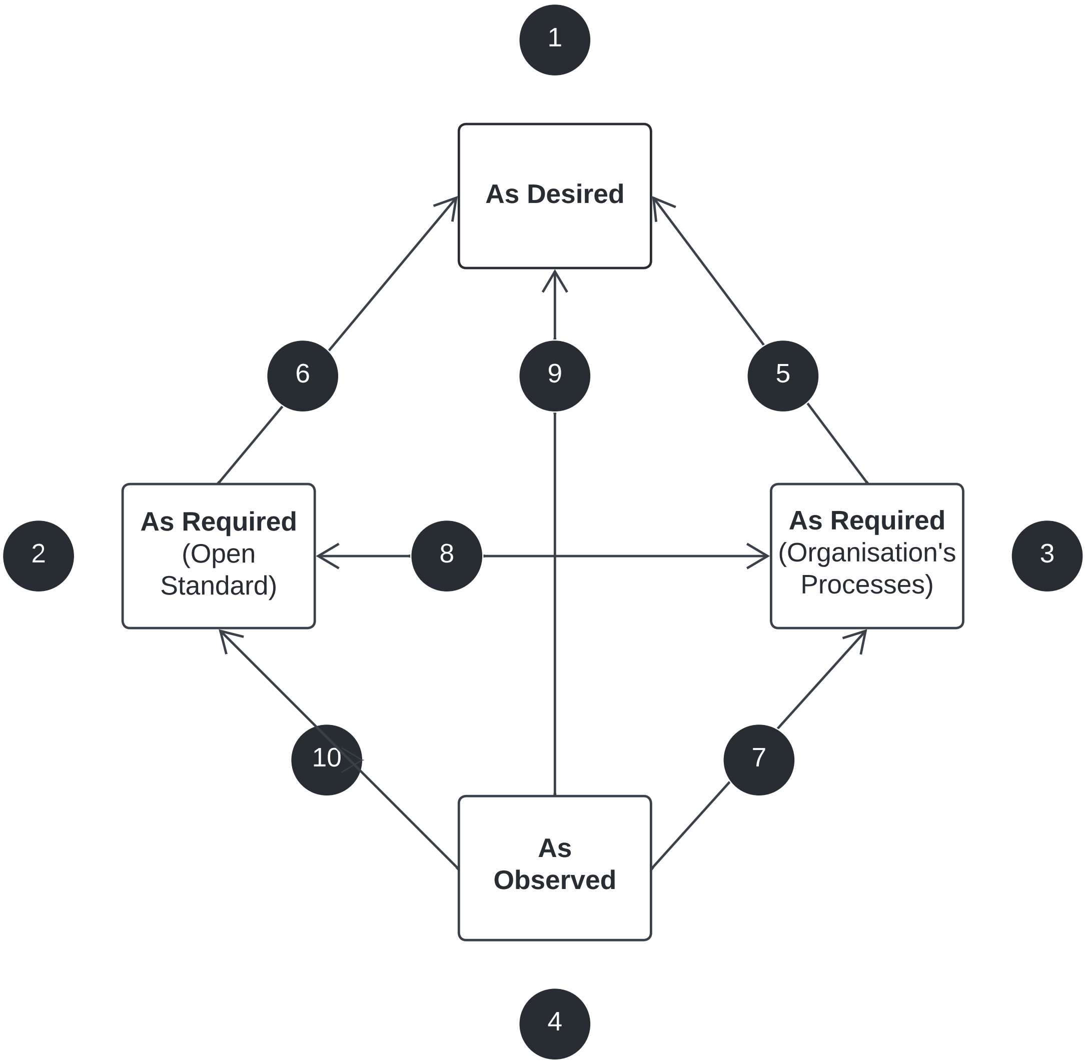
1
As Desired
6
9
5
2
As Required (Open Standard)
8
As Required (Organisation's Processes)
3
10
7
As Observed
4

Figure 1: The Elements of Software Safety Practice

To instantiate this framework for a given organisation the following activities must be undertaken:

1. Model and **r**epresent the organisations as-desired model
2. Model and represent the relevant Open Standard using the selected notation
3. Model and represent the organisations' safety engineering processes (as-required) using the selected notation
4. Model and represent safety practice as carried out (as-observed) using the selected notation
5. Compare the organisation's safety engineering processes (as-required) with the as-desired model
6. Compare the selected Open Standard with the as-desired model
7. Compare safety practice (as-observed) with the safety engineering processes formulated by the organisations' lifecycle (as-required)
8. Compare the organisations' safety engineering lifecycle (as-required) and the Open Standard which informed/influenced its development

9. Compare safety practice (as-observed) with the organisations as-desired model
10. Compare the organisations safety practice (as-observed) with an Open Standard.

Note that Step 9 makes it possible to identify whether software safety practitioners are overcoming perceived deficiencies in the as-required practice in order to meet the as-desired model (intentionally or otherwise). This ensures the process identifies any subtle changes made by those instantiating an organisations safety activities with regard to the as-desired model of practice.

It is possible that these practitioner instigated variations may not actually improve software safety practice, and may instead undermine other elements of practice. They may also introduce new issues. By considering all elements of software safety practice (and the interrelationships between them) the process facilitates the identification and subsequent effective mitigation of the risk of unintentionally undermining software safety practice.

Step 10 of Figure 1 is in place as it is entirely possible that software safety practitioners charged with implementing as-required practice may indirectly/directly appeal to the normative requirements and/or informative guidance from an Open Standard they are familiar with. This could be to recover perceived shortfalls in the as-required processes, or could simply be a default to a standard they know well.

Identify the Activities and Articles Employed

To instantiate the framework effectively, the process must be capable of modelling:

- The activities required of a safety engineering lifecycle
- The required inputs to, and outputs from each activity in a safety engineering lifecycle
- The interactions required throughout a safety engineering lifecycle
- The relationships, dependencies, and constraints
- Methods or techniques that control an activity (such as an international standard that guides the conduct of a safety engineering activity)
- The resources required for each activity (both people and materiel).

To ensure widespread use, the selected representation should also be:

- Ready for use with minimal adaptation
- Capable of use without the need for proprietary software
- Saveable in a portable format
- Capable of construction and analysis in the absence of formal modelling knowledge
- Understandable and interpretable in the absence of prior ontological knowledge/experience
- Capable of construction in the absence of complex background databases.

Further, the ten elements of the framework address four types of practice and their inter-relationships. The process is now outlined. The process encompasses four modelling steps (1-4) and six analysis steps (5-10); each of which take a baseline model from steps 1-4 and annotates it accordingly. Finally, there is a further activity not represented in Figure 1, and this concerns the maintenance of the process outputs throughout the life of a product/project.

The Process:

The proposed process steps associated with the framework each has an Objective, Inputs, Tasks, and its Outputs are shown below. Each step requires a Suitably Qualified and Experienced Person (SQEP) to undertake the process. The argument of what constitutes a SQEP individual is outside of the scope of this document.

STEP 1: Model Safety Practice As Desired

OBJECTIVE:

Define safety practice as desired for the organisation wishing to understand and assess their safety practice.

INPUTS:

An organisation wishing to model Safety Practice as-desired requires the following inputs:

- A Safety Philosophy
- A Risk (acceptance and tolerance) Policy
- A Safety Management Philosophy (which may be instantiated as a Management System and Plan(s))
- A suitably qualified and experienced Safety Manager to determine, represent and agree with the product owners the model of as-desired practice.

TASKS:

1. Define Safety Practice As Desired.

Asserting what constitutes safety practice as-desired is perhaps the most challenging and complex attribute of understanding any aspect of safety engineering practice.

2. Create a tangible and measurable representation of Safety Practice As Desired.

Notwithstanding the complexities and challenges of this task, the organisation must create a representation of as-desired practice which is both tangible and measurable.

OUTPUTS:

The output of this step is either a graphical representation of the model of as-desired practice, or a set of measurable criteria which can then be used to assess the other elements of safety practice for compliance.

STEP 2: Model Safety Practice As Required (Open)

OBJECTIVE:

There are two ways in which safety practice ‘as-required’ is currently modelled and represented in industrial practice. The framework and associated process for understanding safety practice is designed to allow both ways to be modelled, and any relationships between them to be understood and assessed. The process also facilitates the assessment and comparison of both types of as-required practice with safety practice as-desired, and safety practice as-observed. Both types of as-required practice are now considered in turn.

The first way as-required practice is modelled and represented textually by Open Standards such as ARP 4754A or BS EN 61508. Standards such as these prescribe a set of lifecycle activities that are argued by their developing committees to represent good practice. The objective here therefore, is to employ a process to model the set of lifecycle activities described by the relevant Open Standard which may have influenced the development of organisational practice. This is done to facilitate later analysis.

INPUTS:

The single input for this task is the Open Standard which may have influenced the creation of organisational practice.

TASKS:

1. Identify all the activities and produced/consumed documents and other articles required by the standard
2. Identify the sequences of linked activities and articles
3. Represent graphically the lifecycle required by the standard as a sequence of linked activities and articles
4. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. A representation of the As-Required (Open) Model
2. The Report accompanying the As-Required Model.

STEP 3: Modelling Safety Practice As Required (Closed)

OBJECTIVE:

The second way in which safety practice ‘as-required’ is currently defined is by one generated by a specific organisation in its ‘Closed’ Standard. The lifecycle of processes expressed in organisational practice may, or may not have been influenced by / designed as a means to implement the prescribed lifecycle of a specific Open Standard.

The objective here therefore, is to model the set of lifecycle activities de-scribed by the organisational processes and procedures.

INPUTS:

The input for this task is the Closed Standard which constitutes organisational practice.

TASKS:

1. Identify all the activities and produced/consumed documents and other articles required by organisational practice
2. Identify the sequences of linked activities and articles
3. Represent graphically the lifecycle required by the standard as a sequence of linked activities and articles
4. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The appropriately represented As-Required (Closed) Model
2. The Report accompanying the As-Required (Closed) Model

STEP 4: Model Safety Practice As Observed

OBJECTIVE:

Safety practice 'as observed' represents the actual activities of those practitioners within an organisation. The objective is to model the software safety activities carried out by software safety practitioners in a given organisation.

INPUTS:

Instead of relying on a suite of documentary articles, safety engineering practice as-observed necessitates a form of independent ethnographic study. So the single input to this task is an empirical report of as-observed safety practice (carried out by either a safety engineer, or an engineer with responsibility for system safety).

TASKS:

1. Identify all the activities and produced/consumed documents and other articles carried out by the safety practitioner
2. Identify the sequence of activities carried out by the safety practitioner
3. Represent graphically the sequence of linked activities carried out and articles produced/consumed
4. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The appropriately represented As-Observed Model
2. The Report accompanying the As-Observed Model.

Having identified, modelled and represented the elements of safety practice, attention now turns to the process to assess safety practice.

STEP 5: Compare Organisational Practice with Safety Practice As-Desired

OBJECTIVE:

Organisational Practice must be capable demonstrably of complying with Safety Practice as-desired. The objective of this step is therefore to assess the levels of compliance between organisational practice and safety practice as-desired.

INPUTS:

Two modelling elements of the framework instantiation process must have already been completed:

1. The As-Required (Closed) Model of Safety Practice
2. The As-Desired Model of Safety Practice.

TASKS:

1. Create a copy of the model of As-Required (Closed) practice created at Step Three
2. Using this copy, create a representation of where as-required practice conforms with each the as-desired safety practice model or criteria in turn
3. Taking each model element or criteria in turn, evaluate each contributing activity:

   Internal Completeness and Consistency: are the activities correct and commensurate with achieving as-desired practice? Do the right amount of activities exist; and does each activity have the correct amount of supporting contributing activities to ensure it can be completed to the required level of compliance?

   Consideration of Attributes: is the information stated for the attributes the correct information (i.e. Inputs, Outputs, Time, Techniques and Methods, Controls, and Resources); and is the correct amount of information given for the attributes for the as-desired practice to be met?

4. For each model element / criteria, evaluate each article produced / consumed by an activity:

   Sufficiency: is there the correct number of articles to enable successful completion of all activities, and are the articles the correct ones? Does every activity produce an article; and does each activity have the correct amount and type of articles (as inputs) to comply with the model of as- desired practice?

   Consideration of Attributes: is the information stated for the attributes correct (i.e. Time, Quality Criteria and Existence) to denote when they need to be produced or used? Are the correct number and set of quality attributes considered for each article, for as-desired practice to be complied with?

5. Annotate the newly-created model indicating the degree of compliance with as-desired safety practice
6. Should potential deficiencies be evident, then follow-up research with the organisation should be undertaken to establish the reasons why
7. Compile a report which defines the:

a. Modelling process used
b. Modelling symbology used
c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The appropriately annotated Model of As-Required (Closed) Practice Compliance
2. The Report accompanying the Model of As-Required (Closed) Practice Compliance.

STEP 6: Compare the Open Standard with Safety Practice As-Desired

OBJECTIVE:

A published Open Standard must be capable demonstrably of complying with Safety Practice as-desired. The objective of this step is therefore to assess the levels of compliance between an Open Standard and safety practice as-desired.

INPUTS:

For this Step to proceed, two modelling elements of the framework instantiation process must have already been completed:

1. The As-Required (Open) Model of Safety Practice
2. The As-Desired Model of Safety Practice.

TASKS:

1. Create a copy of the model of As-Required (Open) practice created at Step Two
2. Using this copy create a representation of how as-required practice conforms with each as-desired safety practice model element / criteria in turn
3. Taking each model element / criteria in turn, evaluate each contributing activity:

   Internal Completeness and Consistency: are the activities correct and pertinent commensurate with achieving as-desired practice? Do the right amount of activities exist; and does each activity have the correct amount of supporting contributing activities to ensure it can be completed to the required level of compliance?

   Consideration of Attributes: is the information stated for the attributes the correct information (i.e. Inputs, Outputs, Time, Techniques and Methods, Controls, and Resources); and is the correct amount of information given for the attributes for the as-desired practice to be met?

4. For each model element / criteria, evaluate each article which is produced / consumed by an activity:

   Sufficiency: is there the correct number of articles to enable successful completion of all activities, and are the articles the correct ones? Does every activity produce an article; and does each activity have the correct amount and type of articles (as inputs) to comply with the model of as- desired practice?

   Consideration of Attributes: is the information stated for the attributes the correct information (i.e. Time, Quality Criteria and Existence) to denote when they need to be produced or used? Are the correct amount of quality attributes considered for each article, and are they the correct quality attributes for as-desired practice to be complied with?

5. Annotate the newly-created model with the degree of compliance with as-desired safety practice
6. Should potential deficiencies be evident, then follow-up research with the organisation should be undertaken to establish the reasons why
7. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The appropriately represented Model of As-Required (Open) Practice Compliance
2. The Report accompanying the Model of As-Required (Open) Practice Compliance.

STEP 7: Compare As Observed Practice with As Required (Closed) Practice

OBJECTIVE:

Safety Practice As-Observed may be different to, or the same as Safety Practice As-Required (Closed). The objective of this step is therefore to compare as-observed practice with the lifecycle of organisational practice.

INPUTS:

Two modelling elements of the framework instantiation process must have already been completed:

1. The As-Required (Closed) Model of Safety Practice
2. The As-Observed Model of Safety Practice.

TASKS:

1. Create a copy of the model of As-Observed Practice created at Step Four
2. Using the copy, compare the levels of agreement between safety practice as-observed, and safety practice as-required (closed)
3. Annotate the newly created model with the levels of agreement, and the differences between the two models of practice
4. Should differences be evident, then follow-up research with the organisation should be undertaken to establish the reasons why
5. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The annotated Model of how As-Observed Practice compares with As-Required (Closed) Practice

2. The Report accompanying the comparison of how As-Observed Practice compares with As-Required (Closed) Practice.

STEP 8: Compare As Required (Closed) Practice with As Required (Open) Practice

OBJECTIVE:

Safety Practice As-Required (Closed) may be different to, or the same as the Open Standard which may have informed its development (Safety Practice As-Required (Closed)). The objective of this step is therefore to compare both models of safety practice as-required.

INPUTS:

Two modelling elements of the framework instantiation process must have already been completed:

1. The As-Required (Closed) Model of Safety Practice
2. The As-Required (Open) Model of Safety Practice

TASKS:

1. Create a copy of the model of As-Required (Closed) Practice created at Step Three
2. Using the copy, compare the levels of agreement between safety practice as-required (Closed), and safety practice as-required (Open)
3. Annotate the copy with the levels of agreement, and the differences between the two models of as-required practice
4. Should differences be evident, then follow-up research with the organisation should be undertaken to establish the reasons why
5. Compile a report which defines the:
    a. Modelling process used
    b. Modelling symbology used
    c. Location of the model, and any proprietary software required to access it.

OUTPUTS:

Two Outputs are created by this Step:

1. The appropriately represented Model of how As-Required (Closed)Practice compares with As-Required (Open) Practice
2. The Report accompanying the comparison of the two models of As-Required Practice.

STEP 9: Compare As Observed Practice with As Desired Practice

Along with Step 10, this is a conditional step which may not necessarily have an output. The Task for Steps 9 and 10 is identical, only the rationale behind any identified differences will differ.

OBJECTIVE:

Having completed the model of as-observed safety practice, and completed the comparison with organisational practice, differences between the two models may have been identified. The objective here, therefore is to determine whether any differences in the as-observed model exist because those charged with implementing an organisation’s safety lifecycle are aware of deficiencies in organisational practice with regards to achieving as-desired practice. It aims to determine whether any differences which may exist are additional activities to those required by organisational processes, or whether activities are carried out in a manner other than those required by organisational processes.

INPUTS:

Two modelling elements of the framework instantiation process must have already been completed:

1. The Model of how As-Observed Practice compares with As-Required (Closed) Practice
2. The As-Desired Model of Safety Practice.

TASK:

1. Determine whether any differences exist in the Model of how As-Observed Practice compares As-Required (Closed) Practice
2. Conduct further enquiries with the participant(s) in the observation of safety practice to determine the reasons behind identified differences
3. Create a report that documents the reasons for identified differences
4. Carry out further investigations with the organisation whose processes are under analysis.

OUTPUTS:

The single output from this Step is a report outlining the differences between as-observed practice and as-observed (closed) practice - including the posited reasons for the differences.

STEP 10: Comparing As Observed Practice with As Required (Open) Practice

Along with Step 9, this is a conditional step which may not necessarily have an output. The Task for Steps 9 and 10 is identical, only the rationale behind any identified differences will differ.

OBJECTIVE:

Having completed the model of as-observed safety practice, and completed the comparison with as-required (Open) practice, differences between the two models may have been identified.

The objective here, therefore is to determine whether any differences in the as-observed model exist because those charged with implementing an organisation's safety lifecycle are aware of aspects of organisational practice which are not in full agreement with an Open Standard.

There are many potential reasons why a practitioner may carry out activities required of an Open Standard (which are not required by, or differ from their organisation's practice), perhaps even a standard other than the one which influenced organisational practice - and further data is required to establish whether this is a deviation from as-required (Closed) practice, and the reasons why.

INPUTS:

The Model of how As-Observed Practice compares with As-Required (Open) Practice must already have been completed.

TASKS:

1. Determine whether any differences exist in the model of how as-observed practice compares with as-required (open)
2. Conduct further enquiries with the participant(s) in the observation of safety practice to determine the reasons behind any identified differences
3. Create a report that documents the reasons for the identified differences
4. Carry out further investigations with the organisation whose processes are under analysis.

OUTPUTS:

The single output from this Step is a report outlining the differences between as-observed practice and as-observed (closed) practice - including the posited reasons for the differences.

Data Management

The empirical data produced by this process provides an organisation with valuable insights into the current state of their safety practice.

Some of the generated data may reveal the need for further, immediate recovery action, and some data may necessitate further research before any action is taken.

Some potential impediments and their potential next steps are considered in Table 1. The implementation of these next steps is outside the scope of this process.

Table 1: Potential Impediments and their Mitigation(s)

Identified Potential Impediment	**Next Steps**
Non-compliance between As-Required and As-Desired Practice	1. Clear deficiency (i.e. Lack of `activity x' requires the creation of `activity x') 2. Repeat Step 2/3 to ensure sufficiency 3. Repeat Step 5/6 to ensure deficiency has been cleared
Internal consistency deficiencies (insufficient information for activity to successfully conclude/for artefact to be produced)	1. Recover internal inconsistency 2. Repeat Step 2/3 to ensure deficiency is removed
Levels of disagreement between your organisation's process and the Open Standard which influenced its development (Not applicable if your organisation is a Standard's Committee)	1. Determine the reason for each disagreement considering the following: a. Is there evidence of safety clutter? b. Are the disagreements due to contractual/commercial complexities? c. Are the disagreements reasonable (i.e. is there an option asserted?)

Identified Potential Impediment	**Next Steps**
	2. Assess the impact of the disagreement in terms of whether this represents: a. An unsafe act b. A necessary deviation c. Surplus work activities 3. Identify potential mitigation options 4. Assess each mitigation option on the ability of the organisation to meet the as-desired criteria 5. Assess each mitigation option for whether an unintended consequence could manifest 6. Select mitigation and implement 7. Repeat Process Steps 8 and 5
Non-compliance between As-Observed and As-Required (Closed) Practice	1. Determine the reason for each non-compliance considering the following (not exhaustive): a. Whether the non-compliance is an intentional deviation in order to meet As-Desired practice (i.e. recovering a perceived shortfall in As-Required (Closed) Practice) b. Whether there is a lack of clarity in the As-Required (Closed) Practice (an ambiguity or interpretation issue) c. Whether the non-compliance has an impact on safety (i.e. whether the non-compliance predicated on removing clutter) 2. Identify potential mitigation options 3. Assess each mitigation option on the ability of the organisation to meet the as-desired criteria 4. Assess each mitigation option for whether an unintended consequence could manifest 5. Select mitigation and implement 6. Repeat Step 7
Activities emanating from As-Observed Practice which comply with As-Required (Open) Practice – but which are not mandated by As-Required (Closed) Practice	1. Determine the reason for each activity considering the following (not exhaustive): a. Whether the activity is an intentional act in order to meet As-Desired practice (i.e. recovering a perceived shortfall in As-Required (Closed) Practice) b. Whether the activity has a positive/negative impact on safety) 2. Identify potential mitigation options 3. Assess each mitigation option on the ability of the organisation to meet the as-desired criteria 4. Assess each mitigation option for whether an unintended consequence could manifest 5. Select mitigation and implement 6. Repeat Steps 4 (partial) and 10 (as applicable)
Activities emanating from As-Observed Practice which comply with As-Desired Practice – but which are not mandated by As-Required (Open and/or Closed) Practice	1. Determine the rationale for the additional activities of the as-observed practice 2. Determine whether other activities required by as-required practice comply with the same requirement(s) of as-desired practice (using different activities)

Identified Potential Impediment	Next Steps
	3. Assess the data from #1 and #2 and establish which of the activities would be the most prudent to adopt or cease. 4. Repeat Steps 2, 3, and/or 4 as appropriate