FAQs

How does MODAF represent security?

Capabilities are subject to a variety of threats to the integrity, availability and confidentiality of their operation. These threats range from failures of equipment, attempts to gain unauthorised access to their services and data, through to sabotage of their functions. Security engineering is concerned with identifying the potential threats to a capability, and then, using a risk management approach, devising a set of measures which reduce the known and potential vulnerabilities to an acceptable level. In general the measures that can be applied fall into the following categories:

- Physical – measures such as guards, guard dogs, fences, locks, sensors, including CCTV, strong rooms, armour, weapons systems, etc.
- Procedural – the specification of procedures, including vetting (which tests that personnel have a sufficient level of integrity and trust to be given responsibility to access and use a capability's services and data) that will reduce the likelihood of vulnerabilities being exploited.
- COMSEC –using encryption and other techniques to ensure that data transmission is available at sufficient bandwidth, that the traffic pattern and content of data in transit are indecipherable to a third party who might intercept the data, and that its integrity is protected.
- TEMPEST – measures to ensure that the electromagnetic transmissions from equipment can't be intercept in order to derive information about the equipment's operation and the data it processes.
- INFOSEC – ensuring the integrity, availability and confidentiality of data and IT-based services.

In general, the measures employed to protect a capability will have undesirable impacts on all of the capability's lines of development, and in particular on its deployability, usability and procurement and maintenance costs. It is therefore desirable to minimise the strength of the measures to be employed in a fashion commensurate with the value of the assets being protected. This requires a risk-managed approach based on the assessment of the likely threats posed to the asset. The UK undertakes this risk assessment by considering the following characteristcs:

- Environment – The level of hostility of the environment the asset is being deployed to.
- Asset Value – this is denoted by a protective marking which indicates the impact of the loss or disclosure of the asset would have on the effective operation of the UK government and its departments of state.
- Criticality – an assessment of the criticality of the asset to enabling the UK government to undertake its activities.
- Personnel Clearance – a measure of the degree of trust that the UK government is willing to put in the personnel that will have (direct or indirect) access to the asset.

The Defence Manual of Security, JSP 440, formulates MOD's policies for protecting its assets and those of other government departments and nations with whose protection it is entrusted. JSP 440 calls on other HMG policies, particularly for communications and information security those of CESG. Security policies and procedures must also be compliant with various legislation such as the Data Protection Act and Regulation of Investigative Powers Act.

The aim of this guidance for representing security considerations is to enable sufficient information to be recorded for interested parties (accreditors, security advisors, users, system managers) to understand the potential security exposure of capabilities so that security can be managed effectively throughout the life of a capability. It is not the aim to provide an alternative for a formal security policy constructed in accordance with JSP 440, although the information provided using this guidance should provided the starting point for the necessary analysis required to derive such a policy, and the views created could be used as part of a security policy.

The table below shows the MODAF scheme for assigning security characteristics and protective measures to elements of MODAF. There is not a specific “security view” in MODAF: security information can be shown on views using annotations and call -outs, UML features or styling of symbols and edges. An appropriate key should be provided. A model library is provided with the MODAF Meta-Model to underpin the representation of security characteristics in a consistent way between models. Protective Measures are captured in MODAF using sub-types of SysML::Requirement. A non-normative extension to the MODAF Meta-Model is also provided containing these sub-types.

Viewpoint	Element	Security Characteristics	Protective Measures	Notes
Strategic	Capability Requirement	Security Marking Criticality Environment User Security Profile		The security characteristics of a capability requirement provide the security envelope for the capability during a particular epoch.
Operational	Node	User Security Profile Environment		The USP is the lowest clearance of users who will constitute a realised node. The environment identifies the most hostile conditions a node will be realised in. Nested nodes can be used to represent security domains, with sub-nodes in a ‘domain’ deriving their characteristics from the most immediate owning ‘domain.’
	Operational Activity	Security Marking Criticality		The security marking identifies the highest security marking of information that will be processed by a realised Operational Activity, and the Criticality measures the impact on Government operations of the disruption of the activity.
	Node Connector Type	Security Marking		The security marking identifies the highest security marking that will be exchanged across a node connector of this type.
	Organisation/Post	User Security Profile Environment		The minimum clearances, etc of members of the organisation/post.
System	Capability Configuration	Environment* User Security Profile* Criticality* Security Marking*		The security characteristics for a capability configuration are to be derived from the constituents.
	System	Environment* User Security Profile* Criticality* Security Marking*	Physical TEMPEST COMSEC	The environment of a system is derived from the Physical Asset to which is deployed. The USP is derived from the Organisation which uses the system, its Criticality and Security Marking from its Functions.
	Physical Asset	Environment	Physical TEMPEST	The environment identifies the worst environment to which the Physical Asset will be deployed.

	Function	Security Marking Criticality	INFOSEC Procedural	Security Marking identifies the maximum security marking of the data the Function will process, and its criticality represents the degree of harm to Government operations if it is disrupted.
	Resource Interaction Specification	Security Marking	COMSEC	The Security Marking represents the maximum security marking of information transversing the interaction.
	Role	User Security Profile	Procedural	The USP is the lowest clearance, etc of the user who will undertake the role. This should be derived from Organisations and Posts who can undertake the Role, if that information exists.