Ministry of Defence

JSP 815 Volume 2

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 June 23	Final version of Volume 2	DDS

Terms and definitions

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

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 to comply with the policy.

Scope

This policy applies to all those employed by Defence (military or civilian) as well as those working on behalf of Defence (for example, contractors). It applies to all Defence activities carried out in any location (UK or overseas).

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 Element 8 of the Volume 1 to JSP 815 (this JSP). It should be read in conjunction with the Infrastructure Operating Model guidance and JSP 850: Infrastructure and Estate Policy, Standards and Guidance.

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 framework for the operation of the Defence estate is set out in the Infrastructure Operating Model (IOM), the Infrastructure Control Framework (illustrated in Figure 1) and in JSP 850.

Figure 1 – Infrastructure control framework

Key principles

5. Defence organisations should ensure 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 (SKEB) 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 Volume 2.

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 (e.g.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 Volume 2 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 Volume 2 and reporting safety occurrences is set out in Element 10 of this Volume 2.

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

23. 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 Volume 2.

Element summary

24. Defence organisation leaders should make sure that their organisations:

a. Have mechanisms in place to identify and assess safety risks and requirements associated with infrastructure throughout its entire lifecycle.

b. Have mechanisms to ensure risks associated with infrastructure are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate management level.

c. Have mechanisms to ensure infrastructure is compliant with statute or a disapplication or derogation throughout its lifecycle and where necessary an exemption is in place where compliance is not achievable.

d. Have processes in place to ensure infrastructure is maintained and operated within defined design intent. Mechanisms are in place to communicate these processes to the workforce that operate and maintain the infrastructure.

e. Have mechanisms in place to ensure physical changes to infrastructure are evaluated, risk assessed, approved and documented.

f. Have mechanisms to accurately identify and manage the safety risks and dependencies in its infrastructure supply chain.

g. Learn lessons from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities and they are shared effectively across the Defence organisation.