Ministry of Defence

JSP 815

Element 8: Infrastructure Design, Build and Maintenance

Contents

Amendment record

This element has been reviewed by the Directorate of Defence Safety (DDS) together with relevant subject matter experts and key Safety stakeholders. Any suggestions for amendments **should** be sent to COO-DDS-GroupMailbox@mod.gov.uk.

Version No	Date published	Text Affected	Authority
1.0	Dec 22	BETA version for consultation	Dir HS&EP
1.1	7 Jun 23	Final version	DDS
1.2	10 Sep 24	Annual revision and combined element and assurance framework	DDS

Terms and definitions

General safety terms and definitions are provided in the Master Glossary of Safety Terms and Definitions which can also be accessed on GOV.UK.

Must and should

Where this element says must, this means that the action is a compulsory requirement.

Where this element says should, this means that the action is not a compulsory requirement but is considered good practice.

Introduction

1. This element provides the direction that must be followed and the guidance and good practice that should be followed and will assist users to comply with the expectations for the Management of the Defence Estate that are set out in this Element. It should be read in conjunction with JSP 850: Infrastructure and Estate Policy Standards and Guidance, the Infrastructure Operating Model (IOM) guidance and JSP 375 Volume 3: High Risk Activities on the Defence Estate.

Purpose and expectations

2. This element is to assist the Defence organisation in ensuring that that frameworks and working practices are in place to incorporate cradle to grave safety considerations into the whole life asset management approach for estate and its infrastructure.

Infrastructure Asset Management (AM)

3. Defence infrastructure and estate policy requires that any activities relating to its through life management and operation are conducted appropriately and to a clear set of guidelines and rules. In this context, this relates to the management of the whole lifecycle of the estate and its physical assets from strategic planning, acquisition or construction through its operation and maintenance to end of life, disposal or demolition.

4. The infrastructure control framework for the operation of the Defence estate is illustrated in Figure 1.

Figure 1 – Infrastructure control framework

Key principles

5. Defence organisations should make sure that safety risks and dependencies within their organisations, infrastructure assets and their supply chain are effectively managed in accordance with the Infrastructure Operating Model (IOM) to support Defence capabilities, outputs and communities efficiently and effectively. The key principles of the IOM should be applied throughout the whole lifecycle of the infrastructure; for safety this should include:

a. management of infrastructure as a strategic asset through a structured approach with clear line of sight from Defence's overall infrastructure strategy through to operation, management and delivery activities at unit level;

b. a clear and communicated minimum set of common parameters and processes which individuals and organisations are to comply with to ensure the efficient and effective operation of the Defence estate;

c. clarity and separation of roles with organisations operating across defined interfaces;

d. clarity of individual accountability and responsibility reinforced through appropriate mechanisms for holding to account and performance reporting;

e. clarity of delegation of Infrastructure funding and liabilities with financial decision making placed with those who understand what is required and can prioritise expenditure to best effect;

f. clarity of organisational and individual competence where staff develop and maintain the knowledge, skills, experience and behaviours (KSEB) required to be effective to deliver their assigned roles;

g. clear and appropriate management information where decisions are taken based on accurate, robust and assured data and analysis;

h. clear behavioural expectations where organisational and individual ways of working are consistent with pan-Defence behavioural principles and support effective and efficient delivery of 'best for Defence' outputs.

Compliance with legislation

6. Defence organisations must have mechanisms to ensure their infrastructure is compliant with statute throughout its lifecycle, this may include engaging with a delivery agent, such as the Defence Infrastructure Organisation (DIO) to maintain the infrastructure to the required standard. There may be unique circumstances where compliance with legislation is not achievable, it may be necessary for the Defence organisation to seek a disapplication, exemption or derogation (DED). DEDs are covered further in Element 3 of this JSP.

7. Any conflict or concerns in relation to policy or legislation which might prevent compliance should be raised with the functional owner, DCDS (Mil Cap) or other such responsible authority, for resolution and guidance on how to proceed.

Strategy and planning

8. Safety should be embedded into infrastructure and assets at the earliest possible stage of the Whole Life Asset Management (WLAM) life cycle; therefore, it is during the initial design stages where there is the greatest opportunity to ensure that infrastructure is safe. Hazards to be managed in constructing, operating and maintaining the infrastructure, as well as those caused by the auxiliary facilities should be evaluated and risk assessed considering all the options available. In most cases, this will include identification of appropriate standards and improvements to the design to reduce hazards and hazard exposure.

Life cycle delivery

Acquisition / Construction

9. During infrastructure or asset construction, key decisions related to design amendments, change in materials or change in design will impact the safety risks in future operation and maintenance. A change management process should be followed to re-assess risks and evaluate the impact of the proposed changes. During construction (and throughout the WLAM lifecycle), it is essential that organisations and individuals enact their roles and work across interfaces within a capability framework, which is covered more in the IOM. The main activities undertaken by Defence organisations sit within the Capability Framework which are depicted in Figure 1.

Operating and maintaining infrastructure assets

10. During the in-service phase of the WLAM life cycle the appropriate and compliant use and maintenance of infrastructure should be included in the relevant risk assessments and aligned with the safety case. Hazards and corresponding risks of maintenance activities should also be risk assessed including not only the requirement for effective maintenance to ensure continued safe operation but also the hazards and risks of conducting maintenance activities themselves such as access and egress, hazardous substances, hot work, removal of guarding and entrapment and crushing risks, explosive substances and so on. Where infrastructure is authorised to be used outside its normal operating envelope, relevant risk assessments and safe systems of work should be updated to reflect the new situation.

11. For infrastructure assets that are in the in-service phase of the WLAM life cycle, Defence organisations infrastructure teams should capture all required maintenance work planned for their assets as a programme of work (PoW) in their Annual Delivery Plan (e.g., Command Infrastructure Delivery Plan (CIDP)). Defence organisations should work with their delivery agents to develop business cases and seek necessary approval and funding for their required maintenance arrangements based upon a priority order with safety related requirements as the highest priority.

12. Infrastructure planning activities will identify the need to support previously agreed operational capabilities in a way that extends the life of a facility, mitigates infrastructure risks or delivers an improvement that delivers infrastructure efficiencies. These requirements should all be captured in Annual Delivery Plan (for example, CIDPs).

13. All minor repairs and maintenance on infrastructure assets should be included in the Future Defence Infrastructure Services (FDIS) contract, which covers all sites and establishments on the UK Defence estate, except those with long-term contracts already in place (such as current PFIs). FDIS is the delivery programme for Facilities Management (FM), Accommodation Management and Training Management on the UK Defence estate. This includes all Hard FM services required to maintain and support operational outputs and capability.

Disposing of infrastructure assets

14. Through infrastructure planning, customers will identify and raise appropriate requirements for disposal of estate assets no longer required and termination of related contracts. Requirements are captured in Annual Delivery Plan (e.g., CIDPs). Following infrastructure subject matter experts (SME) checks of wider alignment of any other proposals for estate use, Defence organisations and the DIO will programme the disposal activity, including any studies or other enabling work as per the guidance set out in JSP 850 – Infrastructure and Estate Policy, Standards and Guidance.

Infrastructure risk and review

15. Risk management on the Defence estate is articulated within the IOM. In delivering and performance managing Defence infrastructure assets, risks must be identified and managed in a consistent and coherent manner in accordance with JSP 892 (Risk Management). Defence organisations that manage or operate on the Defence estate must have their own internal risk management processes in place which are in accordance with the IOM and JSP 892. Risk assessment is covered in more detail in Element 4 of this JSP and in JSP 375 Chapter 8 - Safety Risk Assessment and Safe Systems of Work.

16. Infrastructure is an integral part of the Defence Performance, Risk and Assurance Framework and the Quarterly Programme and Risk Reviews (QPRR). Head office measures all Defence organisations infrastructure performance against annual objectives set in the Defence Plan and associated Command Plans, and against the medium / long term plans and targets set out in the Strategy for Defence Infrastructure (SDI), Strategic Infrastructure Deliver Direction (SIDD) and the associated medium / long term TLB Infrastructure Management Plans (TIMPs).

17. In delivering and performance managing Defence Infrastructure, customers, with the support of infrastructure SMEs and delivery agents, are responsible for identifying and managing risks that could impact on outputs, capability and reputation, escalating to Head Office where Enterprise level impacts are identified.

Monitoring and Reporting

18. Infrastructure safety issues should be raised at all levels within the Infrastructure Enterprise and included and prioritised within work plans and schedules. There should be a clear rule set and escalation process with communication routes to and from all levels within the Infrastructure Enterprise and the IOM. For example, site level infrastructure safety issues should be raised and addressed at the relevant site level Infrastructure Community Monthly Meeting (ICMM), with a clear escalation route right up to the Infrastructure Joint Committee (IJC) for serious safety issues where they have a wider Defence impact. Raising safety concerns is set out in Element 11 of this JSP and reporting safety occurrences is set out in Element 10 of this JSP.

19. Defence organisations should document (with the help of all stakeholders concerned) and communicate across the Defence organisation, and wider Defence where necessary, any lessons learned from previous infrastructure design, acquisition, manufacture, operation, modification and maintenance activities, where they may prevent recurrence of any safety issues.

20. All safety concerns on the Defence estate and any required actions must be communicated to the relevant stakeholders (for example users or maintainers) in a timely manner as identified in the Defence organisation's communications plan. Procedures must be in place to notify users and potential users of infrastructure that is determined to be defective or inappropriate for specific uses.

21. Continuous and coherent performance management and assurance is critical to ensuring Defence infrastructure is delivered and maintained to meet user requirements within policy, standards and funding constraints. Defence organisations should monitor performance against the agreed PoW captured in their CIDPs and focus on maintaining a safe and compliant estate against the cost and time of programme delivery.

22. A culture of continual improvement, collaboration and communication throughout the IOM and whole life management activities is required to ensure all organisations learn from experience to improve their approaches to safety, in an efficient and effective way.

Roles and responsibilities

Accountability, roles and responsibilities for managing safety across the whole scope, activities and lifecycle of the Defence Estate are articulated in the IOM. Those with clear safety responsibilities for Defence establishments such as the Head of Establishment (HoE) must be formally appointed into such roles and once appointed they should be able to demonstrate that they have accepted that role. Further detail on HoE responsibilities are covered in Annex D to this JSP.

Element assurance framework

23. The focus of this element requires that the Defence organisation has put in place frameworks and working practices to incorporate safety considerations into the strategic and technical design, spatial coordination, acquisition, manufacture and construction, handover, use, modification, maintenance and disposal of infrastructure.

24. The expectations and performance statements for this element are set out in the following pages.

Expectations and performance statements

Element 8: Infrastructure Design, Build and Maintenance

The Expectations in this element are:

E8.1 The Defence Organisation has mechanisms in place to identify and assess safety risks and requirements associated with infrastructure throughout its entire lifecycle; from Concept, Assessment, Design, Manufacture and Construction, Use, Maintenance, and Disposal.

E8.2 The Defence organisation has mechanisms in place to ensure risks associated with infrastructure are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate Duty Holder, SRO, Head of Establishment, and competent person.

E8.3 The Defence organisation has mechanisms in place to ensure infrastructure is compliant with statute and Defence regulation throughout its lifecycle. Where necessary, an exemption / waiver / concession is in place where compliance is not achievable.

E8.4 The Defence organisation has processes in place to ensure infrastructure is maintained and operated within its intended use. Mechanisms are in place to communicate these processes to the workforce that operate and maintain the infrastructure.

E8.5 The Defence organisation has mechanisms in place to ensure physical changes to infrastructure, (including major software changes), materials and associated specifications are evaluated, risk assessed, approved and documented.

E8.6 The Defence organisation has mechanisms to accurately identify and manage the safety risks and dependencies in its infrastructure supply chain.

E8.7 Lessons learned from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities are shared effectively across the Defence organisation.

Documents often associated with this element:

- 10-year infrastructure management plan
- Agenda and minutes of the Equipment and Support steering group meetings
- Annual Budget Cycle (ABC) planning (for inclusion of safety requirements such as routine calibration
- Capability management group meeting minutes
- Capability management strategy and plans
- Command Infrastructure Delivery Plan (CIDP)
- Command / Corporate plan
- Contract management and supply chain management plans
- Corrective action plans arising from assurance, equipment design and infrastructure design
- Defence organisation business plans
- Defence organisation Operating Model
- Defence organisation SMS
- Equipment plan (equipment list with life cycle and replacement plan)
- Exemplar safety case reports (specifically all category A safety cases, high risk / high complexity B & C)
- Project plans including Royal Institute of British Architects (RIBA) stages

Expectation 8.1 The Defence organisation has mechanisms in place to identify and assess safety risks and requirements associated with infrastructure throughout its entire lifecycle; from Concept, Assessment, Design, Manufacture and Construction, Use, Maintenance and Disposal.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that the Defence organisation have a mechanism in place to identify and assess infrastructure safety risks and requirements.	• The Defence organisation has a mechanism to identify and assess safety risks and requirements however does not take account of the full infrastructure lifecycle.	• The Defence organisation has a mechanism to identify and assess safety risks and requirements throughout the entire infrastructure lifecycle. • Infrastructure risk assessments include specific consideration of as-built use and any change of use.	• Risks and requirements are formally re-assessed on a continuous basis throughout the infrastructure lifecycle (including change of use and / or retrofitting), with lessons learned are shared and applied across the Defence organisation.

Expectation 8.2 The Defence organisation has mechanisms in place to ensure risks associated with infrastructure are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate Duty Holder, SRO, head of establishment, and competent person.

Unsatisfactory	Limited	Moderate	Substantial
• Infrastructure safety risks are identified but there is little or no evidence to demonstrate there are mechanisms in place to control and mitigate those risks.	• The Defence organisation has a mechanism to control and mitigate infrastructure safety risks however does not take account of the full infrastructure lifecycle. • Risks are elevated to the appropriate Duty Holder, SRO, head of establishment, and competent person however this is not consistently undertaken across the Defence organisation.	• The Defence organisation has a mechanism to control and mitigate infrastructure safety risks throughout the entire lifecycle. • Risks are consistently elevated to the appropriate Duty Holder, SRO, head of establishment, and competent person across the Defence organisation.	• Processes and controls to manage safety risks are regularly updated, following identification of new risks and re-assessment of existing risks, lessons learned are applied. • Duty Holder, SRO, head of establishment, and competent persons act on risks elevated and ensure risks are controlled and mitigated.

Expectation 8.3 The Defence organisation has mechanisms in place to ensure infrastructure is compliant with statute and Defence regulation throughout its lifecycle. – Where necessary, an exemption / waiver / concession is in place where compliance is not achievable.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that the Defence organisation have mechanisms in place to ensure infrastructure is compliant with statute and Defence regulation. • There is little or no evidence to demonstrate that Exemptions / waivers / concessions are in place where compliance is unachievable.	• The Defence organisation has mechanisms in place to ensure infrastructure is compliant with statute and Defence regulation, but there is not enough evidence of these being reviewed when there is a change of use proposed or realised. • Exemptions / waivers / concessions are sometimes in place where compliance is not achievable.	• There is some but could be improved evidence that mechanisms are in place to ensure infrastructure is compliant with statute and Defence regulation, or where this is not possible or required, alternative arrangements are in place. • Exemptions / waivers / concessions are regularly in place where compliance is not achievable. Exemptions / waivers / concessions from compliance with statute and Defence Regulations are well understood, recorded in a written format centrally and monitored.	• There is robust evidence that the Defence organisation actively monitors changes in statute, Defence regulation, technology, social, environmental, and political influences, or retrofitted infrastructure to remain compliant with changing requirements. • Where required, infrastructure is upgraded, refurbished, retrofitted and / or decommissioned to remain compliant with requirements. • Exemptions / waivers / concessions are approved for defined periods and compliance with statute is reviewed prior to the expiry date.

Expectation 8.4 The Defence organisation has processes in place to ensure infrastructure is maintained and operated within its intended use. Mechanisms are in place to communicate these processes to the workforce that operate and maintain the infrastructure.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that the Defence organisation has processes in place to maintain and operate infrastructure within its intended use and operating specifications. • There is little or no evidence to demonstrate that intended use limits are defined or communicated to those who interface with the infrastructure.	• The Defence organisation has a largely reactive approach to maintenance. Where planned maintenance is in place there is no consistent prioritisation process and delays are evident. • There is some, but not enough evidence of intended use limits being defined, and communicated on a timely basis to those who interface with infrastructure.	• The Defence organisation has successfully implemented an effective preventative maintenance regime which includes a prioritisation process. • Safety critical infrastructure is identified and is subject to specific procedures and protocols and this is communicated. • Risks which impact effectiveness of safety critical infrastructure controls are elevated promptly and the continued use of the infrastructure is avoided where possible. • There is some but could be improved evidence that the intended use and operating limits are clearly defined and communicated to those who interface with infrastructure. This includes where changes are made to the intended use or operating limits of infrastructure out of its initial intended use.	• There is robust evidence of an effective and preventative maintenance regime across the organisation. • There is robust evidence that intended use and operating limits are regularly re-assessed so that infrastructure is maintained and operated within those intended use and operating limits. Those who interface with infrastructure are actively consulted during risk reviews and findings are communicated to them.

		• Where operating limits are exceeded, these are monitored, with documented action taken to maintain operating capability.	

Expectation 8.5 The Defence organisation has mechanisms in place to ensure physical changes to infrastructure (including major software changes), materials and associated specifications are evaluated, risk assessed, approved and documented.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that physical changes to infrastructure are formally evaluated, risk-assessed and documented.	• The Defence organisation has mechanisms in place to ensure physical changes to infrastructure are evaluated. • However, a suitable and sufficient risk-assessment is not consistently performed, and controls are not formally documented or communicated.	• The Defence organisation has mechanisms in place to ensure physical changes to infrastructure are evaluated, risk-assessed and documented. • Those who operate, maintain, inspect, and manage infrastructure are consulted in the evaluation process. • Mitigating safety controls are formally approved by an appropriately competent person before being communicated across the Defence organisation.	• Physical changes to infrastructure are anticipated based on ongoing risk-assessments of the Defence organisations' infrastructure portfolio. • Changes are evaluated and risk assessed regularly. Input is encouraged from stakeholders who maintain, use, and are affected by the operation of this infrastructure.

Expectation 8.6 The Defence organisation has mechanisms to accurately identify and manage the safety risks and dependencies in its infrastructure supply chain.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that there is consideration for infrastructure safety risk management throughout the Defence organisation's supply chain.	• Infrastructure safety risk management is reliant upon the supply chain providing details of safety risks. • Risk ownership is not well defined with respect to dependencies between Defence organisations and the supply chain.	• Infrastructure safety risks are shared openly between Defence organisations and their supply chains. • Risk ownership is understood and dependencies between Defence organisations documented.	• Infrastructure safety risks are shared between Defence organisations and these are recorded, regularly monitored, and collaboratively mitigated and managed. • Where dependencies are present these are proactively managed and deconflicted.

Expectation 8.7 Lessons learned from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities are shared effectively across the Defence organisation.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that infrastructure information is held centrally for the whole Defence organisation to access. • There is little or no evidence to demonstrate that lessons learned from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities are formally documented. • There is little or no evidence to demonstrate that procedures are in place to notify potential users of infrastructure determined to be defective or inappropriate for specific uses.	• Infrastructure information is maintained centrally, however not communicated across the Defence organisation. • There is some, but not enough evidence that lessons learned from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities are documented and communicated across the Defence organisation. • There is some, but not enough evidence that procedures are in place and consistently used to notify potential users of infrastructure determined to be defective or inappropriate for specific uses.	• Infrastructure information is maintained centrally and is communicated across the Defence organisation. • Lessons learned from previous infrastructure design, acquisition, manufacture, operation, modification, and maintenance activities are documented and communicated across the Defence organisation. • There is some but could be improved evidence that procedures are in place and are used to notify potential users that infrastructure has been determined to be defective or inappropriate for specific uses.	• There is robust evidence that lessons learned from previous infrastructure design, acquisition, manufacture, operation, modification and maintenance activities are documented and are proactively communicated across the Defence organisation and wider Defence and have been proven to prevent recurrence of safety issues. • There is robust evidence that procedures are in place and consistently used to notify potential users of infrastructure determined to be defective or inappropriate for specific uses.