12 PROCESS SAFETY ASPECTS OF SAFETY REPORT ASSESSMENT

1.	**Introduction**
2.	**The General Approach to Process Safety Assessment**
3.	**Benchmarks**
4.	**Proportionality**
5.	**Pre-Construction and Pre-Operation Safety Reports**
6.	**Potential Serious Deficiency and Significant Omission**
Appendix 12C 'Process Safety Assessment Criteria and Guidance'	

1. INTRODUCTION

1.1 This guidance is for assessors completing the process safety assessment and is relevant to all types of safety report.

1.2 All process safety assessment must use the criteria and guidance set out in Appendix: 12E *'Process Safety Assessment Criteria and Guidance'*.

1.3 Process safety assessment must be recorded on the form SRAM 19 *'Process Safety Assessment Record'*.

1.4 The criteria are designed to follow in sequence the specific requirements set down in Schedule 3 of the 2015 COMAH regulations and to reflect relevant purposes set out in Regulation 8 of the same regulations. These are minimum legal requirements and are clear and enforceable (Regulation 9).

1.5 Demonstrations should be proportionate to the hazard and risks of identified major accident hazards. This aspect can only be decided by an operator when all the elements of Schedule 3 have been determined. The determination of proportionality is an iterative process both for an operator and an assessor.

1.6 Use of Assessment Criteria

The criteria will be applied by a competent assessor against the content of the safety report. In this context, a competent assessor will have a good understanding of the safety report assessment process, its place within the HID Regulatory Model and of any stated benchmarks.

a. Criteria will be **"met"** when all relevant items are included in descriptions and the necessary supporting information has been provided;

b. Criteria will be **"not met"** when all relevant items are not included in descriptions or the necessary supporting information has not been provided;

c. Criteria will be **"not relevant"** when they are not relevant to the establishment (e.g. functional safety criteria are unlikely to be relevant to a warehouse);

d. Criteria will be **"previously met"** when the previous assessor recorded the criterion as "met".

2. THE GENERAL APPROACH TO PROCESS SAFETY ASSESSMENT

2.1 The process safety assessor is looking for a demonstration that adequate safety and reliability have been taken into account in the design, construction, operation and maintenance of any installation, storage facility, equipment and infrastructure connected with the establishment's operation, which are linked to major accident hazards inside the establishment.

2.2 Use of Examples in the Safety Report

Where relevant, site records should be used as examples to validate descriptions or where demonstration is required by Regulation 8, primarily relating to design, construction, operation and maintenance.

The assessment criteria guidance lists a number of supporting records, e.g. on hazardous area classification, which should be provided by the operator where it is relevant to do so.

3. BENCHMARKS

3.1 Process Safety standards, codes of practice and guidance tend to be industry, process or substance specific. They do not relate directly to the criteria detailed in this document. Therefore benchmarks are not identified against each criterion.

3.2 However, DSEAR is a key piece of legislation for major hazard establishments and there are very few COMAH establishments where DSEAR does not have relevance. Where relevant, Process Safety Assessors should use DSEAR and the supporting ACOP and guidance as a benchmark for all the process safety technical assessment criteria.

It should be noted that DSEAR may not be addressed directly in safety reports, often being considered as part of the overall hazard/risk assessment.

3.3 In addition, a list of standards, codes of practice and guidance commonly accepted by industry and HSE is given in the Appendix 12E. These documents should be used as benchmarks, where appropriate, but this list is not comprehensive and the content is subject to change as documents are revised or updated. Where other publications are more relevant, their use should be clearly recorded by the assessor. Where appropriate, other equally effective measures may be used. Often there will be no relevant benchmark standards and first principles need to be applied.

3.4 Where benchmark standards exist, a COMAH operator is required to consider whether there are any further measures that can be applied and determine which ones are reasonably practicable to implement.

4. PROPORTIONALITY

4.1 Simple establishments may apply established process safety benchmark standards, but they should still demonstrate that they have considered if there are any major accident hazards that require measures beyond those standards and determine if those measures are reasonably practicable. See www.hse.gov.uk/risk/theory/alarp1.htm#P130_16948

5. PRE-CONSTRUCTION AND PRE-OPERATION SAFETY REPORTS

5.1 All engineering projects follow a common process of design, construction, commissioning and operation. These activities comprise sub-tasks and are spread over a schedule that can be subject to significant change, therefore the contents of pre-construction and pre-operation safety reports develop over time. It is, therefore difficult to select a defined point in time when a pre-construction or pre-operation safety report can be issued.

5.2 For the purposes of process safety assessment, a rolling submission is more practical than complete submissions, however, either option is acceptable.

5.3 Pre-Construction Safety Reports
Assessment will be based on the assessment criteria relating to activities up to and including design.

5.4 Pre-Operation Safety Reports
Assessment will be based on the assessment criteria relating to activities up to and including construction.

Pre-Operation safety reports should include details of significant changes to the previously specified design and relevant additional information resulting from the detailed engineering phase.

5.5 For large projects (involving external design / construction contractors) the operator should describe their arrangements for managing the resolution of outstanding issues / actions ('snag items') that are identified prior to the project being formally handed over to the establishment's operations team.

6 POTENTIAL SERIOUS DEFICIENCY AND SIGNIFICANT OMISSION

6.1 Examples of potential serious deficiencies in the on-site measures (as described in the safety report) include but are not limited to:

(i) Hazard study documentation indicates that there is an unacceptable risk associated with a particular hazard but the company have not identified any additional measures that would be required to make the risks tolerable;

(ii) Absence of a technical measure that would be regarded as good practice, such as bunding or adequate pressure relief, and without any suitable alternative

6.2 Significant omissions in the content of the safety report may include:

(i) Insufficient information to support the necessary demonstrations, for example, inadequate description of chemical reaction hazard assessment methodology or management of change procedures.

Appendix 12C 'Process Safety Assessment Criteria and Guidance'

TECHNICAL CRITERION	GUIDANCE
Link with Predictive Criteria	
12.1 The safety report should show a clear link between the measures taken and the major accident hazards described. **Regulation 8(b)** **Schedule 3 Para 4(a)**	This is the core of the Safety Report from the technical point of view and provides the link between identification and analysis of hazards and the selection of measures. This criterion can be regarded as a conclusion and the assessor should consider the other criteria first. **To meet this criterion the Safety Report should:** • Identify the hazards and the major accident scenarios; • Describe the control measures and demonstrate clear links to the major accident scenarios; • Explain the decision criteria for selecting the necessary measures to ensure risks are tolerable and ALARP i.e. there are no further reasonably practicable measures the operator could take. • Demonstrate adequate diversity and redundancy in the control measures (appropriate to the risk).
General Principles	

12.2 The safety report should show how the measures taken will prevent foreseeable failures which could lead to major accidents.
Schedule 3 Paras 4 and 5
	To meet this criterion the Safety Report should describe:
	Effectively a summary of all the other criteria, the assessor should come back to this when the other criteria have been assessed, and then conclude:
	• Whether all the assessed criteria have been met.
	• How significant the failure to meet one or more criteria is to the overall safety demonstration; in particular:
	  ○ identifying any failure to follow appropriate standards, codes of practice and guidance; and
	  ○ any deviations should be fully justified by the operator and the risks should be tolerable and ALARP.

Design	
12.2.1.1 The safety report should describe how the establishment and installations have been designed to an appropriate standard. **Regulation 8(c)**	The assessor should look at the overall design strategy and the justification for the design selected including the associated control measures. **i. Hazard Studies** **To meet this criterion the Safety Report should describe:** • the link between the design and the associated hazard studies;

TECHNICAL CRITERION	GUIDANCE
Schedule 3 para 5 (d)	• how a hierarchical approach has been used and inherent safety designs have been introduced where reasonably practicable. (Note - this may be difficult for existing plant but is relevant to the design of new plant and modifications. It is specifically addressed in 12.2.1.2 below) The Hazard Studies should be • sufficient to identify the hazards arising from the processes and the dangerous substances involved; • appropriate for the scale and nature of the hazards presented. Such studies could include HAZID, HAZOP, Fault Trees, FMEA, hazardous area classification, chemical reaction hazards assessment, SIL and LOPA assessments and where appropriate comparison with published standards; • carried out by competent personnel with sufficient resourcing and independence; • used correctly to inform decision making. **ii. Process Description and Use of Standards:** **<u>To meet this criterion the Safety Report should</u>:** • provide a clear description of each process summarizing each stage and key control measures. This may be in the form of process flow diagrams or other illustrations, as necessary; • give references to standards and codes of practice used as the basis for the design of the process and the selection of appropriate risk control measures. These may be incorporated in the text or as a list; • show that where such standards and codes have been revised or new standards created, these have been considered (e.g. by gap analysis) and incorporated into installations, where reasonably practicable. This is particularly important if the changes relate to incident history or safety alerts; • show that global or company standards (where they are used) align with appropriate published standards and guidance; • identify where the design of equipment is not covered by published standards and codes and demonstrate that safety and environmental protection is not compromised and that the risks are ALARP. Note: Other disciplines will look at the details of some of the standards referenced, for example pressure vessel design. Process Safety assessors will still need to maintain an overview to ensure that those standards are appropriate for the process.

TECHNICAL CRITERION	GUIDANCE
	For common types of installation, reference to published standards or guidance within the safety report may be an effective way of showing that adequate measures have been taken. However, in high hazard situations (those with the potential to harm large numbers of people in a single event), where the circumstances are not fully within the scope of the good practice, additional measures may be required to reduce risks ALARP. In such cases, HSE takes a precautionary approach by giving more weight to the use of sound engineering and operational practice than to arguments about the probability of failure. In simple terms, in such situations operators need to ask the question - are there any other measures which would be effective in further reducing the risks? They should then determine whether the extra measures are reasonably practicable and implement those that are. **iii. In addition, the Safety Report should:** • show that the principles of redundancy, diversity, separation and segregation have been applied to reduce the risk of common mode or common cause failure and to ensure the availability of back-up systems if required. It should also • identify how the behaviour of equipment on failure has been addressed, including events which may cause a fault and disable protective systems. • show that the performance standards (reliability, availability, accuracy, speed of response etc.) are adequate. Note: EC&I specialists will assess the design and performance of control equipment, but process safety specialists need to maintain an overview of the overall control, prevention and mitigation measures.
12.2.1.2 The safety report should show that a hierarchical approach to the selection of measures has been used. **Regulation 8(b) and (c)**	The use of a hierarchical approach is mentioned in 12.2.1.1 and 12.2.1.5. It also has relevance to other criteria. The four stage hierarchy, in order of priority, is: • Eliminate (inherent safety) • Prevent • Control • Mitigate **To meet this criterion the Safety Report should justify** the quantity and type of each dangerous substance on site by, for example, showing that appropriate consideration has been given to: • Reducing inventories of dangerous substances on site • Use of alternative less hazardous substances • Use of inherently safer processes • Use of smaller volume continuous/ semi-continuous processes rather than large batch processes, provided they can be properly controlled.

TECHNICAL CRITERION	GUIDANCE
	<u>To meet this criterion the Safety Report should show that</u> • processes are designed to eliminate or prevent unsafe conditions occurring and that the principles of redundancy, diversity, separation and segregation have been applied; • priority is given to passive rather than active measures; • Safety critical control measures have been identified and alternatives considered
12.2.1.3 Layout of the plant should limit the risk during operations, inspection, testing, maintenance, modification, repair and replacement. **Regulation 8(c)** **Schedule 3 Paras 3(d) and 4(a)**	Design of the layout of a plant can make a big contribution to reducing the likelihood and consequences of a major accident. **<u>To meet this criterion the Safety Report should show that:</u>** Due attention has been given to ensuring safety in the design of the layout of the installation. In particular, it should show how the layout prevents or reduces the development of major accident scenarios. Examples of how this might be achieved include the following: • Separation of hazardous plant from the site boundary to reduce off-site risk and to reduce risk to the plant from off-site causes such as fires; • Safe positioning of occupied buildings; • Separation between hazardous plant(s) and storage areas to limit the spread of fire and other domino effects; • Segregation/separation of incompatible materials; • Separation of hazardous plant and processes from ignition sources, roadways or other activities that may impact on safety; • Adequate ventilation to aid rapid dilution of flammable atmospheres; • Low congestion of structures, equipment, plant or any other obstacle to gas flow that could aggravate the pressure effects resulting from the ignition of a release of a flammable substance; • Access for emergency services; • Adequate shelter for use during any toxic release, and adequate means of escape during other emergencies; • Access for inspection, testing, maintenance and repair, at all times throughout the life of the plant; **<u>Where applicable, the Safety Report should contain the following records, or equivalent</u>:** • Maps of the site layout, identifying process and storage areas, occupied buildings, roadways, locations of dangerous substances; • HAC drawings showing the locations of flammable substances and the associated hazardous areas (see also 12.1.1.13);

TECHNICAL CRITERION	GUIDANCE
	• Drainage diagrams, as appropriate to demonstrate routes to separators etc.; • Location of gas detectors, fire/smoke detectors; • Loading/offloading facilities, delivery arrangements particularly tanker movements; • Vapour recycle/venting systems and emergency venting arrangements. (see also 12.2.1.5).
12.2.1.4 Utilities that are needed to implement any measure defined in the safety report should have suitable reliability, availability and survivability. **Regulation 8(c)** **Schedule 3 Paras 4(a) and 5(d)**	**To meet this criterion the Safety Report should show:** • The role and significance of the utilities has been considered in design, construction, operation and maintenance, to ensure that these utilities and facilities will be available when required; • The effect of the loss of key utilities has been considered as part of a structured hazard identification/analysis process. This should ensure that control systems and safety systems fail to a safe state and that the consequence of a utilities failure does not act as a major accident initiator; • The reliability of safety critical utilities has been determined and independent backup supplies provided where necessary. • Each utility and its back-up system; • Those utilities that are essential for operation of key safety systems. Utilities to be considered, as appropriate include: • Electrical/power supply • Fire water provision • Instrument and compressed air • Cooling water • Nitrogen • Any other safety critical utility [Note: EC&I will assess the effect of loss of utilities on control system instrumentation]
12.2.1.5 The safety report should show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances. **Regulation 8(b and c)**	**To meet this criterion the Safety Report should show:** The means by which dangerous substances (gas, liquid or solid) could be accidentally released from containment and the measures which have been provided to prevent such an occurrence. The Safety Report should show the suitability of measures to prevent or minimise releases. **i. Primary Containment** All process, storage and any other equipment containing dangerous substances should be designed to appropriate standards

TECHNICAL CRITERION	GUIDANCE
Schedule 3 Para 4(a) and 6(a)	as far as is reasonably practicable. Where there are deviations from standards, these should be documented and justified to demonstrate an equal level of safety; **ii. Secondary and tertiary containment measures** Where loss of containment of a significant quantity of dangerous substances is foreseeable, the Safety Report should describe the measures to limit the consequences. These measures include secondary and tertiary containment e.g. bunding, interceptors, catchment pits, dump tanks, diversion walls or grading of the ground. The Safety Report should identify such measures and demonstrate the adequacy of the design and the capacity in relation to the maximum expected spill. The possibility of bund overtopping and containment of firewater should be taken into account; **iii. Venting systems** The Safety Report should justify the design basis for any venting system taking into account foreseeable hazards (including loss of utilities or the effects of fire) and the safety consequences of venting (EA takes the lead on environmental effects); **iv. Isolation arrangements** The Safety Report should describe and justify the emergency automatic and manual isolation arrangements to manage a release including consideration of the time required to isolate. Appropriate performance standards for emergency isolation (e.g. HSG244) should be stated and justified in the report. (Note: Isolation may also be necessary for maintenance but the arrangements for this will be different from those required for emergency isolation where speed of response and accessibility may be important). **v. Detection of releases** The Safety Report should describe the measures to detect a loss of containment or other incident at an early stage. These measures include gas detection, level monitoring, loss of pressure, visual methods (cameras).
12.2.1.8 The safety report should show how the containment structure has been designed to withstand the loads experienced during normal operation of plant and all foreseeable operational extremes during its expected life. **Regulation 8(c)** **Schedule 3 Paras 4(a) and 5(d)**	**To meet this criterion the Safety Report should describe:** • the normal operating conditions of the plant and any foreseen operational extremes such as external loads, ambient temperatures and the full range of process variations (e.g. normal operation, start-up and shutdown, turndown, process upset, emergencies). • how safety margins are determined such that the safe working limits of the plant (pressures, temperatures, flow rates, liquid levels etc.) are compatible with all expected operating extremes. o Specific details should be given where actual applied margins differ significantly from industry practice and the safety implications arising from the variation should be described and justified.

TECHNICAL CRITERION	GUIDANCE

12.2.1.10 The safety report should describe how adequate safeguards have been provided to protect the plant against excursions beyond design conditions.
Regulation 8(c)
Schedule 3 para 5(d)
	<u>To meet this criterion the Safety Report should describe</u>:
	i. The safety related controls and alarms designed to prevent or warn of excursions beyond safe operating limits and upon which the safety of the plant is based;
	ii. How chemical reaction hazards are evaluated and justify the sufficiency of the control measures to prevent thermal runaway, over-pressurisation and loss of containment. This description should include chemical manufacturing processes as designed, and also accidental mixing of incompatible chemicals on site and treatment of waste streams.
	<u>The Safety Report should:</u>
	• Give details of the physical parameters of possible conditions: flows, temperatures and pressures with respect to excursions, runaway, worst case scenarios, etc.;
	• show that the design standards and other applied codes of practice are appropriate to the conditions under which the design must work;
	• Show that hazard identification has covered the possibility of beyond design conditions;
	• Show that accident history for a type of plant has been considered where relevant.
	iii. The emergency prevention and protection measures and show that these are fit for purpose. These measures include:
	• the safety related controls and alarms designed to prevent or warn of excursion beyond safe operating limits and upon which the safety of the plant is based;
	• The pressure relief and emergency venting arrangements. The method for the sizing of the pressure relief and emergency venting should be specified;
	• Explosion relief;
	• Active and passive fire protection;
	• Occupied Building Risk Assessment;
	• Interfaces with other measures designed to limit excursions beyond safe operating limits such as:
	  ○ shutting-off feed streams
	  ○ shutting down of heat sources
	  ○ adding inhibitors to the reagent
	  ○ dump systems
	  ○ inerting
	  ○ flushing through of continuous processes

TECHNICAL CRITERION	GUIDANCE
	○ application of process cooling ○ shut-down of equipment ○ Sprinklers/water deluge **iv.** Whether interventions are automatic or manual. For safety critical interventions, the report should show that the operator has examined the costs and benefits of automating the system and justified the suitability of the adopted approach. Where examples of procedures or operating instructions have been included in the safety report it may be helpful to examine them to clarify the description of the process and the associated control measures.
12.2.1.13 The safety report should show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk. **Regulation 8(c)** **Schedule 3 paras 5(a) and (d)**	**To meet this criterion the Safety Report should show:** • That the relevant requirements of DSEAR have been met and include examples of the hazardous area classification diagram(s); • The procedures and policies for identifying hazardous areas are based on established codes and standards; • The procedures and policies for identifying hazardous areas are consistently applied; • The hazardous area classification data is used in the selection and location of equipment and its maintenance and in considering plant and process changes. • Hazardous area classification is not normally applied to catastrophic failure situations. Nevertheless, the location of sources of ignition in relation to loss of containment events and major accident scenarios should be considered. The MAH risk assessment may indicate that further risk reduction measures are required such as removal of ignition sources or provision of protected electrical equipment in other areas e.g. closure of adjacent roadways during tanker loading / offloading, provision of protected lighting.
Modifications	
12.2.5.1 The safety report should show the system in place for ensuring modifications are adequately conceived, designed, installed and tested. **Regulation 8(c)** **Schedule 2 Para 2(d)**	Failure to manage change is a common cause of accidents. **To meet this criterion the Safety Report should describe:** i) The management of change procedure including: • the criteria for determining when a process change is sufficient to go through a formal management of change process; • whether a process change needs a formal hazard study/risk assessment; • whether the hierarchical approach is used where practicable in relation to process modifications and changes; • the competence and independence of the team or individuals involved in the decision making;

Appendix 12C 'Process Safety Assessment Criteria and Guidance'

TECHNICAL CRITERION	GUIDANCE
	• the method for ensuring that the modification is installed as specified in the change proposal. ii)The system for dealing with changes, updates or modifications to: • plant and equipment; • process parameters, e.g. temperature, pressure; • operating procedures and other documentation; • raw material specifications, suppliers etc.

SOME USEFUL REFERENCES

1.	**General** • Inspection of Process Safety Issues at COMAH Establishments (Operational Delivery Guide) • L138 DSEAR ACOP and guidance
2.	**Industry Guidance** • EI/IP Codes of Practice • LPGA Codes of Practice • BAMA Codes of Practice • BCGA/EIGA Codes of Practice • IGEM Codes of Practice • Other industry guidance British/European standards as appropriate – fire precautions, containment, hazardous area classification
3.	**Flammable Liquids** • HS(G) 51 storage in containers • HS(G) 140 The Safe use and handling of flammable liquids • HS(G) 176 storage in fixed tanks
4.	**Bulk storage** • Safety and Environmental Standards for fuel storage sites Buncefield Standards Task Group Final Report • CDOIF Guideline Process Safety Leadership Group – Other Products in Scope • CIRIA report 164 Containment systems for the prevention of pollution • API RP 2350 Overfill Protection for Storage Tanks in Petroleum Facilities • CDOIF Guideline – Leak Detection

	• SPC/Enforcement/163 Drainage of Floating Roof Tanks
5.	**Terminals** • HS(G) 186 The bulk transfer of dangerous liquids and gases between ship and shore • CDOIF Guideline – Terminal Loading Operations Hazard Awareness • CDOIF Guideline Automatic Overfill Prevention Systems for Terminal Loading Racks • UKPIA Report Automatic Shutdown of Ship Transfers • Energy Institute – Vapour Recovery Units – Guidance on preventing and controlling temperature excursions in carbon beds
6	**Hazardous Area Classification** • L138 Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) Approved Code of Practice and Guidance • BS EN 60079 Part 10 • Energy Institute Area Classification Code for installations handling flammable fluids Model Code of Safe Practice Part 15
7	**Process Precautions** • HS(G) 244 Remotely Operated Shut-off Valves (ROSOVs) for emergency isolation of hazardous substances • Chemicals Information sheet 2 Emergency isolation of process plant in the chemicals industry • FIC 431/10 The use of pigs in pipelines containing flammable liquids
8	**LPG** • UKLPG Codes of Practice • IP9 Liquefied Petroleum Gas Volume 1: Large bulk pressure storage and refrigerated LPG Model code of safe practice Part 9
9	**Miscellaneous** • HS(G) 143 Designing and operating safe chemical processes • HS(G) 71 Chemical Warehousing The storage of packaged dangerous substances • Guidance Note PM 84 Control of Safety Risks at gas turbines used for power generation • Guidance Note CS15 The cleaning and gas freeing of tanks containing flammable residues
10	**Chlorine** • HSG 28 'Safety advice for bulk chlorine installations' • HSG40 'Safe handling of chlorine from drums and cylinders' • Also chlorine covenant supplements
11	**Occupied Buildings guidance** • Guidance for the Location and Design of Occupied Buildings on Chemical Manufacturing Sites, Chemical Industries Association, third edition, 2010.