MINISTRY OF DEFENCE

JOINT SERVICE PUBLICATION

JSP 604

Network Rules

MINISTRY OF DEFENCE

Issue 3.0
Aug 2012

UNCONTROLLED WHEN PRINTED

This policy has been equality and diversity impact assessed in accordance with Departmental policy. This resulted in a Part 1 screening only completed (no direct discrimination or adverse impact identified)

Document History Sheet

ISSUE NUMBER / AUTHOR	DESCRIPTION OF MAJOR CHANGES	DATE
Issue 0.1 ISS Sols-C4 Tech Arch 1	1. Initial draft issue produced by JSP 604 Sponsor (DES D ISS).	23/02/2009
Issue 0.2 – 0.4 ISS Sols-C4 Tech Arch 1	1. Incorporation of initial comments from DES D ISS SvcOps.	10/03/2009
Issue 0.5 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Update of Network Joining Rules and Introduction.	01/04/2009
Issue 0.6 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Incorporation of EDIAT Statement.	01/04/2009
Issue 0.7 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Minor grammatical errors removed.	02/04/2009
Issue 0.8 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Incorporation of comments from CIO-XStrat .	06/04/2009
Issue 1.0 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Formal issue of JSP 604 approved by JSP 604 Owner (Defence CIO).	07/04/2009
Issue 1.1 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	1. Changes to JSP reference and broken hyperlink under Rule 8. Correction of email contact details due to role changes.	08/05/2009
Issue 2.0 ISS Sols-C4 Arch-AIT1 ISS Sols-C4RPM-SRA AsstHd	1. Restructuring of the document and inclusion of appropriate test requirements. 2. Renumbering of rules to reflect changes and amendments 3. Document upissued to version 2 following internal staffing (of draft versions 2.1 to 2.4)	09/06/2010
Issue 3.0 Draft D DES ISS NTA-Coh-OpDel	1. Restructuring of the document based on Principles, Rules and Criteria. 2. Renumbering of rules to reflect changes and amendments.	15/06/2012
Issue 3.0 Draft F DES ISS NTA-Coh-OpDel	1. Comments included from draft D circulation.	11/07/2012
Issue 3.0 DES ISS NTA-Coh-OpDel	1. Comments included from NSAG circulation.	03/08/2012

Contents

Introduction

Background

1. This Defence Chief Information Officer (CIO) owned Joint Service Publication (JSP) has been developed to define the set of Network Rules that are to be applied to all Information and Communications Technology (ICT) that will contribute to or consume Defence network resources. The scope includes those that are either funded by the MOD or interact with the Department's current and planned ICT systems, here after referred to as the 'network'.

2. JSP 604 – The Network Rules – will assist decision makers at all levels in understanding the risk and impact of new or changed ICT. Their decisions play a 'protecting' role in ensuring acceptable conduct as a 'Good Neighbour' across the network. The evolution of these rules will be against increasing levels of interoperability and co-existence.

3. It must be understood that a failure to comply with JSP 604 is most likely to result in capability being prevented from joining or being removed from the network.

Ownership and Authority

4. The Defence CIO, as owner of the JSP 600 series for MOD CIS Policy and Assurance has approved the issue of this document. JSP 604 is sponsored, controlled and maintained by Director Information Systems and Services (D ISS) Network Technical Authority (NTA). The document is designed to be adaptive and will evolve in accordance with the direction given by the Network Authority[1] whose role is to ensure coherence, performance and integrity of all aspects of the Defence Network.

Applicability

5. Application of JSP 604 is mandated by the Defence CIO for <u>all</u> projects and/or programmes across Defence[2] that are funded by the Department, constitute or interact with current and programmed Departmental ICT. This includes Urgent Operational Requirements (UORs), Urgent Operational Tasks (UOTs) and Cloud Services[3]. Hd NTA, as the document's sponsor, is responsible for the content, publication and management of JSP 604.

6. In accordance with the ethos of Through Life Capability Management[4], projects are required to apply the rules <u>throughout</u> the project's and/or programme's acquisition life-cycle. There is a particular focus at the following milestones:

a. Initial and Main Gate;

b. Preliminary and Critical Design Review;

[1] Further explanation of Network Authority is given in para 9.
[2] This extends to all MOD organisations including Trading Funds and Agencies
[3] A Cloud Service is the delivery of computing software, infrastructure and platform as a service to a heterogeneous community of end-recipients.
4 As defined in the Acquisition Operating Framework (AOF)

c. Immediately prior to 'go live' and

d. Six months after go live.

7. Through Life Changes: Projects and/or programmes are required to continue to apply the JSP 604 Network Rules through-life. There is a requirement to ensure that any upgrades or changes (be these part of an incremental acquisition strategy or in-service changes that have an impact on the network) also comply with the Network Rules extant at that time. It is a Project Managers responsibility to consult with the NTA to determine if any upgrades or changes will require formal NTA assured JSP 604 compliance.

8. Whilst Project Teams may choose to delegate responsibility for the provision of evidence, overall responsibility shall rest with the Project Team to present its case to the Network Technical Authority to demonstrate compliance with this JSP.

Governance

9. The Network Authority (NA)[5] is responsible for the coherence, performance and integrity of all aspects of the Defence Network, and the information flows it enables, to support the operational and business needs of the Ministry of Defence.

10. The Network Authority is comprised of three key areas who have been given mandates[6] by Defence CIO:

a. Network Capability Authority: ensures coherent development of all requirements for services, systems, platforms and applications dependent on the Defence network;

b. Network Technical Authority: ensures the technical coherence of the network, informing its future development AND development of the technical architecture, rules and standards – the C4 SOSA Domain;

c. Network Operating Authority: protects, operates and defends the Defence network thereby preserving its operational capability and integrity.

11. Together each area will contribute to ensuring:

a. Systems will connect to each other;

b. Systems do not duplicate function;

c. Communications systems will be able to support information systems;

d. Applications will run on Defence's networks;

e. Applications will not consume excess bandwidth;

f. Data sharing between applications is maximised;

[5] The NA reports to the CIO Systems Direction Group whose Defence Board (DB) endorsed role is to identify where accelerated improvements in existing programmes can be made by applying new policies, architectures, standards or engineering approaches.
[6] Further information on the Network Authority and its Sub Authorities can be found here.

g. Systems will not block other system's management traffic;

h. There is a secure network working environment.

i. Coherence with OGD, NATO and Allies.

12. JSP 604 inherently supports the intent of the Defence Information Reference Model (DIRM) which is to "provide Defence with a means to compare new information and communications technology (ICT) requirements against the existing ICT assets re-using those that are suitable".[7]

Principle, Rules and Criteria Structure.

13. JSP 604 Issue 3 introduces the concept of a 'Principles, Rules and Criteria' construct. This approach has been used to ensure the Rules within JSP 604 support a fundamental attribute of ICT, the Principle. The following definitions explain the Principle, Rule and Criteria levels.

a. Principle: A Fundamental Attribute of ICT: An enduring generalised statement that informs and supports the way in which an organisation sets about fulfilling its mission. A principle may be just one element in a structured set of ideas that collectively define and guide the organisation, from values through to actions (defined by the Rules and Criteria) and results. The JSP 604 Principles are based on those contained in TOGAF (The Open Group Architecture Framework). While the Defence ICT Strategy Principles provide a wider view there is read across to those contained within this document.

b. Rule: What is expected of ICT: A statement that prescribes the required effect of ICT. Rules should be directly linked to one, or more, principles.

c. Criteria: How a Project Shall Demonstrate Compliance with a Rule: Describes the maturity of evidence required for compliance to each rule. The evidence is expected to mature through the project's lifecycle and shall be provided by the project.

14. While the Principles are key to the need for the Rules they are not used in the assessment process. For this reason they are contain in Annex A.

The Rule Format

15. The following table provides an explanation of the component elements of a JSP 604 Rule so users of this document can understand its construct and the intent of the information it contains.

RULE TITLE AND IDENTIFICATION NUMBER	
Rule Owner	*This is the Organisation, Department and Section (eg DE&S ISS, Network Technical Authority, Architecture) that owns the rule and is responsible for its currency. Each rule will have a single owner identified.*

[7] DIRM Single Statement of User Need

Parent Principle(s)	*Identifies the parent Principles that guide the behaviour required from application of the Rule. These Principles are identified in Annex A. More than one Principle may be identified per rule.*
Rationale:	*This is the reasoning why the rule is in place. This may reference wider strategy and policy.*
Policy References:	*Contains references and links to relevant policy, governance and supporting sources of information.*
Subject Matter Expertise POCs:	*Identification of Subject Matter Experts (SME) which have specialist knowledge within the rule area. The SMEs are identified at Organisation, Department and Section level.*
Rule Requirements	*Statement of the requirements(s) that shall be met to comply with the rule. These are written from the perspective of 'ICT shall be……'. This area may refer to specific supporting guidance, policy etc. Multiple requirements may be listed in this area.*

Table 1 - Rule Format

Development Lifecycle Criteria Evidence

The table below provides a development lifecycle view of the maturity of project progress, demonstrated through Criteria Evidence, toward achieving the Rule Requirement. The assessment points shown are based on EP projects, where this is not applicable the assessment points may need to be tailored by the NTA Case Officer.

RULE TITLE AND IDENTIFICATION NUMBER						
Rule Requirement	**Initial Gate (IG)**	**Main Gate (MG)**	**Preliminary Design Review (PDR)**	**Critical Design Review (CDR)**	**Technical Release Readiness Review (TRRA)**	**Authority to Operate (AtO))**
1) Rule Requirement Title	*Description of the maturity of criteria evidence at IG.*	*Description of the maturity of criteria evidence at MG.*	*Description of the maturity of criteria evidence at PDR.*	*Description of the maturity of criteria evidence at CDR.*	*Description of the maturity of criteria evidence required by the NTA to enable the production of the TRRA.*	*Description of the maturity of criteria evidence at AtO.*

Table 2 - Rule Format - Continued

How the Rules are Applied

16. JSP 604 is applied by the NTA with support from identified rule SMEs; paragraphs 18-22 provide a high level view of the NTA assessment process.

17. Responsibility lies with the Project Manager to approach the NTA (via DESISSNTA-PortalMailbox@mod.uk) at the earliest opportunity. The NTA will complete an initial assessment of the capability and advise the Project Manager as to the degree of NTA engagement; this may include the assignment of a NTA Case Officer whom will work with the project through life or it may place responsibility with the Project Manager to effectively self assure against JSP 604.

18. The through-life nature of JSP 604 requires (i) an identification of the project specific rules and criteria, (ii) an assessment of the evidence and (iii) the production of a Technical Release Readiness Assessment (TRRA). This document is a key component of the evidence that the Network Operating Authority (NOA) assesses when making its judgement as to whether a capability can join the network. Detail of each of the three phases follows below.

19. **Define NTA Assessment:** An NTA Case Officer will be assigned to the project. They will assess, in consultation with the Project and, where required, Subject Matter Experts whether JSP 604 assessment is required and what rules are applicable. It is vital that projects engage with the NTA early in their lifecycle. The majority of rules require identification and planning in the concept (or similar) stage of a project as a failure to do so may impact project timescales and cost and ultimately prevent them from joining the network.

20. The criteria evidence points of IG, MG, PDR, CDR, TRRA and ATO identified in the rules are primarily focussed around Equipment Programme (EP) projects. It is understood that projects may have differing procurement strategies and assessment points. The Case Officer will provide guidance with respect to where they fit to the Projects Development Plan.

21. **Conduct NTA Assessment:** The Case Officer will, throughout their engagement, assess the project's progress in achieving compliance with each of the applicable rules.

22. Where there is a concern that an adequate degree of compliance may not be achieved then the Case Officer, in consultation with the project and rule SME, may escalate the issue through the Network Authority governance structure as appropriate. For specific rules, processes may already exist to deal with non-compliance e.g. DSAS Risk Balance Case (JSP 440), these will be used where available.

23. **Review evidence and produce Technical Release Readiness Assessment (TRRA):** Responsibility rests with the Project Manager to provide the NTA Case Officer with the set of interpreted evidence to demonstrate the degree of compliance with the identified rules and criteria. The Case Officer will use this evidence to write a TRRA report. This document aims to quantify the residual risk (i.e. once appropriate mitigation action has been taken to manage any identified network affecting risks) to the network of a capability going live. It forms a core element of the suite of evidence that allows the NOA to consider whether the capability is granted an 'Authority to Deploy' as defined in ISSP 154[8].

[8] ISSP 154: ISS Process: Release and Deployment Process

Document Governance

24. This document is managed by the NTA on behalf of Defence CIO. Any changes to this document must be submitted to the NTA for necessary comment and circulation prior to submission to Defence CIO for approval.

25. Comments or questions on the content of this Joint Service Publication should be directed to:

Network Technical Authority
Bldg 405 Spur E level 3
Westwells Road
Corsham
Wiltshire
SN13 9NR

Mil: 96770 0787 Civ: 030 6770 0787
e-mail: DESISSNTA-PortalMailbox@mod.uk

Introduction of JSP 604 Version 3 Changes

26. Projects shall apply JSP 604 Version 3 from the date of its publication. Those projects that have already engaged with the NTA and have been applying an earlier version of JSP 604 may continue to do so, although it may be in their interests to adopt this new version. Their ongoing engagement with the NTA will address this.

JSP 604 Rules

RULE 1 – ICT SHALL BE REUSED WHERE AVAILABLE.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence, Affordability
Rationale:	This rule embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organisational perspective. Maximum return on investment requires decision makers to adhere to enterprise-wide drivers, policies and priorities. No minority group will detract from the benefit of the whole. Some organisations may have to concede their own preferences for the greater benefit of the entire enterprise.
Policy References:	Cross Government ICT Strategy JSP 906: Design Principles for the Acquisition of Capability DIN 2010DIN05-021: Defence Information Infrastructure (DII) Exemption Policy for Specialist Networks and Standalone Computers
Subject Matter Expertise POCs:	DES ISS NTA Architecture Team DE&S D ISS DIST DE&S D ISS Networks Services Team DE&S D ISS Bowman And Tactical Communication & Information Systems (BATCIS)
Rule Requirements	**1. Reuse of Defence ICT.** 1.1 Defence ICT shall be reused where available. Where appropriate reusable ICT is available but not used justification for this decision must be provided. Use of legacy standards is not enough justification on its own for not reusing ICT. For example, where applicable projects shall consider the following in their solution. a. Technology Architecture – Infrastructure. Defence Information Infrastructure (DII) services shall be progressively adopted as the delivery mechanism for core information services[9] supporting the MOD's business in addition to the joint and combined planning at the strategic and operational levels. Exemption from use of DII-provided core services shall be sought in accordance with 2011DIN05-028. b. Technology Architecture – Network. Defence Fixed Telecommunications System (DFTS) services shall be used for all telephony and WAN services within the UK and UK bases overseas as defined within the DFTS contract. c. Technology Architecture – Network. Paradigm services shall be used for all military satellite services worldwide. d. Technology Architecture – Network. National Allied Long-Lines Agency (NALLA) services shall be used for the provision of terrestrial International Private Leased Circuits (IPLCs) WAN services outside the contractual remit of DFTS. e. Technology Architecture – Network. Defence High Frequency Communications Service (DHFCS) and Very Low Frequency Received Signal Service (VLF RSS) services shall be used for strategic long haul radio (VLF,

[9] Examples of DII core services include: User Access Devices (UADs), e-mail, office automation, Electronic Document Recording and Management (EDRM), application hosting, directories, messaging, web services and browsing.

	LF, HF) services. f. Technology and Application Architecture – The Defence CIS SPOC shall be used for all first line CIS service desk support calls. 1.2 The list above is for illustrative purposes and should not be considered as an exclusive list of ICT for re-use. Note: The Defence Core Network Services (DCNS) change programme will deliver services that will replace those listed above and hence must be consulted to assess any implications for service provision. **2. Reuse of Cross Government ICT and enterprise agreements.** 2.1 Cross Government ICT shall be reused where available in accordance with the Cross Government ICT Strategy. 2.2 Newly developed ICT shall be placed on the Asset and Services Knowledgebase for potential reuse by Other Government Departments.

Development Lifecycle Criteria Evidence

RULE 1 – ICT SHALL BE REUSED WHERE AVAILABLE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Reuse of Defence ICT.	Projects shall confirm if suitable Defence ICT are available. Where no suitable ICT is available this must be recorded in the projects business case. Where applicable reusable ICT is available but not used justification for this decision must be provided.					
2. Reuse of Cross Government ICT and enterprise agreements.	Projects shall interrogate the Asset and Services Knowledge tool and confirm if suitable ICT is available. Where no suitable ICT is available this must be recorded in the projects business case.		Projects shall record any new ICT developed in the Asset and Services Knowledgebase			

RULE 2 – ICT SHALL BE DEVELOPED TO ALIGN WITH THE CROSS GOVERNMENT ICT STRATEGY.	
Rule Owner	DES ISS NTA Architecture (CTO Advisor).
Parent Principle(s)	Coherence, Interoperability, Affordability, Flexibility
Rationale:	To address improve the success of Government ICT programmes in delivering their assumed benefit the Government has published an ICT Strategy which identifies four key themes: Reducing waste and project failure, and stimulating economic growth; Creating a common ICT infrastructure; Using ICT to enable and deliver change Strengthening governance. This strategy applies to all Government ICT procurement. Note: This Rule is intended to ensure the Cross Government ICT Strategy has been considered during ICT development. Some rules within this document already enforce elements of the Strategy. As the implementation and underpinning processes, tools etc of the Strategy mature these will be reflected in later issues of JSP 604.
Policy References:	Cross Government ICT Strategy The Cross-Government ICT Strategy: Implications and Guidance for Defence ICT Projects and Programmes
Subject Matter Expertise POCs:	DES ISS NTA Architecture Team CIO-ISP-POL
Rule Requirements	**1. Cross Government ICT Strategy.** 1.1 Applicable ICT solutions shall be aligned with the Cross Government ICT Strategy.

Development Lifecycle Criteria Evidence

RULE 2 – ICT SHALL BE DEVELOPED WITH RESPECT TO THE CROSS GOVERNMENT ICT STRATEGY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Cross Government ICT Strategy.	Projects shall consider the implications of the Cross Government ICT Strategy during ICT development. Documented evidence of this must be provided to NTA.					

RULE 3 – ICT SHALL BE DEVELOPED WITH RESPECT TO THE RELEVANT DOMAIN ARCHITECTURE.	
Rule Owner	DES ISS NTA Infrastructure Architect.
Parent Principle(s)	Coherence, Feasibility, Interoperability
Rationale:	Defence has a vision of what the future ICT capabilities should look like and needs to make cognisant decisions to converge towards the future state. An architectural approach to engineering ICT solutions is fundamental to deliver this future state
Policy References:	JSP 605 – Defence Enterprise Architecture Policy The Cross-Government ICT Strategy: Implications and Guidance for Defence ICT Projects and Programmes Defence Information Reference Model Fixed Technical Architecture UK MOD Deployed Technical Architecture (DTA)
Subject Matter Expertise POCs:	DES ISS NTA Architect team
Rule Requirements	**1. Architectural compliance** 1.1 ICT shall conform to all technical architectures developed by the relevant authorities using the System of Systems Approach (SOSA). Projects shall obtain compliance approval from each of the relevant Domain Authorities in accordance with JSP 605. NTA is the C4 Domain Architect and as such will review from an end-to-end perspective.

Development Lifecycle Criteria Evidence

RULE 3 – ICT SHALL BE DEVELOPED WITH RESPECT TO THE RELEVANT DOMAIN ARCHITECTURE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Architectural compliance	Projects shall engage with the NTA and relevant domain Architecture authority to determine compliance requirements.		Projects shall obtain acceptance of their ICT preliminary design from the relevant domain architecture authority.	Projects shall obtain acceptance of their ICT design from the relevant domain architecture authority.		
	Projects shall document within the draft SRD the relevant domain architecture requirements.	Projects shall document within the SRD the relevant domain architecture requirements.				

RULE 4 – ICT SHALL BE COMPLIANT WITH QUALITY OF SERVICE (QOS) POLICY.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence
Rationale:	ISS has a responsibility to deliver and manage the Department's funded ICT needs in an efficient and effective manner ensuring that services meet their agreed service levels. One such mechanism is through the definition of a 'Quality of Service' (QoS) policy for IP-based services. IP QoS is the technical ability to allocate network resources to consuming services in an attempt to meet their needs in terms of latency, jitter, loss, errors, bandwidth and availability. In particular IP QoS is required in times of exception where a network is under heavy load or suffering failure.
Policy References:	Currently being drafted
Subject Matter Expertise POCs:	DES ISS NTA Architecture
Rule Requirements	**1. Quality of Service** 1.1 IP based capability shall support QoS through the use of Differentiated Service Code Point (DSCP) in accordance with MOD QoS policy. Design approval shall be obtained from the DES ISS NTA Architects.

Development Lifecycle Criteria Evidence

RULE 4 – ICT SHALL BE COMPLIANT WITH QUALITY OF SERVICE (QOS) POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Quality of Service.	Project shall engage with the NTA to understand the MoD QoS requirements.	Project shall demonstrate understanding of their QoS requirements and engage with the NTA to understand the MoD QoS policy.	Projects shall provide design documentation to show intended compliance with MoD QoS policy. DES ISS NTA Architecture is to approve the projects intended implementation.	Projects shall provide design documentation to show intended compliance with QoS requirements. DES ISS NTA Architecture is to approve the projects intended implementation.		
	Projects shall identify the requirement to implement and test QoS in their draft SRD.	Projects shall identify the requirement to implement and test QoS in their SRD.				
	Projects shall identify the requirement to test QoS operation in their ITEAP.				Projects shall provide evidence obtained through testing on a representative environment that QoS operates as per design requirements.	

RULE 5 – ICT SHALL BE COMPLIANT WITH DOMAIN NAME SYSTEM (DNS) POLICY.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence
Rationale:	DNS is the de facto standard for providing an abstract name-based method for interaction with the IP addressing space.
Policy References:	JSP 457 Volume 1 – IP and DNS
Subject Matter Expertise POCs:	DES ISS NTA Architecture
Rule Requirements	**1. Domain Name System (DNS)** 1.1 Defence ICT shall comply with MOD DNS policy. Projects shall have sought guidance and design approval from the DES ISS NTA Architects.

Development Lifecycle Criteria Evidence

RULE 5 – ICT SHALL BE COMPLIANT WITH DOMAIN NAME SYSTEM (DNS) POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Domain Name System (DNS)	Project shall engage with the NTA to understand the MoD DNS requirements.		Projects shall provide design documentation to show intended compliance with DNS requirements. DES ISS NTA Architecture are to approve the projects intended implementation.	Projects shall provide design documentation to show intended compliance with DNS requirements. DES ISS NTA Architecture are to approve the projects intended implementation.		
	Projects shall identify the requirement to implement and test DNS in their draft SRD.	Projects shall identify the requirement to implement and test DNS in their SRD.				
	Projects shall identify the requirement to test DNS operation in their ITEAP.				Projects shall provide evidence obtained through testing on a representative environment that DNS operates as per design requirements.	

RULE 6 – ICT SHALL BE COMPLIANT WITH INTERNET PROTOCOL (IP) POLICY.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence
Rationale:	Standardisation of network communication protocols, as represented at Layer 3 of the OSI Reference Model, allows for compatibility between any network-connected devices. IPv4 and IPv6 are the de facto standard Layer 3 network protocols. All equipment procured must be capable of supporting IPv6 either now or as a result of an identified manufacturer's roadmap for providing IPv6 capability. However, IPv6 must not be enabled on the network until its use has been sanctioned by Defence policy. A future migration to IPv6 will require careful planning and Defence-wide coordination in order to maintain interoperability and security.
Policy References:	JSP 457 Volume 1 – IP and DNS DIN 2006DIN04-096 – Interim Defence Policy on IPv6
Subject Matter Expertise POCs:	DES ISS NTA Architecture
Rule Requirements	**1. Internet Protocol (IP)** 1.1 Defence ICT shall be IPv4 based and IPv6 compatible in line with MOD policy.

Development Lifecycle Criteria Evidence

RULE 6 – ICT SHALL BE COMPLIANT WITH INTERNET PROTOCOL (IP) POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Internet Protocol (IP)	Project shall engage with the NTA to understand the MoD IP requirements.		Projects shall provide design documentation to show intended compliance with IP requirements. DES ISS NTA Architecture are to approve the projects intended implementation.	Projects shall provide design documentation to show intended compliance with IP requirements. DES ISS NTA Architecture are to approve the projects intended implementation.	.	
	Projects shall identify the requirement to implement and test IP in their draft SRD.	Projects shall identify the requirement to implement and test IP in their SRD.				
	Projects shall identify the requirement to test IP operation in their ITEAP.				Projects shall provide evidence obtained through testing on a representative environment that IP operates as per design requirements	

RULE 7 – ICT SHALL BE COMPLIANT WITH MESSAGING POLICY	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence, Interoperability
Rationale:	SMTP as opposed to X.400 for its primary (or sole) protocol for low/medium grade e-mail messaging. Benefits of Defence-wide use of SMTP include increased interoperability, reduced system complexity, wider vendor/product choice and alignment with de facto international standards and best current practice.
Policy References:	JSP 457 Volume 3 - Messaging
Subject Matter Expertise POCs:	DES ISS NTA Architecture
Rule Requirements	**1. Messaging.** 1.1 Defence ICT shall comply with Messaging policy.

Development Lifecycle Criteria Evidence

RULE 7 – ICT SHALL BE COMPLIANT WITH MESSAGING POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Messaging.	Project shall engage with the NTA to understand the MoD Messaging Policy.		Projects shall provide design documentation to show intended compliance with Messaging Policy. DES ISS NTA Architecture are to approve the projects intended implementation.	Projects shall provide design documentation to show intended compliance with MoD Messaging Policy. DES ISS NTA Architecture are to approve the projects intended implementation.		
	Projects shall identify the requirement to implement and test Messaging in their draft SRD.	Projects shall identify the requirement to implement and test Messaging in their SRD.				
	Projects shall identify the requirement to test IP operation in their ITEAP.				Projects shall provide evidence obtained through testing on a representative environment that messaging services operate as per design requirements.	

RULE 8 – ICT SHALL BE COMPLIANT WITH ELECTRONIC DIRECTORY SERVICES POLICY.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Coherence
Rationale:	An essential enabler of electronic communication is an effective pan-Defence directory service that adheres to common protocols, standards and formats. This requirement is satisfied by the development and maintenance of a Defence wide electronic directory providing ready access to all significant contact information such as messaging, postal and PKI related attributes.
Policy References:	JSP 457: Volume 4 – Directory Services
Subject Matter Expertise POCs:	DES ISS NTA Architecture DE&S D ISS DII Engineering Management
Rule Requirements	**1. Electronic Directory Services** 1.1 Defence ICT shall comply with Electronic Directory Services policy

Development Lifecycle Criteria Evidence

RULE 8 – ICT SHALL BE COMPLIANT WITH ELECTRONIC DIRECTORY SERVICES POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Electronic Directory Services	Project shall engage with the NTA to understand the MoD Electronic Directory Services Policy.		Projects shall provide design documentation to show intended compliance with Electronic Directory Services Policy. DES ISS NTA Architecture are to approve the projects intended implementation.	Projects shall provide design documentation to show intended compliance with MoD Electronic Directory Services Policy. DES ISS NTA Architecture are to approve the projects intended implementation.		
	Projects shall identify the requirement to implement and test Electronic Directory Services in their draft SRD.	Projects shall identify the requirement to implement and test Electronic Directory Services in their SRD.				
	Projects shall identify the requirement to test Electronic Directory Services operation in their ITEAP.				Projects shall provide evidence obtained through testing on a representative environment that electronic directory services operate as per design requirements.	

RULE 9 – ICT SHALL BE DEVELOPED USING THE CROSS DOMAIN SOLUTIONS APPROACH DEFINED BY THE NETWORK TECHNICAL AUTHORITY.	
Rule Owner	DES ISS NTA Network Architect.
Parent Principle(s)	Coherence / Interoperability
Rationale:	ICS in support of the MoD process information of varying levels of sensitivity and provide services of various levels of criticality to the functions of the department. These services operate within broad security domains. A security domain in this context is defined as one where the maximum protective marking of information, the governing security policy and the ownership of Information Services is common. Many capabilities of the MoD's Information and Communications Services require interconnectivity with services external to the security domain in which they operate. Such interconnections represent Cross Domain Solutions (CDS) where security is a critical consideration. The security of a CDS must consider all elements within the end to end solution. As part of that the security capabilities provided at the boundary of the MoD domain represent a primary security capability. Such boundary solutions, sometimes referred to as Gateways are more correctly termed Boundary Protection Services. The provision of CDS and the associated Boundary Protection Services is a complex challenge particularly where the protective marking of involved information is high. All CDS are subject to assessment requirements developed and managed by the NTA Architecture team who must be consulted for all CDS elements of Information and Communications Services provided for the MoD. Key consideration must include the effective identification and management of security threats and risks (link to Rule 10). A CDS is essential in order to ensure that the overall technical architecture of a proposed Information and Communications Service is compatible with achievable CDS capabilities and the delivery of CDS is managed coherently with existing Boundary Protection Services and the overall management of the security status of the domains provided for the MoD. In support of these aims a detailed process for the analysis, design, delivery and in-service management of CDS has been defined by the Network Technical Authority Architecture team and is mandatory for all Cross Domain capabilities provided for the MoD. Evidence that the process has been followed by any CDS included in MoD Information and Communications Services shall be sought from the NTA.
Policy References:	The Cross-Government ICT Strategy: Implications and Guidance for Defence ICT Projects and Programmes Defence Information Reference Model JSP 440 – Defence Manual of Security JSP 457 – Defence Manual of Interoperable Core Network Technologies JSP 906: Design Principles for the Acquisition of Capability
Subject Matter Expertise POCs:	DES ISS NTA Architect – SoSDA Team DES ISS Svc Ops-JCUJCU(Cor) (for the Threat picture) CIO DSAS (for accreditation, as that is their role)
Rule Requirements	**1. Cross Domain Solutions.** 1.1 ICT which is required to exchange information external to the security domain in which it resides shall be developed using the Cross Domain Solutions approach defined by the DES ISS NTA Architect – SoSDA Team. The Cross Domain ICT Architecture shall be owned by the DES ISS NTA Architect – SoSDA Team in the case of high-threat connections or, for lower threat connections and at the discretion of the DES ISS NTA Architect – SoSDA Team, approved by that team. 1.2 ICT shall have Cross Domain Security Threat management processes.

Development Lifecycle Criteria Evidence

RULE 9 – ICT SHALL BE DEVELOPED USING THE CROSS DOMAIN SOLUTIONS APPROACH DEFINED BY THE NETWORK TECHNICAL AUTHORITY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Cross Domain Solutions.	Projects shall engage with the DES ISS NTA Architect – SoSDA Team to adhere to the Cross Domain Solutions Approach. Projects shall have documented in their draft SRD the requirement to comply with the Cross Domain Solutions Approach.	Projects shall maintain engagement with the DES ISS NTA Architect – SoSDA Team to adhere to the Cross Domain Solutions Approach. Projects shall have documented in their SRD the requirement to comply with the Cross Domain Solutions Approach.	Projects shall maintain engagement with the DES ISS NTA Architect – SoSDA Team to adhere to the Cross Domain Solutions Approach. Projects shall have obtained approval of their intended Cross Domain Architecture from DES ISS NTA Architect – SoSDA Team	Projects shall maintain engagement with the DES ISS NTA Architect – SoSDA Team to adhere to the Cross Domain Solutions Approach. Projects shall have obtained approval of their Cross Domain Architecture from DES ISS NTA Architect – SoSDA Team.		
	Projects shall have documented within their Through Life Management Plan the need for Cross Domain Security Threat management.	Projects shall have documented within their Through Life Management Plan the draft Cross Domain Security Threat management process.			Projects shall have documented within their Through Life Management Plan the Issued Cross Domain Security Threat management process.	

Page 26

RULE 10 – ICT SHALL BE SUBJECT TO THREAT, VULNERABILITY & RISK ASSESSMENT IN ACCORDANCE WITH POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security
Rationale:	An initial assessment of the threats and vulnerabilities of any communication or information system/service is a mandatory process in accreditation, without which no such system/service will be allowed to connect to the network. This **must** be the first step taken as it drives all the other Cyber IA functions. All projects will have risks that have been identified as part of their vulnerability assessment and will then be managed in accordance with the appropriate policy having engaged from the outset with the approved accreditor. There is a requirement for this to be done as part of a formal process in the project lifecycle and recorded for scrutiny.
Policy References:	ISO 27001:2005 Control Objectives 5.1.1; 5.1.2; 6.2.1; 8.1.1;10.10.5; 11.4.4; 12.5.4 and 12.6.1 JSP 440 – Defence Manual of Security *JSP 525 Third Edition (23 September 2009) – Corporate Governance & Risk Management* **REPLACED IN JUNE 2010 BY** JSP 892: Risk Management HMG InfoSec No' 1 Issue 3.6 (October 2010) Parts 1 & 2 HMG InfoSec No' 2 Issue 3.2 (January 2010) Part 1 Chapter 2HMG InfoSec No' 2 Issue 3.2 (January 2010) Part 3 Section 3 Paragraph 3.9, Section 4 Paragraph 4.3 and 4.5 HMG InfoSec No' 4 Issue 4.0 (October 2009)
Subject Matter Expertise POCs:	CIO DSAS JCU (CORSHAM) DES ISS NTA Architecture Cyber Defence
Rule Requirements	**1. ICT shall be subject to Threat, Vulnerability & Risk Assessment in accordance with policy.** 1.1 ICT shall be subject to threat, vulnerability and risk assessments as directed by an approved accreditor and JCU (Corsham). Accreditation shall be obtained from the approved accreditor as a result of the assessments and subsequent mitigating actions. 1.2 ICT shall have risk identification, planning, management and reporting processes in place to re-evaluate the threats on an ongoing basis with a minimum gap of 12 months between reassessments. *Additional Notes* *Reassessments can be triggered by a change in threat, vulnerability or architecture. Advice shall be sought from SME's in every case and without exception. In extreme circumstances, resolution of mitigation action to threats/vulnerabilities can be sought through the Risk Balance Case process*[10]*.* *All risks will be regularly reviewed and where technical limitations of the system/service leave it vulnerable to existing threats, it shall be risk balanced against business requirements. Where the residual risk is above the accreditor's risk threshold a Risk Balance Case may be put forward for a resolution by the MoD Chief Information Officer.*

[10] JSP440 Defines the Risk Balance Process.

Development Lifecycle Criteria Evidence

RULE 10 – ICT SHALL BE SUBJECT TO THREAT, VULNERABILITY & RISK ASSESSMENT IN ACCORDANCE WITH POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. ICT shall be subject to Threat, Vulnerability & Risk Assessment in accordance with policy.	Projects shall engage with an approved accreditor and JCU (Corsham) to determine the Threat & Vulnerability analysis requirements. The output shall be outlined in the draft SRD.	Projects shall maintain engagement with an approved accreditor and JCU (Corsham) to determine the Threat & Vulnerability analysis requirements. The output shall be documented in the SRD and Draft RMADS.	Projects shall maintain engagement with an approved accreditor and JCU (Corsham). Threat & Vulnerability analysis requirements are being progressed. The output shall be documented in the Draft RMADS and / or supporting documents.	Projects shall maintain engagement with an approved accreditor and JCU (Corsham). Threat & Vulnerability analysis requirements are being progressed. The output shall be documented in the Draft RMADS and / or supporting documents.	Projects shall provide evidence that Threat & Vulnerability analysis has been undertaken to the requirements of, JCU (Corsham) and an approved accreditor. The output shall be documented in the RMADS and / or supporting documents. Projects shall have obtained an accreditation certificate from the approved accreditor.	
	Project shall engage with approved accreditor and JCU (Corsham) to determine the through life Threat & Vulnerability management requirements	Project shall have a draft through life Threat & Vulnerability management process produced in consultation with an approved accreditor and JCU (Corsham).	Project shall have a published through life Threat & Vulnerability management process produced in consultation with with an approved accreditor and JCU (Corsham).			

RULE 11 – ICT SHALL BE COMPLIANT WITH INFORMATION & NETWORK DEFENCE POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security, Manageability
Rationale:	Monitoring and, where required, reacting to what is occurring on the Network is vital for the protection of information, systems and services in order to ensure their confidentiality, integrity and availability. This includes preventing unauthorised software being introduced into systems/services and protecting the integrity, confidentiality and availability of the systems/service and the information within it. The movement of information is critical to business operations and objectives, therefore the protection of information must be a high priority when designing, building and implementing information systems and services. In order to keep data at rest from being accessed, stolen, or altered by unauthorized entities, security measures such as data encryption and hierarchical password protection are commonly used. For some types of data, specific security measures are mandated by UK law.

Policy References:	ISO 27001:2005 Control Objectives 10.7.1, 10.7.2, 10.7.4, 10.8.3, 10.8.4, 11.6.1; 11.7.1 & 11.7.2; 12.3.1 & 12.3.2 JSP 440 – Defence Manual of Security JSP 541 - MoD Information Security and Computer Network Defence – Organisation and Reporting Procedures JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of Regulations for Installation of Communication & Information Systems JSP 490 - Defence Cryptosecurity Operating Instructions JSP 491 - Compendium of Cryptographic Handling Instructions HMG Infosec Standards No' 2, 4 & 5 Defence Information Assurance Notice (DIAN) 13 – MoD Use of Personal Digital Assistants Defence Information Assurance Notice (DIAN) 14 – MoD Compliance Requirements for Commercial Equivalents to Baseline Grade ***- EXTANT*** Defence Information Assurance Notice (DIAN) 15 - Encryption of CIS Media ***- EXTANT*** Encryption of CIS Media (Version 5) DEFSTAN 21-67 – Data Representation Standard DEFSTAN 21-68 –Message Construction DEFSTAN 08-131 – Standards for Inter-System Communications Protocols (Cat 1) DEFSTAN 00-19 – The ASWE Serial Highway (*Maritime Only*) DEFSTAN 00-81 – Tac ISDN Issue 3 STANAG 4631 – Profile for the use of Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME STANAG 5048 – The Minimum Scale of CIS Connectivity for Communications and Information Systems for NATO Land Forces STANAG 5511 – Tactical Data Link – Link 11/Link 11B STANAG 5514 – Tactical Data Broadcasting – Link 14 STANAG 5516 – Tactical Data Exchange – Link 16 CESG Cryptographic Systems for the Protection of Information Marked Restricted: Requirements and Guidance – RESTRICTED Website – login required
Subject Matter Expertise POCs:	CIO DSAS DES ISS SvcOps-JCU Crypto Services for Defence (CSD) DES ISS NTA Architects Cyber Defence
Rule Requirements	**1. Network Defence** 1.1 ICT shall be compliant with the NOA requirements to enable monitoring of information systems/services. ICT must be developed to provide the data feeds as defined by the NOA. **2. Cryptographic Requirements** 2.1 ICT cryptographic requirements shall be in line with Crypto Services for Defence (CSD) policy.

Development Lifecycle Criteria Evidence

.

RULE 11 – ICT SHALL BE COMPLIANT WITH INFORMATION & NETWORK DEFENCE POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1) Network Defence	Projects shall engage with JCU to confirm the requirements to implement CND and Network Monitoring. Projects shall identify in their draft SRD the requirement to comply with MoD policy on CND and Network Monitoring.	Projects shall provide evidence of continued engagement with JCU and the development of CND and Network Monitoring within project documentation. Projects shall identify in their SRD the requirement to comply with MoD policy on CND and Network Monitoring.	Projects shall include in their PDR their intended implementation of CND and Network Monitoring in accordance with JCU requirements.	Projects shall include in their CDR their intended implementation of CND and Network Monitoring in accordance with JCU requirements.	Projects shall provide evidence that CND and Network Monitoring have been implemented to the requirements of JCU.	Projects shall provide evidence from the NOA that their system/service meets the JCU (Corsham) data feed requirements without any adverse effect on performance and security of the MoD Network.
2) Cryptographic Requirements	Projects shall engage with CSD and produce a draft Project Cryptographic Plan. Projects shall identify in their CONUSE the requirement to comply with MoD crypto policy and strategy.	Projects shall engage with CSD and produce a draft Project Cryptographic Plan. Projects shall identify in their SRD the requirement to comply with MoD cryptographic policy and strategy.	Projects shall provide a Project Cryptographic Plan in their PDR documentation in line with CSD requirements.	Projects shall provide a CSD approved Project Cryptographic Plan in their CDR documentation.		

RULE 12 – ICT SHALL BE COMPLIANT WITH IDENTIFICATION AND AUTHENTICATION POLICY	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security.
Rationale:	To ensure the confidentiality and integrity of the network and the information held thereon, all entities are required to be uniquely identifiable, their actions attributable and their identity to be irrefutably authentic. Consistent approach to naming of entities as laid out in Rule 17 will reduce administrative and network resource overheads. Enterprise wide Identification and Authentication combined with Access Control will ensure a secure working environment.
Policy References:	ISO 27001:2005 Control Objectives 11.2.1, 11.4.2, 11.4.3, 11.5.1, 11.5.2 & 11.5.3 JSP 440 – Defence Manual of Security JSP 457 Vol 5 PKI – not yet issued HMG InfoSec No' 2 Issue 3.2 (January 2010) HMG InfoSec No' 7 Issue 1.0 (October 2010)
Subject Matter Expertise POCs:	DES ISS NTA CYBER DEFENCE
Rule Requirements	**1. Identification and Authentication.** 1.1 ICT shall have Identification and Authentication Management to ensure all entities operating on the network can be uniquely identified and authenticated. Approval of the mechanisms to be used shall be obtained from NTA Cyber Architects.

Development Lifecycle Criteria Evidence

RULE 12 – ICT SHALL BE COMPLIANT WITH IDENTIFICATION AND AUTHENTICATION POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Identification and Authentication.	Projects shall engage with NTA Cyber Architecture Team to determine the Identification and Authentication requirements.	Projects shall provide evidence of the development of a NTA Cyber Architecture approved Identification and Authentication plan and controls within their project documentation.	Projects shall provide evidence in their PDR that a NTA Cyber Architecture approved Identification and Authentication control is included.	Projects shall provide evidence in their CDR that a NTA Cyber Architecture approved Identification and Authentication control is included.		
	Projects shall identify the requirement to implement and test Identification and Authentication in their draft SRD.	Projects shall identify the requirement to implement and test Identification and Authentication in their SRD.				
	Projects shall identify the requirement to test Identification and Authentication operation in their ITEAP.				Projects shall provide evidence through testing that Identification and Authentication controls operate to the requirements of the NTA Cyber Architecture Team.	

RULE 13 – ICT SHALL BE COMPLIANT WITH ACCESS CONTROL POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security
Rationale:	In order to ensure against the loss of information or abuse of network resources, access control needs to be applied. Only authorised entities, as defined in Rule 12, are to be allowed access to those network resources and information for which they have permission. Projects that deliver communication and information systems or services will ensure that access[11] to those systems or services by any entities[12] are strictly controlled.
Policy References:	ISO 27001:2005 Control Objectives 11.1.1, 11.2 (all), 11.4.2., 11.4.3, 11.5.4, 11.5.5, 11.5.6 JSP 440 – Defence Manual of Security HMG Infosec Standards No' 1 HMG InfoSec No' 2 Issue 3.2 (January 2010) Part 3 Section 3 Paragraph 3.9 &Section 4 Paragraph 4.3 HMG InfoSec No' 4 Issue 4.0 (October 2009)
Subject Matter Expertise POCs:	DES ISS NTA Cyber Architecture JCU (CORSHAM) NOA CIO DSAS
Rule Requirements	**1. Access Control** 1.1 ICT shall have approved access control mechanisms. Approval of these mechanisms must be obtained from DES ISS NTA Cyber Architecture Team.

[11] Access is defined as any means by which an entity can interact with the communication and information system/service.
[12] An entity is defined as anything that is capable of operating on the network, such as a person, a router, an application or a service.

Development Lifecycle Criteria Evidence

RULE 13 – ICT SHALL BE COMPLIANT WITH ACCESS CONTROL POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Access Control	Projects shall engage with NTA Cyber Architecture Team to determine the Access Control requirements.	Projects shall provide evidence of a draft Access Control Policy developed in consultation with NTA Cyber Architecture Team.	Projects shall provide evidence of an Access Control Policy developed in consultation with NTA Cyber Architecture Team.	Projects shall provide evidence of an Access Control Policy approved by an accreditor.		
	Projects shall identify the requirement to implement and test Access Control in their draft SRD.	Projects shall identify the requirement to implement and test Access Control in their SRD.				
	Projects shall identify the requirement to test that Access Control operation in their ITEAP.				Projects shall provide interpreted test evidence that Access Control operates in accordance with their Access Control Policy. Acceptance of this evidence shall be obtained from NTA Cyber Architecture Team.	

RULE 14 – ICT SHALL BE COMPLIANT WITH SECURE SYSTEM MANAGEMENT POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security, Manageability
Rationale:	Systems and services follow a distinct lifecycle during which there are many occasions when both the threat/vulnerability to the system/service and/or the business requirements of that system/service change. It is the responsibility of the SRO of the system/service to ensure that security of those systems/services are maintained to the appropriate level through such mechanisms as patch management, through life vendor support etc In order to maintain effective control of changes to network resources and information, it is essential to be able to know what information assets are on the network; what their original status was and what business value and criticality has been attributed (as defined in Rule 17).
Policy References:	ISO 27001:2005 Control Objectives (6.1.7); 9.2.4; 10.3.1; 10.1.2; 10.4.1; 10.4.2; 12.5.1; 12.5.2; 12.5 3; 12.6.1 JSP 440 – Defence Manual of Security Part 3 Chapter 2 paragraph 10 & 11 Part 5 Section 4 Chapter 1 paragraph 17-20 & Annex A Part 5 Section 5 Chapter 1 & Chapter 2 Part 7 Section 2 Chapter 2 Part 8 Section 1 Chapter 2 Part 8 Section 2 Chapter 2 & Chapter 3 Part 8 Section 4 Chapter 1, Chapter 2 & Chapter 3 Part 8 Section 6 Chapter 2 & Chapter 3 Part 9 Chapter 4 JSP 541 - MoD Information Security and Computer Network Defence – Organisation and Reporting Procedures
Subject Matter Expertise POCs:	DES ISS SvcOps - JCU DES ISS Service Ops
Rule Requirements	**1. Secure System Management** 1.1 ICT shall have Secure System Management in place in accordance with policy that is approved by JCU(Corsham).

Development Lifecycle Criteria Evidence

RULE 14 – ICT SHALL BE COMPLIANT WITH SECURE SYSTEM MANAGEMENT POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Secure System Management	Projects shall engage with JCU to determine the requirement to demonstrate that ICT they are responsible for will be managed throughout its life and maintained securely in accordance with policy.	Projects shall provide evidence of continued engagement with JCU and the development of secure system management controls within project documentation.	Projects shall show in their PDR that secure data & system management controls are planned to be implemented to the satisfaction of JCU.	Projects shall show in their CDR that secure data & system management controls are planned to be implemented to the satisfaction of JCU.	Projects shall have obtained acceptance from JCU that the ICT they are responsible for is managed throughout its life and maintained securely in accordance with policy.	

RULE 15 – ICT SHALL BE COMPLIANT WITH ACCOUNTABILITY AND AUDIT POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security.
Rationale:	In the event of any type of incident occurring, the use of entity[13] accounting and audit information logs[14] assists the identification and resolution of such incidents. Projects must plan appropriate entity accounting and audit control measures to provide the necessary information required for incident resolution. Audit and accounting information can also be used to fulfil the information requirements of Network Performance Monitoring. This can include a capability for providing forensic evidence in the event the incident was of a criminal nature. Accounting and audit controls should be planned and resourced in a proportionate manner to the business value and criticality of the information assets it is protecting.
Policy References:	ISO 27001:2005 Control Objectives 10.10.1, 10.10.2, 10.10.3, 10.10.4, 11.4.7, 13.1.1, 13.2.3 JSP 440 – Defence Manual of Security Part 8 Section 1 Chapter 1 (paragraph 36) Part 8 Section 1 Chapter 3 (paragraph 45) Part 8 Section 4 Chapter 1 (paragraph 48, 82-99, Annex A paragraphs 9-11 & 21c & Appendix 1 to Annex A paragraph 1d) Part 8 Section 6 Chapter 3 Paragraph 4f & 10 JSP 541 - MoD Information Security and Computer Network Defence – Organisation and Reporting Procedures HMG InfoSec No' 2 Issue 3.2 (January 2010) Part 3 (Section 3 Paragraph 3.9 & 4.1-4.4) ISO/IEC 27004:2009 Information Technology 0 Security techniques – Information security management - Measurement
Subject Matter Expertise POCs:	JCU (CORSHAM) DES ISS Service Ops DES ISS NTA Architects Cyber Defence
Rule Requirements	**1. Audit & Accountability** 1.1 ICT shall have audit and accountability mechanisms approved by NTA Cyber Architecture Team to log and check activities carried out by any entity on the network in accordance with the requirements of DES ISS SvcOps-JCU.

[13] An entity is defined as anything that is capable of operating on the network, such as a person, a router, an application or a service.
[14] Logging information would be details of entity activity on operating system logs, device access logs and firewall activity logs.

Development Lifecycle Criteria Evidence

RULE 15 – ICT SHALL BE COMPLIANT WITH AUDIT AND ACCOUNTABILITY POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Audit & Accountability	Projects shall engage with NTA Cyber Architecture Team on approved auditing and accounting controls.	Projects shall provide evidence of the development of accounting and audit controls within project documentation.	Projects shall show in their PDR that accounting and audit controls are to be implemented iaw NTA Cyber Architecture Team approved methods.	Projects shall show in their CDR that accounting and audit controls are to be implemented iaw NTA Cyber Architecture Team approved methods.		
	Projects shall identify the requirement to implement and test accounting and audit controls in their draft SRD.	Projects shall identify the requirement to implement and test accounting and audit controls in their SRD.				
	Projects shall identify the requirement to test accounting and audit controls operation in their ITEAP.				Projects shall have demonstrated through testing that accounting and audit controls have been implemented iaw NTA Cyber Architecture Team approved methods.	

RULE 16 – ICT SHALL BE COMPLIANT WITH ICT CONTINGENCY PLANNING POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security.
Rationale:	To minimise disruptions to business activities and to protect critical business information from the effects of major failures of information systems or disasters and to ensure the integrity and availability of that information upon recovery. ICT is essential to business success, so it is critical that systems and services are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures and technical measures that can enable ICT to be recovered as quickly, effectively and securely as possible following a service disruption.
Policy References:	ISO 27001:2005 Control Objectives 10.5.1, 14.1.1, 14.1.2, 14.1.3, 14.1.4, 14.1.5 JSP 440 – Defence Manual of Security JSP 441 - Defence Records Management Policy & Procedures JSP 491 - Compendium of Cryptographic Handling Instructions JSP 503: Business Continuity Management HMG Information Standards No' 2 Part 3 (paragraph 3.9 &Section 4 Paragraph 4.3) ISO/IEC 24762:2008, Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
Subject Matter Expertise POCs:	JCU (CORSHAM) DES ISS Service Ops DES ISS NTA Architects Cyber Defence CIO DSAS
Rule Requirements	**1. Contingency Planning.** 1.1 ICT shall have approved mechanisms to securely backup information and enable its restoration in the event of business interruptions or disasters. These mechanisms must be approved by NTA Cyber Architecture Team.

Development Lifecycle Criteria Evidence

RULE 16 – ICT SHALL BE COMPLIANT WITH ICT CONTINGENCY PLANNING POLICY.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Contingency Planning.	Projects shall engage with DES ISS NTA Cyber Architecture Team to determine backup and recovery control requirements.	Projects shall provide evidence of the development (in consultation with NTA Cyber Architecture Team) of information backup and recovery controls within project documentation.	Projects shall show in their PDR that NTA Cyber Architecture Team approved information backup and recovery controls are to be implemented.	Projects shall show in their CDR that NTA Cyber Architecture Team approved information backup and recovery controls are to be implemented.		
	Projects shall have identified the requirement to implement information backup and recovery controls within their draft SRD.	Projects shall have identified the requirement to implement information backup and recovery controls within their SRD.				
	Projects shall identify the requirement to test backup and recovery operation in their ITEAP.				Projects shall demonstrate through testing that their backup and recovery controls operate as per approved NTA Cyber Architecture Team method.	

RULE 17 – ICT SHALL BE COMPLIANT WITH INFORMATION ATTRIBUTE MANAGEMENT POLICY.	
Rule Owner	DES ISS NTA CYBER DEFENCE
Parent Principle(s)	Security.
Rationale:	The objective is to ensure that entities[15] and information are labelled and identified so that information is accessed by those who have permission. This applies to all the attributes and associations of all MoD entities and information. It allows them to be defined in terms of their value, legal requirements, sensitivity or criticality to the organisation.
Policy References:	ISO 27001:2005 Control Objectives 7.2.1 & 7.2.2 JSP 329 Chapter 2 & Chapter 5 JSP 440 – Defence Manual of Security Part 3 Chapter 4 (paragraphs 3 & 11) Part 4 Chapter 6 (paragraph 13) Part 5 Section 5 Chapter 1 (paragraph 3) Part 5 Section 1 Chapter 2 Part 5 Section 5 Chapter 1 (paragraph 1) Part 5 Section 1 Chapter 2 (paragraphs 1,2 & 4-7) Part 8 Section 1 Chapter 1 (paragraph 29) Part 8 Section 2 Chapter 1 (paragraph 11, 17 & 33) Part 8 Section 2 Chapter 4 (paragraph 13) Part 8 Section 3 Chapter 1 (paragraph 2 & 15-16) Part 8 Section 3 Chapter 2 Part 8 Section 4 Chapter 3 (paragraph 35) Part 8 Section 4 Chapter 4 (paragraphs 20,24, 47-48, 54 & 63) Part 8 Section 5 Chapter 5 (paragraph 9 & Annex B paragraphs 3-4) Part 9 Chapter 3 (paragraph 13) JSP 457 Vol 7 Labelling JSP 717: Using the MOD Metadata Standards HMG InfoSec No' 6 (March 2009)
Subject Matter Expertise POCs:	DES ISS NTA Architects Cyber Defence MoD CIO
Rule Requirements	**1. Information Management** 1.1 ICT shall have attribute definition and association controls so information receives an appropriate level of protection and control in accordance with the MoD Protective Marking Scheme. 1.2 ICT shall have mechanisms to verify the information has not been altered by unauthorised entities and that the integrity of the data can be verified,

[15] An entity is defined as anything that is capable of operating on the network, such as a person, a router, an application or a service.

Development Lifecycle Criteria Evidence

RULE 17 – ICT SHALL BE COMPLIANT WITH INFORMATION ATTRIBUTE MANAGEMENT POLICY.						
Rule Requirement	Initial Gate	Main Gate	PDR	CDR	TRRA	AtO
1. Information Management	Projects shall engage with NTA Cyber Architecture Team to determine the requirements for attribute definition and association controls.	Projects shall provide evidence of the development of attribute definition and association controls within project documentation.	Projects shall show in their PDR that attribute definition and association controls are to be implemented.	Projects shall show in their CDR that attribute definition and association controls are to be implemented and they have been approved by the NTA Cyber Architecture Team.	Projects shall have demonstrated through testing that attribute definition and association controls operate as approved by the NTA Cyber Architecture Team.	
	Projects shall have identified the requirement to implement attribute definition and association controls within their CONUSE.	Projects shall have identified the requirement to implement attribute definition and association controls within their SRD.				
	Projects shall identify the requirement to test attribute definition and association control operation in their ITEAP.				Projects shall have demonstrated through testing that attribute definition and association controls operate as approved by the NTA Cyber Architecture Team.	

RULE 18 – ICT SHALL BE DEVELOPED AND ITS PERFORMANCE DEMONSTRATED WITH RESPECT TO THE ENVIRONMENT IN WHICH IT WILL OPERATE.	
Rule Owner	DES ISS NTA Architecture - InnTI
Parent Principle(s)	Usability, Feasibility
Rationale:	It is essential that ICT is developed with respect to the environmental constraints and limitations it will operate in. This environment will have a bearing on a solution being able to deliver the performance expected of it. This is of particular importance in the Deployed Environment where networks often have high latency and low bandwidth. In conjunction with understanding the environment the solution must be properly defined in terms of use, information exchange requirements and performance. Without these being properly defined a solution cannot be developed, tested and demonstrated against them. The impact of new or changed ICT on the performance of other capabilities must be quantified and accepted. Any new or changed ICT will have an impact on other capabilities where there is a use of common resources. This impact must be understood to allow informed decisions on whether it is accepted.
Policy References:	Not Applicable
Subject Matter Expertise POCs:	DES ISS NTA Architecture – InnTI team
Rule Requirements	**1. ICT shall be developed and its performance demonstrated with respect to the following being defined and documented.** 1.1 Definition of how ICT is to be used / employed and the Information Exchange Requirements to be supported. 1.2 Quantification of the required network characteristics (to include, but not be limited to: bandwidth, latency, jitter, packet loss). 1.3 The capability's operational and technical architecture shall be documented and maintained. 1.4 Performance metrics shall be defined. 1.5 The ICT environment characteristics (to include but not be limited to: bandwidth, latency, jitter, traffic, security) within which it will operate shall be understood. **2. ICT performance shall be demonstrated.** 2.1 ICT performance shall be demonstrated under Normal[16] operating conditions. 2.2 ICT performance shall be demonstrated under less than ideal conditions; this may be the result of insufficient bandwidth, high latency or jitter. The boundary of unacceptable ICT performance must be identified 2.3 The above shall be demonstrated through: 2.3.1 Prediction of expected performance based on modelling and characterisation 2.3.2 Testing in a representative environment. 2.3.3 Analysis of 'experienced against predicted' performance on the live environment. **3. ICT impact on the existing environment shall be demonstrated and quantified.** 3.1 Evidence that delivery of ICT does not have an unacceptable operational impact on other capabilities. This shall be demonstrated through:

[16] Normal operating conditions will be determined when the environment within which ICT is operated is understood and how the ICT will be used has been defined.

	3.1.1 Prediction of expected impact based on modelling and characterisation. 3.1.2 Testing the capability in a representative environment. 3.1.3 Analysis of ‘experienced against predicted’ performance on the live environment.

Development Lifecycle Criteria Evidence

RULE 18 – ICT SHALL BE DEVELOPED AND PERFORMANCE DEMONSTRATED WITH RESPECT TO THE ENVIRONMENT IN WHICH IT WILL OPERATE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. ICT shall be developed and performance demonstrated with respect to the following being defined and / or documented.	Projects shall define and document how the system/service is to be employed in the CONEMP.	Projects shall define and document how the system/service is to be employed (locations, no of users) in the CONUSE. CONUSE maintained in line with changes in requirements.				
	Projects shall define and document the system/service Information Exchange Requirements.		Projects shall define and document the Information Exchange Requirements accepted by delivery partners. IERs shall be maintained in line with changes in requirements.			
	Projects shall undertake an Initial assessment of required network resources.		Projects shall undertake assessment(s) of network resources of proposed systems/services. The assessment(s) shall be supported by evidence from modelling/ application characterisation.		Projects shall undertake assessment(s) of network resources. This assessment shall be supported by evidence from testing on a representative test environment to confirm the previous modelling work.	
	Projects shall develop and document the system/service Operational Architecture.	Projects shall develop and document the system/service Technical Architecture.	Projects shall maintain the system/service Technical Architecture documentation.	Projects shall freeze the system/service Operational and Technical Architecture and documentation.		
	Projects shall define Key system/service performance	Projects shall define Key system/service performance	Projects shall have defined performance metrics. Contracts			

RULE 18 – ICT SHALL BE DEVELOPED AND PERFORMANCE DEMONSTRATED WITH RESPECT TO THE ENVIRONMENT IN WHICH IT WILL OPERATE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
	requirements in the URD.	requirements in the SRD.	with delivery partners shall state required system and service performance requirements			
	Projects have documented the characteristics (to include but not be limited to: latency, bandwidth, jitter, security) of the intended ICT environment(s).					
2. ICT performance shall be demonstrated.	Projects shall identify the requirement to assess ICT performance by: analysis of solution(s), demonstration through representative environment testing and proving on the live environment. This shall be recorded in their ITEAP and planned to be undertaken. Projects have performed high level analysis of environment(s) characteristics to confirm they can support the solution.		Projects shall identify the requirement to assess ICT performance by demonstration through representative environment testing and proving on the live environment. This shall be recorded in their ITEAP and planned to be undertaken. Projects have performed detailed analysis of environment(s) characteristics to confirm they can support the solution. This analysis may be supported by modelling and characterisation.		Projects shall identify the requirement to assess ICT performance by monitoring on the live environment. This shall be recorded in their ITEAP and planned to be undertaken. Projects shall have undertaken Testing on a representative test environment and demonstrated the performance requirements can be achieved.	Projects shall have undertaken performance monitoring to demonstrate actual performance on the live environment.
3. ICT impact on the existing environment shall be demonstrated	Projects shall identify the requirement to assess the impact on the existing environment through prediction of expected impact based on modelling and characterisation analysis, demonstration through representative		Projects shall identify the requirement to assess the impact on the existing environment through demonstration through representative environment testing and proving on the live environment. This shall be recorded in their		Projects shall identify the requirement to assess the impact on the existing environment by	Projects shall have undertaken performance monitoring to quantify the impact on the live

RULE 18 – ICT SHALL BE DEVELOPED AND PERFORMANCE DEMONSTRATED WITH RESPECT TO THE ENVIRONMENT IN WHICH IT WILL OPERATE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
and quantified	environment testing and proving on the live environment. This shall be recorded in their ITEAP and planned to be undertaken. *Note: From Q1 2013 ISS Svc Ops will have the ability to model the deployed environment and will be available to predict network resource utilisation with the introduction of new capabilities. Project teams shall request support through Svc Ops, SOI tbc.*		ITEAP and planned to be undertaken. *Note: From Q1 2013 - Once a capability is characterised it shall be modelled by ISS Svc Ops to provide supporting evidence regarding how it will affect the deployed environment.*		monitoring on the live environment. This shall be recorded in their ITEAP and planned to be undertaken. Projects shall have undertaken Testing on a representative test environment and demonstrated there will not be a significant impact on the existing ICT environment.	environment.

RULE 19 – ICT SHALL HAVE SUITABLE REPRESENTATIVE TEST ENVIRONMENTS (RTE) AVAILABLE TO ENABLE THROUGH LIFE TESTING TO BE CONDUCTED.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Usability, Interoperability, Manageability, Supportability, Feasibility
Rationale:	Without suitable representative test environments new or changed ICT cannot be tested to understand its impact on existing ICT or its performance alongside it.
Policy References:	None
Subject Matter Expertise POCs:	DES ISS NTA Architecture – InnTI team
Rule Requirements	**1. Representative Test Environment.** 1.1 Suitable Representative Test Environments shall be available and endure for the life of the ICT it supports. Use of existing Defence Test Facilities shall be exploited where available.

Development Lifecycle Criteria Evidence

RULE 19 – ICT SHALL HAVE SUITABLE REPRESENTATIVE TEST ENVIRONMENTS AVAILABLE TO ENABLE THROUGH LIFE TESTING TO BE CONDUCTED.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1) Representative Test Environment	The project shall acknowledge the need for a suitable representative test environment. This RTE shall be utilised to demonstrate performance and impact. This shall make maximum use of existing Defence test facilities and cover the provision of any additional resources for these facilities to meet this requirement. This capability shall be enduring to enable through life testing of changes. This capability shall be identified in the ITEAP and draft SRD.		The project shall produce a maturing design for the test environment, including any capability upgrade. This shall be documented in the ITEAP.	The project shall have developed a mature ITEAP document that includes the proposedTest Architecture; Test capabilities should be available and suitably augmented to deliver the testing.	The project shall ensure that a representative test environment is available as a through life capability to support the change management process.	

RULE 20 – ICT SHALL BE DESIGNED TO PERMIT HOLISTIC NETWORK SERVICE MANAGEMENT.	
Rule Owner	NOA
Parent Principle(s)	Manageability
Rationale:	The Defence Network is a complex system of systems with multiple commercial and technical boundaries that underpins almost all the Capabilities delivered by Defence. Without a cohesive approach to Network Management, a project may inadvertently introduce vulnerability in another part of the Network that may degrade the service delivered. This is not unique to Defence and most enterprise IT organisations are adopting similar approaches allowing them to apply Service Management and Deter, Detect, Defend, Respond or Recover to any incident.
Policy References:	None
Subject Matter Expertise POCs:	DES ISS Svc Ops – Ops Team
Rule Requirements	**1. Service Asset and Configuration Management (SACM)** 1.1 ICT shall be such that SACM is integral to the design and the data held is relevant, accurate, and appropriately presented to the NOA Configuration Management System (CMS). **2. Change Management** 2.1 ICT shall have appropriate change management procedures established. They shall include change categorisation and a RACI (Responsible, Accountable, Consulted, Informed) matrix. Formal change evaluation must be mandated for major changes with potential impact beyond the boundary of the project. **3. Knowledge Management** 3.1 ICT shall be such that appropriate knowledge transfer to the NOA Service Knowledge Management System (SKMS) during service transition is possible. **4. Event Management** 4.1 ICT shall be designed to ensure appropriate event activity can be managed/configured/received by the NOA toolset. **5. Service Management toolset** 5.1 ICT shall be designed to ensure appropriate data flow integration with the NOA Service Management toolset; to include incident/problem management work flows and service dashboard presentation, where appropriate.

Development Lifecycle Criteria Evidence

RULE 20 – ICT SHALL BE DESIGNED TO PERMIT HOLISTIC NETWORK SERVICE MANAGEMENT.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Service Asset and Configuration Management	Projects shall engage with the NOA and include agreed SACM requirements in the draft SRD.	Projects shall engage with the NOA and include agreed SACM requirements in their SRD, including appropriate data presentation to the NOA CMS	Projects shall draft their SACM Plan. It shall include: • scope/scale and characterisation of Configuration Items (CIs) • Configuration Management DataBase (CMDB) design • Configuration control mechanisms • Data presentation to the NOA CMS	Projects shall have produced their SACM Plan. It shall include: • scope/scale and characterisation of CIs • CMDB design • Configuration control mechanisms • Data presentation to the NOA CMS • Projects shall ensure that SACM considerations are included in the ITEAP	The project shall make Testing and Evaluation reports for CMDB, including verification of integration with NOA CMS available. The project shall establish the Initial configuration baseline including relational dependencies. The project shall confirm the appropriate Knowledge transfer to NOA Service Ops staff	The project shall produce an evaluation report, including: • review of configuration control mechanisms • validity of scope/scale and characterisation of CIs • Integrity of baseline vs snapshot
2. Change Management	Projects shall engage with the NOA and include agreed Change management requirements in the draft SRD.	Projects shall engage with the NOA and include agreed Change management requirements in their SRD.	Projects shall draft their Change Management Plan. It shall include: • Stakeholder analysis • Accountabilities and responsibilities assigned to roles • Identification, classification, assessment, and	Projects shall have change management procedures produced, to include: • Stakeholder analysis • Accountabilities and responsibilities assigned to roles • Identification, classification, assessment, and	Projects shall have NOA endorsed change management procedures, to include: • Stakeholder analysis • Accountabilities and responsibilities assigned to roles • Identification, classification, assessment, and	Projects shall produce an Evaluation report, including: • unauthorised changes • emergency fixes • Change success rate • Remediation work • Failed changes • Incidents attributed

			evaluation • Remediation planning	evaluation • Remediation planning	evaluation • Remediation planning Confirmation of appropriate Knowledge transfer to NOA Service Ops staff	to changes
3. Knowledge Management	Projects shall engage with the NOA and include agreed Knowledge management requirements in the draft SRD.	Projects shall engage with the NOA and include agreed Knowledge management requirements in their SRD.	Projects shall have a Knowledge management plan drafted, to include: • Stakeholder analysis • Mechanisms/ procedures for knowledge transfer to service operations staff (inc GOSCC) during service transition	Projects shall have a Knowledge management plan produced, to include: • Stakeholder analysis • Mechanisms/ procedures for knowledge transfer to service operations staff (inc GOSCC) during service transition	Projects shall have an Appropriate, NOA endorsed knowledge transfer to the NOA SKMS, to include: • SACM • Change Management • Event Management • Support Solution Envelope, iaw ISSP 154	Projects shall produce an Evaluation report, including: • Identified knowledge gaps by Service Ops staff • Number of incidents caused by 'lack of user knowledge'
4. Event Management	Projects shall engage with the NOA and include agreed Event management requirements in the draft SRD.	Projects shall engage with the NOA and include agreed Event management requirements in their SRD, including Integration with the NOA service management toolset	Projects shall have an Event management plan drafted, to include: • Appropriate thresholds • Instrumentation, • categorisation, correlation, and response • Integration with the NOA service management	Projects shall have an Event management plan produced, to include: • Appropriate thresholds • Instrumentation, • categorisation, correlation, and response • Integration with the NOA service management	Projects shall provide Testing and Evaluation reports for Event management, including verification of integration with NOA service management toolset Confirmation of appropriate Knowledge transfer to NOA Service Ops staff	Projects shall produce an Evaluation report, including: • review of event management mechanisms • validity of thresholds • Effectiveness of Instrumentation, categorisation, correlation, and response

			toolset	toolset • Event management considerations included in the ITEAP		
5. Service Management toolset integration	Projects shall engage with the NOA and include agreed Service management toolset integration requirements in the draft SRD.	Projects shall engage with the NOA and include agreed Service management toolset integration requirements in their SRD, including: • Open interfaces to industry standards • Workflow or process control (including Incident, Problem, Change) • Reporting capabilities • Dashboard capabilities (where appropriate)	Projects shall have a Service management toolset integration plan drafted, to include: • interface standards • Workflow or process control (including Incident, Problem, Change) • Reporting processes • Dashboard capabilities (where appropriate)	Projects shall have a Service management toolset integration plan produced, to include: • interface standards • Workflow or process control (including Incident, Problem, Change) • Reporting processes • Dashboard capabilities (where appropriate) Service management toolset integration considerations included in the ITEAP	Projects shall provide Testing and Evaluation reports verifying integration with NOA service management toolset Confirmation of appropriate Knowledge transfer to NOA Service Ops staff	Projects shall produce an Evaluation report, including: • Effectiveness of workflow and process control • Reporting and Dashboard presentation

RULE 21 – ICT SHALL HAVE DEFINED SUPPORT ARRANGEMENTS.	
Rule Owner	NOA
Parent Principle(s)	Sustainability
Rationale:	ICT should have then necessary funded support arrangements in place to satisfy the customers requirements for levels of service. Support arrangements should be considered from the earliest stages of the project lifecycle. Gartner have identified that, on average, the cost to maintain an application for a service life of 5 years accounts for 40% of the total cost of ownership. With increasing financial constraints, Defence must ensure that the logistics burden of its ICT is minimized.
Policy References:	ISSP 154 ISS Release Process and Deployment Process
Subject Matter Expertise POCs:	DES ISS Svc Ops – Ops Team
Rule Requirements	**1. Support Arrangements** 1.1 ICT shall be coherent with ISSP 154 and DES ISS SvcOps GOSCC shall be furnished with the necessary service support wrap information.

Development Lifecycle Criteria Evidence

RULE 21 – ICT SHALL HAVE DEFINED SUPPORT ARRANGEMENTS.						
Rule Requirements	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Support Arrangements	Projects shall engage with the NOA to ensure that the Service Support requirements identified in ISSP 154 are considered throughout the project lifecycle. Projects shall ensure that Service Support requirements are identified in the URD.	Projects shall continue their engagement with the NOA to ensure that the Service Support requirements identified in ISSP 154 are considered throughout the project lifecycle. Projects shall ensure that Service Support requirements are identified in SRD.	Projects shall continue their engagement with the NOA to ensure that the Service Support requirements identified in ISSP 154 are considered throughout the project lifecycle. Projects shall ensure that Service Support Plan drafted, to comply with ISSP 154.	Projects shall continue their engagement with the NOA to ensure that the Service Support requirements identified in ISSP 154 are considered throughout the project lifecycle. Projects shall ensure that Service Support Plan is produced, to comply with ISSP 154.	Projects shall continue their engagement with the NOA to ensure that the Service Support requirements identified in ISSP 154 are approved by the NOA. Projects shall ensure that a NOA endorsed ISSP 154 annex A is produced and captured in the NOA SKMS. Projects shall ensure that support for their capability is funded through life.	Projects shall undertake a review of their Service Support arrangements with the NOA to ensure that they are appropriate through life. Evaluation report of the service support wrap, including: • Recorded gaps in the support arrangements. Projects shall demonstrate that support for their capability is funded through life.

RULE 22 – ICT SHALL BE DEVELOPED TO MEET THE AGREED INSTALLATION REQUIREMENTS.	
Rule Owner	CIO-DSAS-CIDA
Parent Principle(s)	Security, Usability
Rationale:	All capability providers must develop and maintain physical and environmental CIS design and installation documentation, appropriate to the required level of confidentiality, integrity and availability as defined by the Co-ordinating Installation Design Authority (CIDA) in JSP 480. Defence CIDA is mandated with the responsibility for optimising the maintenance of operational capability, flight safety and electrical security by co-ordinating changes into MOD CIS facilities and by regulating installation standards. CIDA authority applies to all sites, buildings, rooms and mobile/transportable equipment facilities but not to aircraft, ships or submarines.
Policy References:	JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of regulations for installation of communication & information systems
Subject Matter Expertise POCs:	**CIO-DSAS-CIDA** E-mail: CIO-DSAS-CIDA (MULTIUSER)
General	**1. CIDA Design Conformance** 1.1 ICT shall conform with CIDA design approval in accordance with JSP 480 before proceeding with installations

Development Lifecycle Criteria Evidence

RULE 22 – ICT SHALL BE DEVELOPED TO MEET THE AGREED INSTALLATION REQUIREMENTS.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. CIDA Design Conformance	Projects shall define the physical ICT requirements to the Defence CIDA		Projects shall obtain generic ICT design assurance from CIO-DSAS-CIDA.	Projects shall obtain generic ICT design assurance from CIO-DSAS-CIDA.	Projects shall obtain installation conformance assurance from CIO-DSAS-CIDA.	

RULE 23 – ICT SHALL HAVE APPROPRIATE SOFTWARE LICENSES PROCURED AND MANAGED THROUGH LIFE.	
Rule Owner	DES ISS NTA Architecture
Parent Principle(s)	Manageability, Legality
Rationale:	Software Licensing requirements must be adhered to through life or Defence could be using software illegally and subject to vendor claims. Software licensing is a contract of agreement between the software publisher and the end user, sometimes referred to as the End User License Agreement (EULA). Software licensing protects the copyright by placing restrictions on the end user in relation to the product.
Policy References:	Not Applicable
Subject Matter Expertise POCs:	DES ISS NTA Architecture
Rule Requirements	**1. Software Licenses** 1.1 ICT shall have the appropriate license(s) purchased and managed through life.

Development Lifecycle Criteria Evidence

RULE 23 – ICT SHALL HAVE APPROPRIATE SOFTWARE LICENSES PROCURED AND MANAGED THROUGH LIFE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Software Licences	Projects shall identify the requirement to acquire software licenses.				Projects shall provide evidence that the required software licenses have been acquired.	Projects shall provide evidence that the required software licenses are in force through life.
	Projects shall identify the requirement to manage software licenses through life within the Through Life Management Plan.			Projects shall document how the required software licenses are managed through life within the Through Life Management Plan.		

RULE 24 – ICT SHALL COMPLY WITH SPECTRUM MANAGEMENT REQUIREMENTS.	
Rule Owner	Defence Spectrum Organisation (DSO)
Parent Principle(s)	Interoperability
Rationale:	The DSO is responsible for allocating radio frequencies (RF) for ops, trial and exercise use in the UK by any UK or visiting nation's military equipment that can transmit or receive RF energy (otherwise known as Spectrum Dependent Equipment, or SDE). The DSO also helps to negotiate with host nation spectrum authorities frequencies for use overseas by UK Force Elements (including visiting RN ships). This frequency management discipline is required in order to avoid: • interference between different UK military equipments (e.g. voice communications and UAV downlinks) • interference between UK military equipments and civil or commercial equipments (e.g. Force Protection and mobile phone providers) • congestion of the RF spectrum. *Note: Defence Projects must engage with the DSO through the Network Capability Authority (NCA) as early as practicable in order to register the development of potential spectrum-dependent equipment, and to seek guidance regarding the intended spectrum use.*
Policy References:	JSP 921: Policy for the Management and Use of Electromagnetic Spectrum. JSP 602 Leaflet1038: Radio Frequency and Radio Site Clearance. JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of Regulations for Installation of Communication & Information Systems AOF Systems of Systems Approach (SOSA) Principles and Guidance.
Subject Matter Expertise POCs:	Defence Spectrum Organisation DES SE SEIG-EI-DSO-Mailbox
Rule Requirements	**1. Spectrum** 1.1 ICT shall have Defence Spectrum Organisation approval for any system that utilises electromagnetic transmissions. Projects shall provide evidence to the Network Authorities[17] that they have sought *and complied with* guidance from the DSO regarding all future spectrum requirements, that they have registered the technical details of their SDE, and that they have requested specific operating frequencies through the DSO for both development trials and live operational use (including live exercise use).

[17] Projects will also need to present this evidence to the Investment Approval Authorities. This is not included in the Rule requirement as it is outside of the assurance scope of this document.

Development Lifecycle Criteria Evidence

RULE 24 – ICT SHALL COMPLY WITH SPECTRUM MANAGEMENT REQUIREMENTS.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Spectrum	Projects shall have engaged with the DSO and sought advice regarding the likely suitability and availability of their perceived future Spectrum Requirements.	Projects shall have engaged with the DSO and obtained necessary approval to continue with the development of spectrum-dependent projects.	Projects shall engage with the DSO and provide final details of equipment radio-frequency characteristics (bandwidth, centre frequency, modulation, EIRP etc) when required. This spectrum clearance information must be followed up by individual requests for operating/exercise/trial frequency assignments to cover each actual use of the equipment (including development trials).			

RULE 25 – ICT SHALL COMPLY WITH ELECTROMAGNETIC INTEGRATION REQUIREMENTS.	
Rule Owner	DES D Tech SEIG EI
Parent Principle(s)	Interoperability
Rationale:	To maximise the effect of capabilities it is essential that Electromagnetic Integration aspects are determined early in the projects development and necessary measures are taken to protect Information Communication Technology (ICT) as well as hosted and co-mounter systems. Electromagnetic Integration covers the following areas: Electromagnetic Compatability (EMC) Mutual Interference (MI) Electronic Emission Security (ELSEC) RF Radiation Hazards (RADHAZ) Electromagnetic Pulse Protection (EMPP) Technical Attack Countermeasures (TAC)
Policy References:	JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of Regulations for Installation of Communication & Information Systems
Subject Matter Expertise POCs:	DES SE SEIG EI
Rule Requirements	**1. Electromagnetic Integration** 1.1 ICT shall adhere to Defence Electromagnetic Integration policy.

Development Lifecycle Criteria Evidence

RULE 25 – ICT SHALL COMPLY WITH ELECTROMAGNETIC INTEGRATION REQUIREMENTS.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Electromagnetic Integration	Projects shall have engaged with E3A and determined the necessary Electromagnetic Integration policy that applies.					

RULE 26 – ICT SHALL BE COMPLIANT WITH SAFETY AND ENVIRONMENTAL REQUIREMENTS THROUGH LIFE.	
Rule Owner	DES ISS NTA Coherence
Parent Principle(s)	Safety
Rationale:	Safety Cases contain evidence that the delivered product is safe. Failure to comply with legislation, or follow MoD policy and instructions could lead to inadequate safety cases and hence delivery of unsafe products, equipment or services, with the associated risk of censure or prosecution. A Safety Case must be suitable and sufficient for the particular project or programme. The effort involved in preparing and maintaining the Safety Case shall be commensurate with the level of safety risk. Safety Cases shall be produced by individuals who are suitably qualified and experienced to do so.
Policy References:	SEI No.3 - Acquisition Safety & Environment Mgmt ***– formerly SI 14*** Acquisition Safety & Environmental Management System (ASEMS)
Subject Matter Expertise POCs:	DE&S ISS NTA-Acquisition Safety and Environment Team
Rule Requirements	**1. Safety & Environmental** 1.1 ICT shall comply with Safety Management Requirements Through Life.

Development Lifecycle Criteria Evidence

RULE 26 – ICT SHALL BE COMPLIANT WITH SAFETY AND ENVIRONMENTAL REQUIREMENTS THROUGH LIFE.						
Rule Requirement	**Initial Gate**	**Main Gate**	**PDR**	**CDR**	**TRRA**	**AtO**
1. Safety & Environmental	Projects shall demonstrate the need/ degree of required Safety Case to support Initial Gate Submission.	Projects shall provide evidence that a safety 'expert' has been engaged to support the Main Gate Submission.	Projects shall provide evidence that a Safety Case has been/is being developed by a suitably qualified expert to support PDR.	Projects shall provide evidence of a maturing Safety Case to support CDR.	Projects shall provide evidence of a Safety Case to support entry into service.	

ANNEX A - Principles

The Principles below are based on those contained in The Open Group Architecture Framework (TOGAF). The Defence ICT Guiding Principles in the Defence ICT Strategy should also be referred to as they provide a wider Strategic shaping view.

1. Legality

Statement:
ICT will be compliant with National and International legislation
Rationale:
Defence is increasingly becoming subject to a variety of legislation, both National and International, which was previously ignored on the basis that "Crown Immunity" or the Official Secrets Act exempted compliance. Examples of legislation that must be considered by ICT projects includes such legislation as: Data Protection Act Public Records Acts. Freedom of Information Act Legislation covering the disposal of ICT such as the WEEE directive. Licensing (e.g. Software) Equal opportunities legislation, including disability discrimination. Climate Change and its associated targets for sustainable ICT across government, the introduction of Carbon Accounting, Sustainable Operations on the Government Estate (SOGE) and Sustainable Development in Government (SDiG) targets. Health and Safety legislation.

2. Affordability

Statement:
Defence ICT will be a cost effective solution when considered in both enterprise capability terms and whole life costs.
Rationale:
The procurement of Defence ICT must consider through life affordability of the capability being delivered. It is the responsibility of the sponsor to consider the wider value for money impact of the through life changes and evolution of their capability. Examples of where project decisions may have an effect upon the Defence Enterprise include: • Designing to open standards and open architectures allowing obsolescent components to be replaced easily. • Procuring systems that use proprietary standards or have an aggressive maintenance schedule that is incompatible with the Defence ICT enterprise. • Choosing a lower cost technical solution that places significant overheads on the Network. • Choosing a lower cost technical solution that requires additional items to be put into the logistics chain or requires components to be run longer than originally intended.

3. Feasibility

Statement:
Defence ICT will be designed to accommodate the constraints within which it operates.
Rationale:
There are a number of non-functional requirements and constraints that will affect the feasibility of any system. ICT projects need to identify the relevant constraints and manage solutions so that the effects e.g.latency, are mitigated.

4. Usability

Statement:
Defence ICT will be designed to be capable of operation under accepted conditions
Rationale:
Defence ICT supports military and business activities. Any new ICT must transition into operation smoothly and operate in a way that is consistent with the agreed service levels and agreed operational cost model. Defence ICT may have to support a variety of operational environments. .Defence applications need to work with a variety of underlying services and systems and it is vital that an approach that allows applications to be written once, used anywhere is adopted.

5. Interoperability

Statement:
Defence ICT shall conform to defined standards that promote interoperability for data, software and hardware.
Rationale:
This is a Network Domain specialisation of the SOSA Principle: Designing for Flexible Interoperability. Network interoperability is not a capability in its own right; rather it is a critical enabler for operations and vital to Information Superiority. NATO defines interoperability as the ability of forces and nations to Communicate, Operate, Support, Train and Exercise together in the execution of assigned missions and tasks. . Dir(IS) has recently emphasised the importance of Interoperability stating that while not a DLOD itself, Interoperability covers cross cutting interactions between coalitions, single Services, OGDs and the civil aspects of interoperability. A key strand of the Government ICT strategy is to improve the degree of interoperability by championing the use of open standards in all Government ICT programmes. Mandating the use of open standards will not guarantee interoperability. To avoid the pitfalls of procuring a system that does not fully interoperate with other systems as intended, integration into the System of Systems needs to be considered from project conception.

6. Coherence

Statement:
Defence ICT will be designed to be developed once and used many times without constraining the need for innovation.
Rationale:
This is a Network Domain specialisation of the SOSA principles of minimising diversity and ensuring commonality of services. Duplication of capability is expensive and can create information conflicts. There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs. The business advantages of optimum technical diversity include: standard packaging of components; predictable valuations and returns; standardised testing and management; predictable implementation impact; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale across DLODs. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

7. Manageability

Statement:
Defence needs to manage the network and its components throughout its life.
Rationale:
The Defence Network is a complex system of systems with multiple commercial and technical boundaries that underpins almost all the Capabilities delivered by Defence. Without a unified approach to the operation and defence of the Network, a project may inadvertently degrade the services provided and / or introduce vulnerabilities.

8. Security

Statement:
Defence ICT will be designed to meet agreed security and data integrity targets.
Rationale:
Defence ICT will be designed with the appropriate technical measures, alongside procedural and personal measures (across confidentiality, integrity, availability) to protect it to an assured level that enables it to be accredited within the context of the Defence network.

9. Flexibility

Statement:
Defence ICT will be designed to accommodate the uncertainty relating to the evolution of ICT and the environment within which it will be deployed.
Rationale:
ICT evolves very rapidly compared to many other Defence technologies and awarding contracts too early in the development cycle increases the risk of obsolescence, causing costly redesign later in the cycle. Defence cannot afford to develop and deploy infrastructures or networks to support specific applications and thus there is a need to isolate systems from the underlying technology.

10. Sustainability

Statement:
Defence ICT will be designed to meet the operation and mission requirement throughout the operation cycle (ie 'be adequate to achieve the prescribed Defence requirement').
Rationale:
Gartner have identified that, on average, the cost to maintain an application for a service life of 5 years accounts for 40% of the total cost of ownership; with increasing financial constraints, Defence must ensure that the logistics burden of its ICT is properly accounted for.

11. Safety

Statement:
Defence ICT will be designed to meet agreed safety targets.
Rationale:
The processes that Defence ICT support may have safety implications and therefore the ICT must achieve ALARP safety requirements in order that the solution can meet its targets. This consideration has to be wider than individual systems as the Network acts as a platform for Defence's information and behaviour of Network Components may introduce emergent safety constraints on other systems.

12. Supportability

Statement:
Supportability is the totality of the support arrangements that deliver the required level of service over the intended period of operation. It encompasses the availability, reliability and maintainability aspect of the capability.
Rationale:
Defence ICT supports most of the processes of Defence and therefore if it is not available when a user needs it, there is an adverse effect upon Defence.

ANNEX B - References

a. Information Technology Infrastructure Library (ITIL)

b. The Open Group Architecture Framework (TOGAF)

c. Centre for the Protection of National Infrastructure (CPNI) Policy and best practice: Patch Management – Good Practice Guide

d. JSP 777: Network Enabled Capability Handbook

e. JSP 815: Defence Environment and Safety Management

f. Ministry Of Defence Architecture Framework (MODAF)

g. Global Information Infrastructure (GII).

h. DG Info/8/5/1 (107/05) Convergence to Defence Information Infrastructure (DII) Core Services, 10 Aug 05

i. DII Application Development Guide

j. MOD Service Oriented Architecture (SOA) Handbook

k. Acquisition Operating Framework (AOF)

l. DE&S Safety & Engineering Instructions (SEI) ***– formerly DE&S Standing Instructions***

m. Fixed Technical Architecture

n. Defence ICT Strategy.

ANNEX C - Glossary

Term	Description
ICT	ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically. For example, personal computers, digital television, email.
ICT Environment	The ICT Environment covers the conditions that any ICT will operate in. This will cover characteristics like bandwidth, latency and jitter.
Principle	A Fundamental Attribute of ICT; an enduring generalised statement that informs and supports the way in which an organisation sets about fulfilling its mission. In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organisation, from values through to actions and results. The JSP 604 Principles are based on TOGAF (The Open Group Architecture Framework) Principles.
Rule	What is expected of ICT; a statement that prescribes the required effect of ICT. Rules should be directly linked to one, or more, principles.
Criteria	How a Project Shall Demonstrate Compliance with a Rule; provides the maturity of evidence required for compliance to each rule. The evidence is expected to mature through the project's lifecycle and shall be provided by the project.
PDR	The Preliminary Design Review assesses the proposed technical solution(s) before the project can proceed into detailed design.
CDR	The Critical Design Review assesses the technical solution before it is frozen and start of production.
TRRA	The Technical Release Readiness Assessment (TRRA) is the report produced by the NTA identifying the compliance status of a project to JSP 604.
AtO	An Authority to Operate (AtO) is given to a project following a successful probationary period after the introduced/changed ICTs has joined the network. It is issued by the NOA following assessment of its behaviour on the Network.

ANNEX D - Acronym List

Acronym	Meaning
AOF	Acquisition Operating Framework
ASEMS	Acquisition Safety and Environmental Management System
AtO	Authority to Operate
BPS	Boundary Protection Service
CDR	Critical Design Review
CDS	Cross-Domain Solution
CI	Configuration Item
CIDA	Coordination Installation Design Authority
CIO	Chief Information Officer
CIS	Communication and Information System
CMDB	Configuration Management Database
CMS	Configuration Management System
CND	Computer Network Defence
CPNI	Centre for the Protection of National Infrastructure
CSD	Crypto Services for Defence
CTO	Chief Technology Officer
D ISS	Director Information Systems and Services
DCNS	Defence Core Network Services
DE&S	Defence Equipment and Support
DFTS	Defence Fixed Telecommunications Service
DHFCS	Defence High Frequency Communications Service
DIAN	Defence Information Assurance Notice
DII	Defence Information Infrastructure
DIN	Defence Instruction Notice
DNS	Domain Name System
DSAS	Defence Security and Assurances Service
DSCP	Differentiated Service Code Point
DSO	Defence Spectrum Organisation
DTA	Deployed Technical Architecture
E3A	Electromagnetic Environmental Effects Authority
EDRM	Electronic Document Recording and Management
EI	Electromagnetic Integration
ELSEC	Electronic Emission Security

Acronym	Meaning
EMC	Electromagnetic Compatibility
EMPP	Electromagnetic Pulse Protection
EP	Equipment Programme
EULA	End User Licencing Agreement
GII	Global Information Infrastructure
GOSCC	Global Operations Security Control Centre
HF	High Frequency
HMG	Her Majesty's Government
IA	Information Assurance
ICT	Information and Communication Technology
IDAM	Identification and Authentication Management
IEC	International Electro-technical Commission
IG	Initial Gate
InnTI	Innovation and Technical Investigation
IP	Internet Protocol
IPLC	International Private Leased Circuit
ISO	International Standards Organisation
ISSP	Information Systems and Services Publication
ITEAP	Integrated Testing, Evaluation and Acceptance Plan
ITIL	Information Technology Infrastructure Library
JCU	Joint Cyber Unit
JSP	Joint Service Publication
LF	Low Frequency
MG	Main Gate
MI	Mutual Inteference
MODAF	Ministry of Defence Architecture Framework
NA	Network Authority
NALLA	National Allied Long-Lines Agency
NATO	North Atlantic Treaty Organisation
NCA	Network Capability Authority
NEC	Network Enabled Capability
NOA	Network Operating Authority
NTA	Network Technical Authority
OGD	Other Government Department
OSI	Open Systems Interconnection
PDR	Preliminary Design Review

Acronym	Meaning
PKI	Public Key Infrastructure
QoS	Quality of Service
RACI	Responsible, Accountable, Consulted, Informed
RBC	Risk Balance Case
RF	Radio Frequency
RMADS	Risk Management and Accreditation Document Set
RSS	Received Signal Service
RTE	Representative Testing Environment
SACM	Service Asset and Configuration Management
SDE	Spectrum Dependent Equipment
SKMS	Service Knowledge Management System
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOSA	System of Systems Approach
SOSDA	System of Systems Deployed Architecture
SPOC	Single Point of Contact
SRD	System Requirements Document
SRO	Senior Responsible Owner
TAC	Technical Attack Countermeasures
TOGAF	The Open Group Architecture Framework
TRRA	Technical Release Readiness Assessment
UAD	User Access Device
UAV	Unmanned Air Vehicle
UOR	Urgent Operational Requirement
UOT	Urgent Operational Task
URD	User Requirements Document
VLF	Very Low Frequency