GSA
MANAGEMENT CONSULTING

INVESTED IN YOUR SUCCESS

Consideration of a Rationalisation Strategy for Defence ICT Systems

There are hundreds of Defence Information, Communication and Technology (ICT) systems currently hosted on the Defence Standard Operating Environment (SOE), standalone networks, and individual laptops. Consideration of a rationalisation strategy by capability managers before procurement and during sustainment of Defence ICT systems offers an opportunity for enhanced efficiency across Defence.

With an increased focus on cyber security and use of ICT systems across Defence, opportunities exist to rationalise Defence ICT systems to increase effectiveness and reduce cost. GSA Management Consulting bring insights from extensive experience as advisors, operators and system / fleet managers of Defence ICT systems. These insights highlight the opportunity for capability managers to consider a rationalisation strategy to meet their capability needs.

Operability – enhanced capability outcomes through better integration

Defence ICT systems are a fundamental enabler to the operations of Defence. The ability to fight as one relies on integration across services, domains and platforms underpinned by ICT systems capable of supporting such integration. New capabilities that seek to operate with bespoke, stove piped and commercially controlled ICT systems often risk degrading the integration and interoperability of platforms, systems and ultimately capability effects.

Rationalisation of ICT systems presents an opportunity for enhanced integration by reducing the number of systems operating in the SOE and increasing consistency across the Capability Lifecycle. Increased integration of Defence ICT systems naturally leads to enhanced capability outcomes at reduced cost.

Cyber Security – minimising exposure

Introducing additional systems to the existing Defence ICT network increases exposure to cyber security risk and adds to the burden of safeguarding against cyber-attack. Limiting the exposure to cyber threats by reducing the amount ICT systems can help to decrease the risk of breach and vulnerability to attack.

This was identified when growing numbers of standalone networks and laptops in operation within Defence led to the Chief Information Officer Group (CIOG) recommendation to remediate standalone networks to ensure appropriate security controls were applied. This remediation is leading to a reduction in standalone networks and the various ICT systems in operation. This reduces the burden of security assessment, certification, and accreditation while minimising exposure to risk.

Security Accreditation – reducing the burden

Accreditation of systems through CIOG is a critical step for introduction to service but can often induce delay to capability delivery. The volume of assessments, reviews, recommendations, support, and ultimate approval of systems to allow operation within Defence may be reduced through rationalisation of the systems in operation.

Further to the initial accreditation process, it is important to note that if the operating system is updated by network administrators, all existing systems are likely to require re-packaging in order to operate on the new environment which again increases the sustainment burden.

Sustainment – minimising costs

Sustainment of Defence ICT systems comes at significant cost which can sometimes be overlooked in the acquisition phase with a “set and forget” mindset.

Sustainment can include system updates, security patches, hardware and software refreshes, and constant monitoring to deal with outages and incidents. For every Defence ICT system in sustainment, there is often duplication of resources caused by multiple similar systems performing niche roles that could be streamlined through rationalisation.

Increasingly, access control for Defence ICT systems is being limited to CIOG staff. These access changes are affecting engineering support to some systems that are hosted on the network. By rationalising the number of ICT systems operating on the network, the limitations associated with access control can be reduced.

User Needs

Critical to achieving effective rationalisation is the ability and willingness to distinguish the genuinely unique / bespoke capability requirements from perceived unique / bespoke requirements. The facilitation of an approach that navigates this assessment objectively whilst generating commitment from stakeholders sits at the heart of successful rationalisation.

Trade offs must be made by users to ensure rationalisation of Defence ICT systems can be carried out. To manage the competing need for tailored Defence ICT systems vs rationalisation, it is imperative that users are involved in the design process to ensure unique needs are addressed and all opportunities for common approaches across capabilities are exploited.

One Defence

The One Defence mindset should be applied when it comes to Defence ICT systems. Every user, capability manager and system manager should be looking for opportunities to rationalise. Whether it is a system, version of a system, a tool or an application, a rationalisation strategy should be applied to ensure that Defence ICT systems do not grow exponentially and detract from the effective and efficient delivery of Defence capability rather than enabling it.

A fully networked system of systems approach that considers the joint effects when combined with a coordinated Defence ICT rationalisation strategy is essential for future success. Commitment to a rationalisation strategy will allow exploitation and integration of extant systems before rolling out your new Defence ICT system.

> “Critical to achieving effective rationalisation is the ability and willingness to distinguish genuinely unique / bespoke capability requirements from perceived unique / bespoke requirements. The facilitation of an approach that navigates this assessment objectively whilst generating commitment from stakeholders sits at the heart of successful rationalisation.”

Andrew O’Donnell
Manager
GSA Management Consulting

Contacts:

Andrew O’Donnell
Manager
Andrew.odonnell@gsamc.com.au

Heath Smith
Director
Heath.smith@gsamc.com.au