The UK Nuclear Industry Good Practice Guide To:

**Risk and Shortfalls Management**



This Nuclear Industry Good Practice Guide was produced by the Safety Case Forum and published on behalf of the Nuclear Industry Safety Directors’ Forum (SDF)

**Issue 1 – June 2020**

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Issue Number** | **Revision Date** | **Changes** |
| Issue 1 | June 2020 | Initial Publication |
|  |  |  |

It is recognised that – through the experience of using this Guide – there may be comments, questions and suggestions regarding its contents.

In the first instance, any such comments should be sent to all of the following:

safetycaseforum@awe.co.uk

Author: Dr John Malget (Radioactive Waste Management Ltd)

Contributions have been provided through the Safety Case Forum by
all participating members, particularly:

Jennie Costello (Atomic Weapons Establishment)

Gordon Turner (Radioactive Waste Management Ltd)

Carolyn Page (Sellafield Ltd)

This document was reviewed and approved by the Safety Case Forum
of the Safety Directors’ Forum.

# Foreword

The Safety Case Forum develops industry guides aimed at improving the approach, outcomes from and cost‑effective delivery of fit-for-purpose safety cases at all stages of a facility’s life cycle. This guide is focussed on resolution of issues associated with the approach to and management of shortfalls. It explores the root cause of current process failings and develops principles geared towards improving outcomes. The areas for improvement fall into four general themes:

* Organisational *engagement;*
* Management *commitment;*
* *Communication* of the process and outcomes;
* Decision making *authority.*

The full set of principles is listed below:

|  |  |
| --- | --- |
| **Theme** | **Principle** |
| *Engagement* | GP\_4 | *The Key Success Factors for the shortfalls (risk) management process should be defined and agreed with key stakeholders* |
| *Commitment* | GP\_5 | *The shortfalls (risk) management process should be a pro-active and integral part of business as usual* |
| GP\_6 | *The shortfalls (risk) management process should be integrated with, not separate from, safety case maintenance* |
| GP\_7 | *A shortfalls (risk) management process requires an approved baseline for comparison* |
| *Communication* | GP\_1 | *The organisation should ensure that the difference between risks and issues is understood* |
| GP\_2 | *The organisation should use language that helps not hinders understanding of the shortfalls (risk) management process* |
| GP\_3 | *The difference between what is required to be operational and what is required to permit operation should be understood* |
| GP\_9 | *The rationale for what needs to be done, and what does not should be self-evident from the arguments and evidence presented to stakeholders* |
| GP\_11 | *The methodology that is used should align well with the manner in which the Licensee or Authorisee will be assessed* |
| GP\_12 | *The method of communication that is selected should be appropriate to the size and complexity of the systems being managed; one size does not fit all*  |
| *Authority* | GP\_8 | *The sentencing of shortfalls (risks) should only be undertaken by competent and authorised individuals* |
| GP\_10 | *The sentencing of shortfalls (risks) against an approved baseline should follow clearly defined processes that implement well defined criteria.* |

In order to simplify understanding, and encourage adoption, the guide contains a number of worked examples. They explore a range of typical issues from misinterpretation of simple observations to rationalisation of more complex situations.

## Safety Directors’ Forum

In a sector where safety, security and the protection of the environment is, and must always be the number one priority, the Safety Directors’ Forum (SDF) plays a crucial role in bringing together senior level nuclear executives to:

* Promote learning;
* Agree strategy on key issues facing the industry;
* Provide a network within the industry (including with government and regulators) and external to the industry;
* Provide an industry input to new developments in the industry; and,
* To ensure that the industry stays on its path of continual improvement.

It also looks to identify key strategic challenges facing the industry in the fields of environment, health, safety, quality, safeguards and security (EHSQS&S) and resolve them, often through working with the UK regulators and government, both of whom SDF meets twice yearly. The SDF members represent every part of the fuel cycle from fuel manufacture, through generation to reprocessing and waste treatment, including research, design, new build, decommissioning and care and maintenance and waste disposal. The Forum also has members who represent the Ministry of Defence nuclear operations, as well as “smaller licensees” such as universities and pharmaceutical companies. With over 25 members from every site licence company in the UK, every MoD authorised site and organisations which are planning to become site licensees the SDF represents a vast pool of knowledge and experience, which has made it a key consultee for Government and regulators on new legislation and regulation.

The Forum has a strong focus on improvement across the industry. It has in place a number of subject-specific sub-groups looking in detail at issues such as radiological protection, human performance, learning from experience and the implementation of the new regulatory framework for security. Such sub-groups have developed a number of Codes of Practice which have been adopted by the industry.

## Sub-Group Description

This Guide has been produced by the Periodic Review Forum, a workstream of the Safety Case Forum, which is in turn a sub-group of the SDF.

The Safety Case Forum was established in June 2012 and brings together a wide range of representatives of nuclear operators, from all the Licensees and Authorisees across the UK, including:

* Civil, commercial and defence activities;
* Design, operation and decommissioning of nuclear facilities;
* Research facilities.

The purpose of the Safety Case Forum is to provide guidance that is useful to, and will benefit the widest possible range of UK nuclear operators.

Such guidance is not mandatory, nor does it seek to identify minimum standards. It aims to provide a tool kit of methods and processes that nuclear operators can use if appropriate to their sites and facilities.

These guides are intended to improve the standardisation of approach to the delivery of fit-for-purpose safety cases, while improving quality and reducing the cost of production. They are designed to cater for all stages of a facility’s life cycle and for all processes within that life cycle. This includes any interim, continuous and periodic safety reviews, allowing for the safe and efficient operation of nuclear facilities.

When using the information contained within these guides, the role of the Intelligent Customer shall always remain with the individual nuclear operator, which shall retain responsibility for justifying the arguments in their respective Safety Cases. The ONR and the defence Nuclear Safety Regulator are consultative members of the Safety Case Forum.

The following companies and organisations are participating members of the Safety Case Forum:

   

  

  

  

   

  

  

Safety Case Forum Guides are available on the Nuclear Institute Website:

<http://www.nuclearinst.com/SDF-safety-cases>

**Disclaimer**

This UK Nuclear Industry Guide has been prepared on behalf of the Safety Directors’ Forum by a Technical Working Group. Statements and technical information contained in this Guide are believed to be accurate at the time of writing. However, it may not be accurate, complete, up to date or applicable to the circumstances of any particular case. This Guide is not a standard, specification or regulation, nor a Code of Practice and should not be read as such. We shall not be liable for any direct, indirect, special, punitive or consequential damages or loss whether in statute, contract, negligence or otherwise, arising out of or in connection with the use of information within this UK Nuclear Industry Guide.

This guide is produced by the Nuclear Industry. It is not prescriptive but offers guidance and in some cases a toolbox of methods and techniques that can be used to demonstrate compliance with regulatory requirements and approaches.

**Contents**

[Foreword 3](#_Toc42778869)

[Safety Directors’ Forum 4](#_Toc42778870)

[Sub-Group Description 4](#_Toc42778871)

[1 Introduction 8](#_Toc42778872)

[2 Background 8](#_Toc42778873)

[3 Organisational Opportunities for Improvement 8](#_Toc42778874)

[3.1 Engagement 8](#_Toc42778875)

[3.2 Commitment 9](#_Toc42778876)

[3.3 Communication 9](#_Toc42778877)

[3.4 Authority 9](#_Toc42778878)

[4 Setting Up For Success 9](#_Toc42778879)

[5 Issues for Resolution & Opportunities 10](#_Toc42778880)

[5.1 General Principles 14](#_Toc42778881)

[5.2 The Process 17](#_Toc42778882)

[5.3 The Presentation 19](#_Toc42778883)

[6 Glossary and Definitions 21](#_Toc42778884)

[6.1 Table of Abbreviations 21](#_Toc42778885)

[6.2 Summary of Concepts and Logic 22](#_Toc42778886)

[Appendices 23](#_Toc42778887)

[Appendix A: ONR Inspection Framework (See ONR-INSP-GD-064 Revision 3) 24](#_Toc42778888)

[Appendix B1: Worked Example 1 and Explanation 25](#_Toc42778889)

[Appendix B2: Worked Example 2 26](#_Toc42778890)

[Appendix B3: Worked Example 3 27](#_Toc42778891)

[Appendix B4: Worked Example 4 (Consolidation) 28](#_Toc42778892)

[Appendix C: (Resolution Strategy Compliance Matrix) 29](#_Toc42778893)

[7 References 30](#_Toc42778894)

**Figures**

[Figure 1: The importance of shared understanding 11](#_Toc42778778)

[Figure 2: Key Pillars Supporting Delivery of Successful Outcomes from Shortfalls Management 13](#_Toc42778779)

[Figure 3: Shortfalls Activities Presented as a Risk Management Process 15](#_Toc42778780)

[Figure 4: Mapping Risks to Priority for Action 18](#_Toc42778781)

[Figure 5: Summary of Logic from ONR Enforcement Guidance 18](#_Toc42778782)

[Figure 6: Identification, Classification and Sentencing of Shortfalls 19](#_Toc42778783)

# Introduction

The Safety Case Forum, a sub-group of the Safety Directors Forum convened a working group to address issues associated with the ‘Shortfalls Management’ process, the backbone of the Periodic Review of Safety (PRS). This was in response to regulatory feedback to UK SLCs that PRS is not having the desired outcome. It is currently viewed as a reactive and therefore lagging process not a proactive and continuous demonstration of safety. This guide seeks to address these issues by synthesising relevant good practice (RGP) from across the UK Site Licensees and Authorisees, international standards for risk management (i.e. ISO 31000:2018) and where applicable learning from other high hazard industries. It should be noted that consideration of the Shortfalls Management process in isolation will not ensure a successful Periodic Review of Safety.

# Background

The strategic objective of the shortfall’s management process is to identify, assess and develop plans to address risks that could undermine a Licensee’s or Authorisee’s ability to justify continued use or operation of a plant, facility or site. It is important in the context of risk management that ‘address’ does not necessarily mean ‘remove’; risks can either be treated or tolerated subject to appropriate justification. For instance, maintaining an ISO quality certification may be a prerequisite to allow nuclear manufacturing operations. The activities required to achieve this align to general requirements from the international standard (ISO) for risk management ISO 31000:2018. The ISO standard does not differentiate between types of risk and as such is applicable whether the issues of concern relate to legal requirements, management systems, procedures or engineered systems. It provides a clear and understandable framework around which to frame the issues to be addressed and act as an aid to improve the shortfalls management process.

# Organisational Opportunities for Improvement

Organisational factors contributing to poor outcomes from shortfalls management processes were collated through consultation with the contributing members of the Safety Directors’ Forum (SDF) Safety Case Forum (SCF) sub‑group[[1]](#footnote-2). That is not to say that all issues affect all organisations or that the list is exhaustive, rather these appear to be recurrent problems and therefore are considered to present significant opportunities for improvement, they were:

* Organisational *engagement;*
* Management *commitment;*
* *Communication* of the process and outcomes;
* Decision making *authority.*

Each will be discussed in turn presenting desirable organisational attributes, which if present would be expected to result in generally improved outcomes.

## Engagement

An organisation with a robust safety culture and commitment to pro-active risk management will recognise the role the ‘shortfalls’ process plays in supporting the basis for ongoing operations. A mature organisation with stable management structures, depth of capability and root and branch commitment will typically:

* Appoint a project sponsor with authority to effect change and secure resources;
* Treat ‘shortfalls’ management as a business-critical project;
* Trust appointed subject matter experts and empower them to make decisions (i.e. macro not micro‑management);
* Develop, train-out and maintain a company-wide process;
* Be proactive in ensuring involvement of all key stakeholders;
* Adopt structures and processes that foster collaboration.

## Commitment

Senior management plays a key role in both setting expectations and securing the necessary resources to ensure a successful outcome. A mature organisation with the support of its senior management team will typically:

* Understand the resource commitment required to ensure success;
* Allow sufficient time to complete the activity to the required quality;
* Will challenge when insufficient resources are provided;
* Will demand collaboration and constructive interaction.

## Communication

All successful projects develop and operate a stakeholder management and communication plan. One of the key elements of the shortfall’s management process is timely, clear and unambiguous communication with stakeholders at many levels within and outside the organisation. The use of ‘safety case speak’ will be an obstacle to understanding, engagement and support for change. A mature organisation with a clear communication and stakeholder engagement plan will typically:

* Ensure communication is factual;
* Use plain English where possible;
* Present a balanced and considered view;
* Tailor communication to the audience.

## Authority

The ‘shortfalls’ process will involve a wide range of people from a variety of technical and non-technical disciplines. It should be designed to ensure that there is clear differentiation between decision making, accountability for delivery and responsibility for doing work. This may differ from business as usual roles and responsibilities. Ensuring this is understood up front will ensure the whole organisation understands:

* Who has final authority on decisions made during the process?
* If there is an escalation route, what that is and who owns it?
* Who is ultimately responsible for approval of risk management plans?
* The context and basis for decisions at various stages of the process.

# Setting Up For Success

Understanding and defining success criteria for the process itself is critical. A review of both unsuccessful and comparatively successful shortfalls processes was undertaken in order to establish what would represent a set of desirable process attributes. As with the organisational aspects this was reduced to the most significant and recurring themes. The high-level attributes of a successful shortfall’s management process are defined below:

* ***Concise*** – should communicate the facts, and only the facts, and meet *all* stakeholder needs;
* ***Logical*** – process and outputs should be self-evidently related;
* ***Evidential*** - ‘golden thread’ is transparent, related to the identified shortfall and is supported by facts, not speculation, that support the justification for the action to be taken;
* ***Accessible*** – all communication should be in a form that meets the end-user needs;
* ***Relevant*** – shortfalls identified for action should be focussed on the here and now and be associated with *real* risks.

An acronym can be derived from these principles to convey in simple terms what a well-designed and operated process should be; it should be CLEAR in its objectives, the process to be followed, the manner in which it is communicated and the quality of the expected outcome. This aligns with the definition of a ‘quality’ process (Ref. 1) which is stated as:

*“The purpose of the Information Management Process is to generate, obtain, confirm, transform, retain, retrieve and dispose of information, to designated stakeholders.*

*Information management plans, executes, and controls provision of information to designated stakeholders that is unambiguous, complete, verifiable, consistent, modifiable, traceable, and presentable.”* (Ref. 1).

# Issues for Resolution & Opportunities

*Understanding the Difference*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication: GP\_1** |
| *The organisation should ensure that the difference between risks and issues is understood* |

The scope of what should be considered is well defined by the Office for Nuclear Regulation (ONR) (Ref. 1) but what constitutes a ‘shortfall’ is not unambiguously defined or universally agreed per se:

*“The PSR should identify any* ***shortfalls*** *against modern standards and good practices, with a programme to implement all reasonably practicable improvements in the facility and its operations, including to the documented safety case, to ensure that risks to the public and workers will be ALARP.*

This is a ‘risk’, whereas:

*“Where the PSR identifies an* ***issue*** *that significantly compromises the safety of the facility, the licensee should take immediate action to ensure that its operations remain in compliance with an adequate safety case (LC23(1) and LC23(3)).”*

This is inferring that the risk has been realised; an issue. Both statements could be taken literally as inferring a shortfall (delta) by comparison to something in the context of Periodic Review of Safety. In this example, the shortfall is not an inadequate safety case but an observation that leads to a conclusion that the safety case claims cannot be supported with the evidence that is currently available; operations may need to be suspended so that harm cannot occur because the risk is too high, such that it could.

*Talking the Same Language*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication: GP\_2** |
| *The organisation should use language that helps not hinders understanding of the shortfalls (risk) management process* |

Receiving, analysing and interpreting information correctly is one of the key (process) success factors (Ref. 1). For these reasons, it is recommended that *all* key terms are:

* Simply, but well, defined;
* Consistently used throughout the management system; and
* Invariant to ensure shared understanding.

Learning from experience (LfE) exercises, conducted during the development of this guide, established this issue as one of the major stumbling blocks. For instance, there was no agreement as to what constitutes a gap, issue, risk, and nature of the relationship between them (See Figure 1). All of these words are to some extent synonymous in common (i.e. non-specialised) usage.



Figure 1: The importance of shared understanding

Such issues can be addressed through a simple, well defined syntax and use of plain English[[2]](#footnote-3). This approach is deliberately applied in the fields of systems engineering (SE) and risk management to limit ambiguity. Using terms from these specialisms could both simplify what needs to be defined and how it is defined. It is not appropriate for this guide to prescribe what constitutes ‘correct’ terminology as each Licensee or Authorisee will have its own corporate language which will be used widely within its management system. Examples of how this might be applied are given below:

* A user requirement is;
	+ What is expected, the top-level statement of ‘good’.
* A functional requirement is;
	+ What a system needs to do to be operational.
* A non-functional requirement is;
	+ What a system needs to do to be compliant.
* A defect is;
	+ A system that is non-operational or non-compliant in some sense (applies equally to information, physical and organisational systems).
* An observation is;
	+ Something that requires interpretation.
* A root cause is;
	+ The origin of the defect.
* A risk is;
	+ Something that may occur if action is not taken.
* An issue is;
	+ Something that has occurred or is extremely likely to occur if no action is taken.

Whether or how this is adopted will depend on the organisational context, business priorities and range of stakeholders that may be involved. Without such rigour it is likely that the application of the processes to support the activity will continue to be more challenging, complicated, costly and time consuming than would otherwise be the case.

*What is Being Assessed?*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication:GP\_3** |
| *The difference between what is required to be operational and what is required to permit operation should be understood* |

The full ‘system of systems’ for any enterprise (Ref. 3) has a common set of components regardless of the nature of the undertaking. These may be described in simple terms as:

* Management systems (all quality and compliance processes);
* Physical systems (assets taken to include the safety case itself);
* Operational capability (people).

This interpretation is entirely consistent with the ONR guidance to Licensees and Authorisees on the general focus of a periodic review (Ref. 2) which is stated as:

“*The review should be wide ranging, ‘open minded’ and challenging. It must not be simply an assertion of safety. The review needs to encompass organisational and management system (people and process) aspects as well as the technical aspects of the facility. This includes so called ‘softer issues’ such as leadership and culture which can have a profound effect on safety, as evidenced in the lessons from major events in the nuclear and other sectors.”*

The adoption of systems thinking and a requirements informed approach as the cornerstone for identifying ‘shortfalls’ would greatly simplify communication with both internal and external stakeholders; there is tacit agreement of what good is and what constitutes failure (of a system) before it is observed in practice.



Figure 2: Key Pillars Supporting Delivery of Successful Outcomes from Shortfalls Management

The manner in which the requirements should be written is a matter for each licensee; there are no prescribed rules. There is extensive guidance on this topic published by expert bodies such as INCOSE (Ref. 1). In the context of the Licence Conditions a compliance assessment matrix (Ref. 1) would then include:

* What the requirement is;
* Who is responsible for compliance;
* What arrangements should be in place;
* How to assess the current state (i.e. pass/fail criteria).

Assuming that all enterprise-level requirements were clearly and unambiguously defined and are under active management, any observation interpreted as a ‘shortfall’ should logically lead to a decision that one of these systems (a barrier to an ‘unsafe/unacceptable’ state of some description) is:

* Ineffective (cannot function as required);
* Defective (will not function as required);
* Absent (the function is not present).

Such terminology is fully consistent with that used by the ONR in guidance issued to inspectors for enforcement (Ref. 1). The shortfalls management process should be designed to ensure that it clearly identifies:

* Which requirement (placed on a system) is not being fulfilled;
* Why this is the case (i.e. root cause not initial observation);
* How serious this is (which will be defined by the requirement itself);
* Timescales for resolution (i.e. now, later, never).

It should be self-evident that the issues of relevance and the associated importance will change through the lifecycle; ageing, degradation and maintenance issues ramping up would be unexpected when a facility first enters service. Similarly, issues related to drift in operational effectiveness may be of more concern over longer timescales inferring a loss of corporate knowledge or lack of understanding (or management) of the cumulative effects of modifications to the organisational baseline. The outcome of the assessment could be expressed in terms of a simple RAG[[3]](#footnote-4) analysis. This is the basis of the approach adopted by ONR when determining the appropriate enforcement action (Ref. 1). For mature operating sites, with established arrangements and processes embedded as ‘custom and practice’, a clear case for root and branch change may need to be made. The benefits of implementing such a change should consider the benefits that can be realised; there would be little to be gained from implementing such an approach at a well-managed low hazard facility at the end of its operational life, or where the decommissioning phase would be complete prior to the next periodic review cycle.

## General Principles

*Planning for Success*

|  |  |
| --- | --- |
| ***General Principle:*** | **Engagement: GP\_4** |
| *The Key Success Factors for the shortfalls (risk) management process should be defined and agreed with key stakeholders* |

The objectives and related key success factors (KSF), should guide the development of the process used to deliver the periodic review of safety (risk management process). This should be self-evident, but without top to bottom integration the expected outcomes and benefits will not be delivered. Equally, the application (use) of the process will provide opportunities to identify areas for its improvement. The organisation-level Critical Success Factor for the required outcome may be expressed in terms of a ‘Mission Statement’:

* Ensure the organisation can demonstrate to all relevant *stakeholders* that it has *adequate arrangements in place* to permit *continued operation*.

In order to achieve this, KSFs (for the process) should be defined. KSFs are generally accepted (Ref. 1) as being one of:

* Plan;
* Process;
* People;
* Power;
* Contingency.

Particular aspects of relevance to improving outcomes from the shortfall’s management process, and discussed in this guide, are:

| ***What*** | ***How*** | ***Why*** |
| --- | --- | --- |
| Plan | How it will be done | Failure to define reduces predictability of timely outcomes (Right on time) |
| Process | What will be done | Failure to define reduces predictability of compliant outcomes (Right first time) |
| People | Who will do what | Failure to define increases risk of non-compliant outcomes (Right by right person) |
| Power | Who can or cannot do what | Failure to define increases risk of non-compliant outcomes (Right decision maker) |
| Contingency | What else may need to be done | Failure to define introduces unplanned risk management strategies (Right reaction) |

The management systems supporting these activities and the processes developed to deliver them should not be static; they should be reviewed, at least, on the same frequency as the process itself is undertaken. Acting on this LfE will ensure that the process remains fit for purpose and ‘alive’ within the organisation.

*Defining the Management Process*

|  |  |
| --- | --- |
| ***General Principle:*** | **Commitment:GP\_5** |
| *The shortfalls (risk) management process should be a pro-active and integral part of business as usual* |

The general process should be consistent with the philosophy of a well-defined, organised and coherent approach to risk management (See Figure 3). Each process step should be supported by formalised procedures with clear decision-making frameworks.



Figure 3: Shortfalls Activities Presented as a Risk Management Process

*From Observation to Action*

|  |  |
| --- | --- |
| ***General Principle:*** | **Commitment:GP\_6** |
| *The shortfalls (risk) management process should be integrated with, not separate from, safety case maintenance* |

Whilst all Licensees and Authorisees have approved arrangements and continue to improve their approach to delivery of Periodic Review of Safety (LC15) the ONR have suggested, through their participation in the industry forum, that their requirements are not yet being met in full. It is also fairly common that the process overruns into the next review cycle. The root cause of the problem is in part that most Licensees and Authorisees view periodic review and ‘shortfalls’ management as a reactive, not continuous, assurance process. It is one of the tools to be used by the licensee to satisfy themselves that all obligations to their employees, the public and other stakeholders are being, and will continue to be, met. These issues are compounded by the current ‘document-centric’ management of requirements and slow adoption of a ‘live safety case’ philosophy.

*The Shifting Sands Problem*

|  |  |
| --- | --- |
| ***General Principle:*** | **Commitment: GP\_7** |
| *A shortfalls (risk) management process requires an approved baseline for comparison* |

As previously discussed in a different context, one of the concerns raised by the ONR, via their participation in the SDF SCF, relates to the ability of Licensees or Authorisees to correctly identify ‘shortfalls’ and then address them in required timescales. The planning and resourcing issue that this may infer is not in the scope of this guide and would be resolved through robust application of project, programme and portfolio management (P3M) processes[[4]](#footnote-5). In order to identify a shortfall, a static baseline is assumed to exist against which the comparison can be made. If the organisation, its facilities, procedures and safety cases are in a constant state of flux, delivery of the shortfalls process will be challenging. In order to address this issue an operational baseline needs to be set and frozen. This ensures that a meaningful comparison can be made but does not preclude improvements being made in parallel; all that is required is to record the resolution plan, regardless of whether or not it has been or is in the process of being implemented.

*Decisions Made by Decision Makers*

|  |  |
| --- | --- |
| ***General Principle:*** | **Authority:GP\_8** |
| *The sentencing of shortfalls (risks) should only be undertaken by competent and authorised individuals* |

Any decision-making activity requires in-depth domain knowledge to ensure that correct and robust decisions are made and this in turn defines the competences that will be required. Whilst other stakeholders may be consulted or informed, they should not unduly influence the decision-making process if they are neither qualified to make such judgments, nor accountable for managing the risk. The onward management and decision-making process should record the rationale at each stage and the final outcome including who was:

* **R**esponsible for estimating the risk and defining the mitigation strategy;
* **A**ccountable for approving the mitigation plan (if any);
* **C**onsulted to validate assumptions (if required);
* **I**nformed during the process.

*The Golden Thread*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication: GP\_9** |
| *The rationale for what needs to be done, and what does not should be self-evident from the arguments and evidence presented to stakeholders* |

The ONR has provided clear guidance on the arguments that would be expected in support of a decision not to implement an improvement plan (Ref. 2).

*“Reasonable practicability arguments for not implementing improvements should follow ONR’s ALARP guidance. For PSRs, these might include:*

*i) that the benefit would only be applicable during normal operation; the time to implement would extend beyond final shutdown; and the shutdown date has been guaranteed, e.g. in a letter to ONR (without such a guarantee a period of at least a further ten years of normal operation should be assumed in the ALARP argument);*

*ii) that it is physically impossible or impracticable to modify the facility so as to achieve compliance with modern standards; or*

*iii) that the sacrifice from bringing the facility up to modern standards (e.g. in terms of time, trouble or cost) would be grossly disproportionate to the safety benefit gained”.*

These considerations are directly linked to the risk ascribed to taking no action and the stakeholder that would be affected. The ONR has a framework it uses to determine the importance of findings from the Periodic Review of Safety process. Whilst this is guidance to inspectors, not Licensees or Authorisees, it provides a clear indication of the general process and decision-making logic that should be applied (Ref. 5).

## The Process

*Plan for success*

|  |  |
| --- | --- |
| ***General Principle:*** | **Authority:GP\_10** |
| *The sentencing of shortfalls (risks) against an approved baseline should follow clearly defined processes that implement well defined criteria.* |

This guide does not prescribe what the criteria should be or how these decisions should be made, rather that they should be developed and applied. The general logic of review and rationalisation should be familiar to engineers and safety case practitioners alike, as the application of a risk matrix (e.g. a DBAA scheme). This ensures that the important ‘needle’ does not get lost in a ‘haystack of needles’.



Figure 4: Mapping Risks to Priority for Action

*Understand stakeholder expectations*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication:GP\_11** |
| *The methodology that is used should align well with the manner in which the Licensee or Authorisee will be assessed* |

The ONR has set out in very clear terms its expectations for the framework, the process and what it defines as a shortfall for the purposes of enforcement (See Appendix A, extract from Ref. 5). The general process and decision points are summarised below:



Figure 5: Summary of Logic from ONR Enforcement Guidance

Whilst the ONR uses the framework of the licence conditions to make its assessment, it encompasses all relevant regulatory requirements:

“*Whilst intervention priorities are guided by the ONR Strategic Plan, inspectors have discretion in deciding the priorities for regulatory action within ONR due process. ONR inspectors inspect compliance with the;*

* *security regime against the Approved Site Security Plan, Temporary Security Plans, Transport Security Statements, Transport Security Plans and other associated regulatory compliance documents.*
* *health and safety regime against the licence conditions, health and safety legislation including HSWA, fire safety legislation, the civil carriage of radioactive materials by road and rail.”*

Within the guidance to ONR inspectors, four risk levels (terms) are stated:

* Extreme;
* Substantial;
* Moderate;
* Nominal.

This framework is developed further to define what constitutes:

* Absent;
* Inadequate;
* Minor.

This aligns with the general approach and terminology that is recommended in this guide. For example, Appendix 2 of (Ref. 6) provides a clear indication of what leads to a conclusion that there is a compliance shortfall from a regulatory perspective against each licence condition. The type and number of the observations should also be considered when assessing the importance and risk associated with the shortfall. It is also important to recognise that without a root-cause analysis any action designed to address the shortfall may ultimately be ineffective; it will only address the symptom and not the cause. Any process that is implemented (See Figure 6) should be capable of delivering an outcome that would align with regulatory assessment of the same information. The combined logic and generic framework for deciding on what action should be taken based on the risks that are identified is presented below:



Figure 6: Identification, Classification and Sentencing of Shortfalls

## The Presentation

*What Does Better Look Like?*

|  |  |
| --- | --- |
| ***General Principle:*** | **Communication:GP\_12** |
| *The method of communication that is selected should be appropriate to the size and complexity of the systems being managed; one size does not fit all*  |

There is no right or wrong way to present the outcome from the shortfalls process. The overarching objective is to ensure that what has been found is correct, the risk that has been identified is well defined and the planned action will deliver the required outcome. The logic of the argument rests on the ‘golden thread’ within the information. As such the end-to-end configuration control, from the initial observation to the requirement to take action, is of fundamental importance.

However it is presented, it should be clear at the end of the process to all stakeholders that a proposed shortfall is only an actual shortfall if:

There is an <*unacceptable level of risk*> of <*an unwanted state of some kind*> due to <*demonstration of, and agreement on, the inadequacy of some aspect of the safety management arrangements*>

In order to simplify understanding and encourage adoption the guide contains worked examples based on hypothetical observations. When testing, and prior to applying this process, it is essential that problems ranging from misinterpretation of simple observations to rationalisation of more complex situations are explored. This will ensure that both an expected and consistent outcome is achieved. (See Appendices B1 ‑ B4).

# Glossary and Definitions

## Table of Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Definition** |
| ALARP | as low as reasonably practicable |
| CAE | claims, arguments, evidence |
| DBAA | design basis accident analysis |
| HSWA | Health and Safety at Work Act 1974 |
| INCOSE | International Council on Systems Engineering |
| ISO | International Organization for Standardization |
| KSF | Key Success Factors |
| LfE | learning from experience |
| ONR | Office for Nuclear Regulation |
| P3M | Project, Programme and Portfolio Management |
| PRS | Periodic Review of Safety (PRoS and PSR currently in usage with same meaning across UK SLCs and Authorisees) |
| RACI | Responsible, Accountable, Consulted, and Informed |
| RGP | relevant good practice |
| SCF | Safety Case Forum |
| SDF | Safety Directors’ Forum |
| SE | Systems Engineering |
| SLC | Site Licence Company |

## Summary of Concepts and Logic

|  |  |
| --- | --- |
| **Term** | **Definition** |
| System | A group of interacting or interrelated entities that form a unified whole. |
| System of Systems | A collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system. |
| User Requirement | What is expected, the top-level statement of ’good’. |
| Functional Requirement | What a system needs to do to be operational. |
| Non-functional Requirement | What a system needs to do to be compliant. |
| Defect | A system that is non-operational or non-compliant in some sense (applies equally to information, physical and organisational systems). |
| Observation | Something that requires interpretation. |
| Root Cause | Is the origin of the defect. |
| Risk | Something that may occur if action is not taken. |
| Issue | Something that has occurred or is extremely likely to occur if no action is taken. |

# Appendices

This guide has been written to highlight those areas, which if addressed are most likely to improve outcomes from the shortfalls process. The Appendices in this document contain additional information for UK Licensees and Authorisees to assist in understanding and implementation.

## Appendix A: ONR Inspection Framework (See ONR-INSP-GD-064 Revision 3)



## Appendix B1: Worked Example 1 and Explanation



## Appendix B2: Worked Example 2



## Appendix B3: Worked Example 3



## Appendix B4: Worked Example 4 (Consolidation)



## Appendix C: (Resolution Strategy Compliance Matrix)

| **Topics for Consideration in the Work package** | **Addressed in Guide** |
| --- | --- |
| **i. Process definition** | a. Agree the key steps, expected outcomes, and format of the output | Section 5.1 | General principles developed and explanatory text provided. |
| b. Define “gap”, “importance”, “actions” in general terms | Section 5 | General principles developed and explanatory text provided. |
| c. Define responsibilities, “who”, “what”, “why”, “when” | Section 5.1 | General principles developed and explanatory text provided. |
| d. Clarity on decision making “what needs to be done” and “why”  | Section 5.1 | Various general principles developed and explanatory text provided. |
| **ii. Language and terminology** | a. A well-defined and agreed glossary or an “agree to differ” mapping of terms (similar to approach to DBA if there is no agreement initially) | Section 5 | General principles developed and explanatory text provided. |
| **iii. Process efficiency** | a. Look outside the industry for best practice  | Section 5 | General principles developed and explanatory text provided. |
| **iv. Managing expectations** | a. Clarify what can be done, timetable for improvement and what is required to do this | Section 5.1 | General principles developed and explanatory text provided. |
| Section 5.3 | General principles developed and explanatory text provided. |
| **v. Communication**  | a. What does a successful PRS look like and how do we get buy in | Section 5.1 | General principles developed and explanatory text provided. |
| **vi. Challenges** | a. Identify what internal and external factors are contributing to failure | Section 3 | General principles developed and explanatory text provided. |
| b. Framework to make recommendations to resolve the issues  | Section 3 | Various general principles developed and explanatory text provided. |
| **vii. When and what is enough?** | a. Maintaining focus on key issues (requirements/CAE etc) | Section 5.1 | General principles developed and explanatory text provided. |

# References

|  |  |
| --- | --- |
| Ref. No: | **Title** |
| 1.
 | International Organisation for Standardisation, Systems and Software Engineering - System Lifecycle Processes ISO/IEC/IEEE 15288:2015. |
| 1.
 | Office for Nuclear Regulation, Periodic Safety Reviews, NS-TAST-GD-050 Revision 7. |
| 1.
 | See <https://www.incose.org> and INCOSE approved Systems Engineering Book of Knowledge (SEBoK), <https://www.sebokwiki.org/wiki/ISO/IEC/IEEE_15288>. |
| 1.
 | See example from published Horizon Licence Application:https://www.horizonnuclearpower.com/files/downloads/3\_4\_Nuclear%20Site%20Licence%20Application%20Compliance%20Matrix.pdf |
| 1.
 | Office for Nuclear Regulation, Enforcement, ONR-ENF-GD-006, Revision 2 |
| 1.
 | Office for Nuclear Regulation, Inspection Rating Guide, ONR-INSP-GD-064 Revision 3 (Table included as Appendix) |
|  | Mesly, Olivier (2017). Project feasibility – Tools for uncovering points of vulnerability. New York, NY: Taylor and Francis, CRC Press, ISBN 9 781498 757911 |

1. Safety Directors’ Forum Safety Case sub-group, Work Stream A, Shortfalls Management Working Group [↑](#footnote-ref-2)
2. See <http://www.plainenglish.co.uk/files/howto.pdf> [↑](#footnote-ref-3)
3. Red, Amber, Green [↑](#footnote-ref-4)
4. See <https://www.apm.org.uk/media/13832/guide-to-se-and-p3m-processes.pdf> for further background reading [↑](#footnote-ref-5)