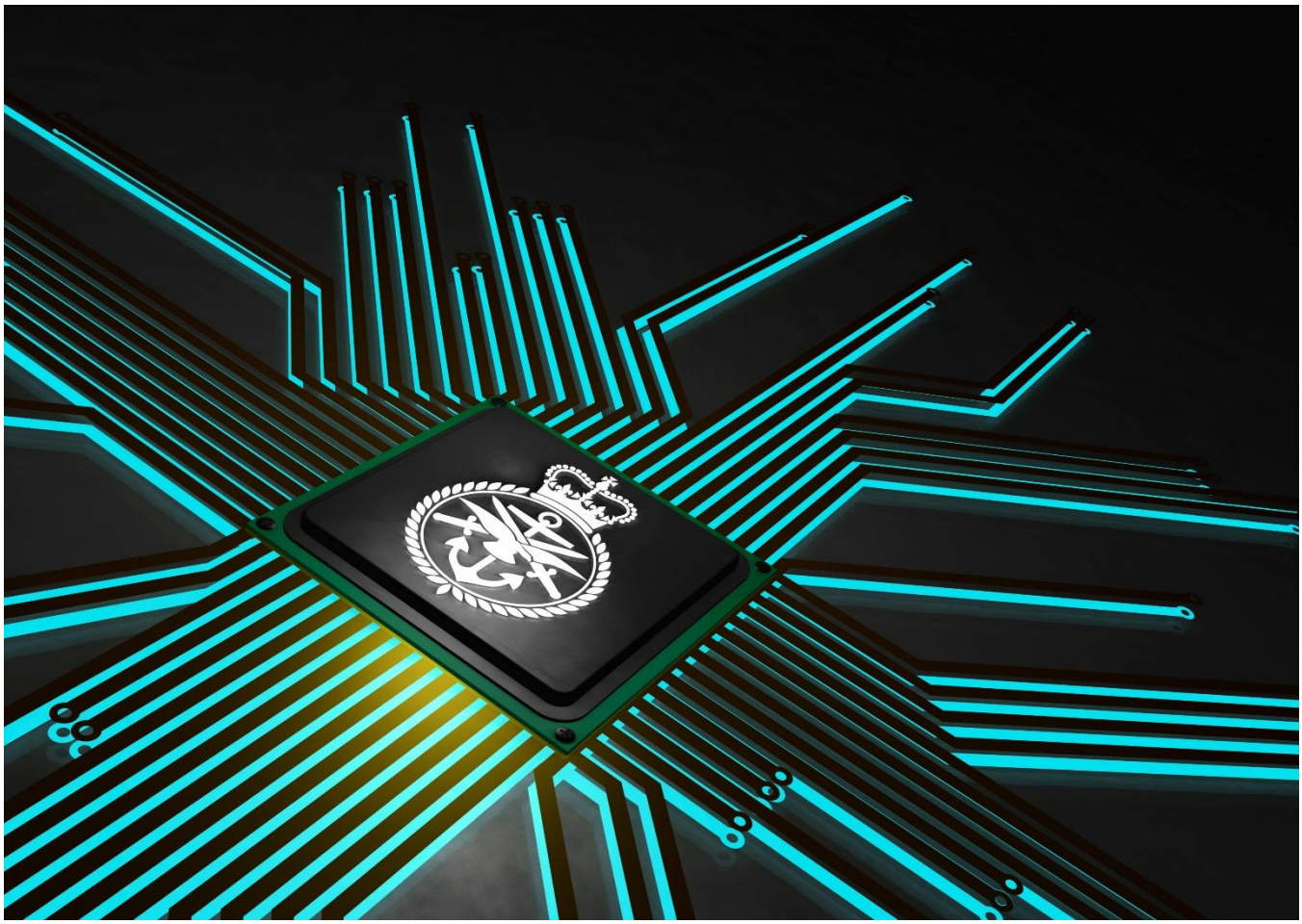
Ministry of Defence

Defence Digital
Digital Enablement

Enterprise Tooling Strategy Principles
DSM version



Document Summary

Purpose

1. This document has been produced to provide a clear viewpoint for the Architectural Principles to be adopted when considering tooling selection for introduction into the Defence ICT Eco System.

2. Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organisation sets about fulfilling its mission.

3. 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.

Intended Audience

4. Defence Digital Senior Management, and all areas across Defence Digital with responsibilities for tooling provision internally or acquisition of tooling in relation to delivery programmes/projects.

5. The Architecture Governance Board for approvals.

6. UK Strategic Command, Joint User and C4ISR stakeholders

7. Defence-wide Functions who have responsibility for tooling within their specific domains

Timing

8. Immediate - This document complements and extends the previous tooling strategy and will be reviewed regularly by the <governance board TBC>.

Document References and Sources

9. This document draws from several sources to gather input and context for the principles, some of which are:

   a. Enterprise Architecture – Defence Digital – Enterprise Digital Tooling Strategy - Issued May 2023. On MODNet please search “Enterprise Digital Tooling strategy 2023”.

Review Period of this Principles Document

10. This document will be reviewed at least annually by the <governance board TBC>, following formal issue of Version 1.0.

List of Contents

List of Tables

Specific Tooling Principles

12. These specific principles have been derived to meet the needs of the overall Tooling Strategy and should be applied when designing, procuring, and deploying tooling solutions within the Defence ICT Eco System. Their scope of use is Defence-wide.

13. Each principle has been developed using the template shown below in Table 1 and is aligned with TOGAF[1].

Name	**<Name of Principle>**
Statement	The Statement should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement be unambiguous.
Rationale	The Rationale should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.
Implications	The Implications should highlight the requirements, both for the business and IT, for carrying out the principle – in terms of resources, costs, and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. The impact to the business and consequences of adopting a principle should be clearly stated. The reader should readily discern the answer to: "How does this affect me?" It is important not to oversimplify, trivialize, or judge the merit of the impact. Some of the implications will be identified as potential impacts only and may be speculative rather than fully analysed.
Defence Technology Principle	Providing a 'golden-thread' link between the tooling principle to enable alignment of to the overarching defence technology to drive coherence of approach.

Table 1 – Principles Template

Business Principles

Name	**BP1: Greening and Sustainability**
Statement	Consideration should be given to reuse and/or reduction of the tooling landscape through introduction of specific greening and sustainment policies to reduce energy costs, tool proliferation and uncontrolled introduction.
Rationale	There is increasing pressure on Government Departments to reduce the footprint of energy usage across the estate. This can be achieved in part by: REUSE of current assets rather than buying new (both hardware and software); REDUCTION on the high numbers of tools that cater for the same or similar requirements: RECYCLING old licenses by upgrading rather than replacing with new (cost savings). Use of the 3Rs aligns with the GOV.UK policy https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025

[1] TOGAF 9.2 https://pubs.opengroup.org/architecture/togaf9-doc/arch/

Implications	Proliferation of tools providing similar, or the same functionality has high through life costs. Controlling introduction through careful adoption of Greening principle can help to reduce this. Uncontrolled introduction of tools has implications for increase in energy consumption through inadvertent costs of hardware increases needed to run the tooling. It can often be cheaper to recycle (resell) or reuse existing tools through cost-effective upgrades rather than replacement with different tooling.
Defence Technology Principle	Principle 8: Reuse when you can Share, reuse and work together on existing solutions to save time and money.

Name	**BP2: Simplify the Tooling Landscape**
Statement	New tooling should only be introduced where there is a clear requirement, and consideration should first be given to current tooling in the landscape. Tools no longer required should be retired.
Rationale	When a new tool is introduced, often catering for requirements already provided for in other tools, there is little regard paid for the validity or retention of those other tools. In order to simplify the tooling landscape, any approval for new tools must also consider what can be retired from the existing landscape (if any). This will also directly impact the through life costs of the overall tooling catalogue and potentially reduce the energy costs of running the tooling.
Implications	Introduction of new tooling without cross-reference to existing capabilities increases through life costs, increases use of energy (contrary to BP1), and potentially introduces more complexity into the landscape.
Defence Technology Principle	Principle 8: Reuse when you can Share, reuse and work together on existing solutions to save time and money.

Name	**BP3: Requirements driven selection**
Statement	Tooling should be selected based on the needs of the customer, through requirements capture and specific product testing (of selected tools) against them. A repeatable process should be adopted to ensure a consistent approach to this is used on every occasion.
Rationale	There has often been introduction of new tooling without a clear user requirement, often as a “Proof of Concept” where tooling of a similar nature already exists. In some extreme cases this has been done purely based on software vendor(s) being in close touch to key personnel within the Department. We need to stop this “introduction by stealth” and base all new tooling (including upgrades/replacements) on a clear requirements traceability process, with governed approvals, enabling simplification of the tooling landscape
Implications	Lack of coherency between procurements of new tools leads to increased costs, more complexity in the landscape and overlap of functionality without cross-checks. Potential for more stove-pipe activities further dilutes the usefulness of a landscape catalogue for all tooling.
Defence Technology Principle	Principle 5: Build in futureproofing from the start Futureproofing ensures the technology we use remains current, supported, secure and reliable.

Name	BP4: Exploit current Enterprise Agreements & Licensing
Statement	Where an Enterprise Agreement or licensing deal exists, these should be assessed for fitness for purpose first so that Defence gets the best Return on Investment (RoI).
Rationale	Defence has invested heavily in Enterprise Agreements for many vendor products. This also includes license deals for multiple products. So that Defence can get the best Return on Investment for these tools, any new requirement should first assess existing agreements for applicability and potential costs savings. If no agreement exists, options to explore creation of one should be considered if there would be sufficient take-up.
Implications	By not exploiting these agreements, there is a risk that the through life costs of tooling will be excessive. By stove-piping procurements, the Department ends up paying significantly more for licenses. Version control, patching and upgrades can be out-of-step leading to obsolescence and supportability issues. Licencing is governed under the Commercial Policy Statement for Software Licencing. Please search Knowledge in Defence for “Commercial Policy Statement for Software Licensing”
Defence Technology Principle	Principle 1 Use common standards and patterns Build your solution from approved technology. Data and services to avoid duplication and unnecessary costs.

Information Principles

Name	IP1: Data shall be delaminated from tools
Statement	All data shall be able to be exchanged independently of the tool it is generated and/or used within.
Rationale	Data exchange must be a key principle to avoid vendor and tool lock-in. This can be done through the use of Open Standards (TP1 applies).
Implications	COTS[2] products may only have proprietary data models which limit data exchange and reuse. Exit and migration costs need to be factored into data model designs as part of the tooling whole life costs. Choice of data standards may also be limited by the tooling vendor, whereby specific customisations may be in place to “add value” to each specific product, potentially limiting functionality when used in “pure standards” mode.
Defence Technology Principle	Principle 3 Make Data easy to access Our data should be available to users and systems when and where they need it, on appropriate devices and infrastructure

Name	IP2: Document all designs
Statement	All tooling designs shall be fully documented, reviewed and approved so that any tooling implementation, change, upgrade, exchange, or replacement can be easily assimilated into the Defence ICT Eco System.

[2] Or GOTS (Government off the shelf) will also fit into this category.

Rationale	Undocumented tools create difficulties across the tooling landscape in terms of knowledge of what is actually there. By documenting all designs, with rigour applied to reviews and architectural approvals, the landscape becomes fully catalogued and much easier to manage. As tools evolve, change, or are retired it is important to understand the implications of that tool which can only be done through detailed information pertaining to it i.e. design documents.
Implications	A rigorous review and approvals process can be onerous and time consuming, resulting in poor documentation or indeed complete lack of designs. Consistency of documentation needs to be carefully managed so that comparisons between tools and systems is repeatable. Without standardised processes and templates etc. this can become a free-for-all. Lack of design approvals impacts the ability to catalogue the landscape, resulting in more complexity and overlapping functionality of tools. Through-life costs can spiral when the landscape is not fully known.
Defence Technology Principle	Principle 1 Use common standards and patterns Build your solution from approved technology. Data and services to avoid duplication and unnecessary costs.

Application Principles

Name	**AP1: Use existing services**
Statement	Consume and use existing Application Programming Interfaces (APIs). Where applicable consider the best enabler to deliver functionality whether via internal (Private APIs) or external (Public APIs) rather than developing in-house solutions.
Rationale	Modern tools (digital services) can be built utilising a wide range of APIs. Eliminating the effort designing and implementing a duplicate service will reduce ICT project costs and shorten the time to deliver ICT projects.
Implications	Projects and ICT service providers need to understand what services exists, are being built and planned so that they can plan and cost implementation activities accordingly. A service catalogue needs to be developed and maintained as the source of this information. This must be established for Future ICT bottom-up based on users' needs to avoid defining services based on existing legacy IT services. There must be a single service catalogue supporting ITSM and EA. This needs to communicate a pipeline of services to clearly show those proposed, under development, in operation and being retired. The API strategy manages the APIs standards across Defence. On MODNet search "API strategy".
Defence Technology Principle	Principle 2 Integrate and adapt When designing a solution, you need to plan integrations with current and future Defence data and systems.

Name	**AP2: COTS first**
Statement	Component technology, tools and services shall, as much as possible, be purchased as Commercial Off the Shelf (COTS).

Rationale	COTS[3] products often provide a wealth of business logic, process modelling, and workflows already developed or that can be configured (see AP3) to meet the enterprise's requirements. Roadmaps detail forthcoming improvements, in terms of security and functionality which ultimately benefit the planning processes; these business essentials are not present in solutions that are locally engineered. Commercial products provide a greater longevity, supportability and are therefore more sustainable; whereas in house developments are likely to be constrained by the developer of the solution and their availability. Acquiring commercial products provide a greater level of support, knowledge and upgradeability than can be afforded by internal developments. Any new products procured for the enterprise, must be able to integrate with the existing architecture, unless it is replacing or significantly enhancing the current provision of service. Otherwise, software diversity increases and reduces the effectiveness of our ability to serve the needs of our customers.
Implications	There may be limited choices, as many of these tools are vendor, technology and/or platform dependent. This principle will require standards which support sustainability (see BP1). Following the initial set-up of the product, integration with additional systems should facilitate agile development. Formalised training programmes can be undertaken for both developers and staff managing the solution, thus enhancing both staff knowledge and expediting the benefits afforded to the business. Enterprise agreements should be used wherever possible (see BP4).
Defence Technology Principle	Principle 5 Build in futureproofing from the start Futureproofing ensures the technology we use remains current, supported, secure and reliable.

Name	**AP3: Configuration not customisation**
Statement	Tools should not be modified beyond the ability to change predefined fields and settings provided within the tool by the tooling vendor.
Rationale	So that we can operate independently of tools, with both data exchange (Open Standards) and standard exchange mechanisms (APIs), we need to ensure that COTS packages are not changed through custom scripts or code changes specific to Defence. It is acceptable to utilise configuration fields provided as part of the COTS package, as they are accessible to all customers of that package. Configuration changes and field entries must be documented (IP2 applies)
Implications	Vendor lock-in and difficulties in exiting the tool become costly issues to manage once changes are made to underlying code and systems. It is more likely that Open Standards and Open Source (TP1 applies) will be disadvantaged through customisation.
Defence Technology Principle	Principle 2 Integrate and adapt When designing a solution, you need to plan integrations with current and future Defence data and systems

Name	**AP4: Build services not tools**
Statement	Tools will be built as a collection of services that deliver via an Application Program Interface (API) a business service to users.
Rationale	This facilitates reuse, interoperability, and the ability to scale by reducing tight dependencies between components.

[3] Or GOTS (Government off the shelf) will also fit into this category.

Implications	Cloud-services and COTS products are expected to have well-defined APIs. An overlap of functionality can exist within multiple Cloud and COTS solutions. This must be managed to prevent unnecessary duplication of services. Tooling design will need to cater for all Service Management processes.
Defence Technology Principle	Principle 2 Integrate and adapt When designing a solution you need to plan integrations with current and future Defence data and systems

Name	**AP5: User interfaces should be browser-based**
Statement	User interfaces shall be delivered as web-based HTTP tools using HTML5, CSS and JavaScript.
Rationale	Ensures that tools are independent of underlying platforms and are easy to use, providing Technology Independence. This enables accessibility across different devices and decreases maintenance and deployment effort. GOV.UK Service Manual "Designing for different browsers and devices" applies.
Implications	Tools are web-based and stateless as reasonably possible. Commercial Off-The-Shelf (COTS) solutions may limit choices. Exceptions may arise for functions and services that are constrained by the selected platform, for example bandwidth constrained environments/technology.
Defence Technology Principle	Principle 2 Integrate and adapt When designing a solution you need to plan integrations with current and future Defence data and systems.

Technology Principles

Name	**TP1: Use Open Standards and Open Source**
Statement	Open standards must be used in all solution designs to enable interoperability. Open-source software must be compared and considered alongside commercial software when selecting technology / tooling solutions.
Rationale	Closed proprietary standards restrict reuse, reduce interoperability, and can create vendor lock-in that leads to unforeseen financial costs. Compliance with HM Government Open Standards Principles and GOV.UK Technology Code of Practice points 3 and 4.
Implications	Exit, rebid and rebuild costs must be taken into consideration during procurement decisions for best value for money comparisons, between open source and proprietary solutions. Open-source is not necessarily free to use. Many independent software vendors and value-added resellers use open-source technology within proprietary for-profit services. Other departments provide commercial service management wrappers around open-source products. Commercial software needs to be considered alongside open-source equivalents from a total cost of ownership perspective. Open-Source software may carry security implications
Defence Technology Principle	Principle 1 Use common standards and patterns Build your solution from approved technology. Data and services to avoid duplication and unnecessary costs.

Name	**TP2: Manage technical debt and obsolescence**
Statement	The Future ICT for defence must make changes easier. Any tactical decisions that introduce technical debt (quick but messy solutions) will only be endorsed if there is a recognised actionable plan to address both of them technically and financially.

Rationale	Unaddressed technical debt increases the complexity and costs of maintaining ICT making it harder to upgrade software, transition services and deliver solutions that meet users' needs.
Implications	Reducing technical debt must become part of the Authority's culture so that the current accrued debt in the ICT estate can be addressed. Dispensations for short term technical debt to meet tactical business imperatives can be granted. Tools and services need to be designed and delivered to be as technology independent as possible. An increased level of service-based architecture will be required. See AP1. Delivery projects adopting an Agile delivery method will need to have a solution architect to safeguard against adding new technical debt into the Future ICT estate. Software and hardware ICT assets (non-Cloud) must be recorded and managed in a configuration management system.
Defence Technology Principle	Principle 5 Build in futureproofing from the start Futureproofing ensures the technology we use remains current, supported, secure and reliable.