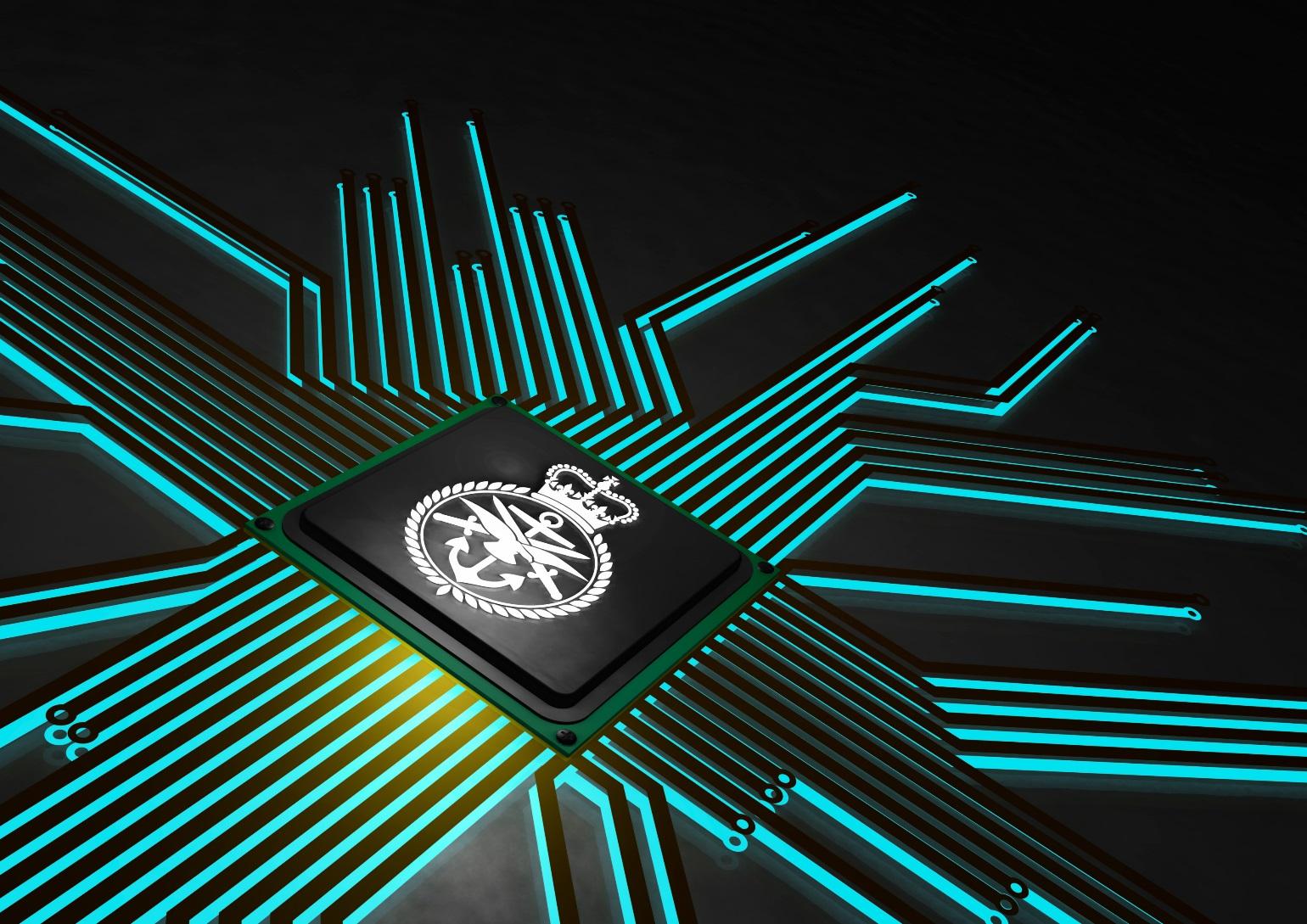
**Defence Digital**

**Digital Enablement**

Enterprise Tooling Strategy Principles



**Document Control**

| **Document Identification** | |
| --- | --- |
| Document Owner | DD, Digital Enablement, Architecture Head |
| Document Author | Paul Smith |
| Document File Name | 20200128 Tooling Strategy Principles.docx |
| Document File Location | DD Digital Enablement Architecture SharePoint Online Area |

| **Document Version Control** | | | |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change(s)** |
| 0.1 | 28/01/2020 | Paul Smith | Initial draft |
| 0.2 |  | Paul Smith | Update following initial peer review |
| 0.3 | 01/03/2022 | Alex Taylor | Update to reflect stakeholder comments and alignment to Digital Technology Rules |
| 1.0 | 14/04/2022 | Alex Taylor | Update following second peer review |
|  |  |  |  |
|  |  |  |  |

| **Key Stakeholder** | | | |
| --- | --- | --- | --- |
| **Copy** | **Date Sent** | **Name, Role** | **Organisation, Location, Contact** |
|  |  |  |  |
|  |  |  |  |

UK Strategic Command | Defence Digital

Digital Enablement | Architecture

Building 405, Floorplate E3

MOD Corsham

Westwells Road

Corsham

Wilts

SN13 9NR

# 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

1. 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.
2. The Architecture Governance Board for approvals.
3. UK Strategic Command, Joint User and C4ISR stakeholders
4. Defence-wide Functions who have responsibility for tooling within their specific domains

## Timing

1. Immediate - This document complements and extends the previous tooling strategy[[1]](#footnote-0) and will be reviewed regularly by the <governance board TBC>.

## Document References and Sources

1. This document draws from several sources to gather input and context for the principles, some of which are:
   1. Defence Authority for Information – Defence Digital Service Design - Enterprise Tooling Strategy, Issued November 2017 - [The Strategy](https://modgovuk.sharepoint.com/:w:/r/teams/3114/Shared%20Documents/20171117%20Defence%20Enterprise%20Tooling%20Strategy%20%26%20Outcomes%20v1.0.docx?d=waf8c19fcb7c64a75ad0e1bd30f7ae4f5&csf=1&e=5BKax4). NOTE - that due to our licensing arrangements with Gartner, this document must not be distributed outside of MOD personnel. There is a separate redacted version for release to Industry available [here](https://modgovuk.sharepoint.com/:b:/r/teams/3114/Shared%20Documents/Industry%20Releasable%20Tooling%20Strategy/20180112%20Defence%20Enterprise%20Tooling%20Strategy%20%26%20Outcomes%20%5bIndustry%20Releasable%5d%20v1.3.pdf?csf=1&e=ZiP06L);
   2. Future of Defence EA – Digital Technology Rules – DRAFT – circulated September 2021 - [Digital Technology Rules](https://modgovuk.sharepoint.com/:p:/r/sites/MOD-CTOTeam/Shared%20Documents/01-W1%20Strategy/Digital%20Technology%20Rules.pptx?d=wd792897fb5d8495daa9f71087d48d4a8&csf=1&web=1&e=mo7hhJ)

## Review Period of this Principles Document

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

**List of Contents**

[**Document Control 2**](#_heading=h.gjdgxs)

[**Document Summary 3**](#_heading=h.1fob9te)

[**Purpose 3**](#_heading=h.3znysh7)

[**Intended Audience 3**](#_heading=h.2et92p0)

[**Timing 3**](#_heading=h.tyjcwt)

[**Document References and Sources 3**](#_heading=h.3dy6vkm)

[**Review Period of this Principles Document 3**](#_heading=h.1t3h5sf)

[**List of Contents 4**](#_heading=h.4d34og8)

[**List of Tables 4**](#_heading=h.17dp8vu)

[**Overarching Digital Technology Rules 5**](#_heading=h.26in1rg)

[**Specific Tooling Principles 7**](#_heading=h.lnxbz9)

[**Business Principles 7**](#_heading=h.1ksv4uv)

[**Information Principles 9**](#_heading=h.44sinio)

[**Application Principles 10**](#_heading=h.2jxsxqh)

[**Technology Principles 12**](#_heading=h.z337ya)

## List of Tables

[**Table 1 – Principles Template 7**](#_heading=h.35nkun2)

# Overarching Digital Technology Rules

1. At the highest level, the Digital Technology Rules for Defence (“Digital Rules”) brings together the key elements of existing rulesets and incorporates new, additional direction aligned to the core principles of the Common Technology Architecture (CTA).
2. The CTA describes the underlying architecture used to deliver the Defence Digital Backbone and articulates a common taxonomy to be applied across all Defence ICT activities.
3. These rules have primacy over every other specific Tooling Principle detailed within this document. Should any conflict occur between the Digital Rules and the Specific Tooling Principles, the <Governance Board TBC> shall provide arbitration as to which takes precedence.
4. Further, any requests for exemptions to *any* Architectural and/or Tooling Principle should be referred to the <Governance Board TBC> for approval or if unable to approve, for escalation to Director Digital Enablement - Architecture Governance Board for ratification.
5. In all tooling selection, analysis and ongoing capability, each tool should be assessed against the Digital Rules:
   1. **Common Rules, Standards and Patterns** to guide, support, and cohere technology solutions in the best interests of Defence as a whole. Wherever specified follow Defence’s Digital Technology Rules utilise approved common standards, technical reference architectures and patterns in order to drive coherence across the Digital estate.
   2. **Realise Interoperability** to accelerate the shift to ‘integrated’ activities and more closely align with our allies across all classifications. Support the shift to multi-domain integration, partner interoperability and functional coherence by promoting and realising interoperability of data, software, and technology. Continue the move away from ‘joint’ activity towards ‘integrated’ activity and align with initiatives that bring us closer to our allies e.g., NATO across all classifications.
   3. **Data as a Strategic Asset,** so that we can enable sustainable exploitation of data for modern warfare, both from the centre and at the edge***.*** Allow timely and secure access across Defence to a sovereign, enduring, curated, and standardised data core, enabling sustainable exploitation of data.
   4. **Secure by Design** enabling proactive risk management and appropriate security consideration; connecting principles, roles, processes, tools, and techniques to achieve secure systems. Protect and defend Defence’s data, networks, systems, and decisions based on a zero-trust framework and data centric security, compliant with all organisational, legal and interoperability obligations.
   5. **Cloud First** to grow our elastic, evergreen technology estate in which hyperscale datasets can be effectively managed and seamlessly exploited across the organisation. Public, hyperscale cloud solutions must be used as the default option in order to grow our elastic, scalable, evergreen technology estate at multiple classification levels, enhancing agility and reducing the cost and risk of technology refresh. Private cloud or other on-premises hosting options by exception only
   6. **Accelerate and Innovate** through exploitation of modern delivery methods and a focus on architecting for success with greenfield technologies such as AI and Synthetics. Enable a shift to modern ways of working and intelligent decision making through exploitation of technologies such as CI/CD, Automation, AI, ML and RPA. Embrace innovation and rapid prototyping
   7. **Re-use Before Buy, Before Build** so that we can get the most value from what we have, share, and scale the best innovations from across the organisation. Focus on reusing and building from our existing technology components, identifying pockets of good practice that can scale to meet the needs of the wider Defence, evolving our way out of our legacy and obsolescence challenges.
   8. **Value for Money** enhancing taxpayer value though simplified, commoditised shared services, differentiating only to provide an economic or competitive advantage on the battlefield. Enhance value to the taxpayer though the use of simplified, efficient shared services and commodity technologies wherever possible, differentiating our technology only where required to meet specific classification requirements, or to provide an economic or competitive advantage.

# Specific Tooling Principles

1. 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.
2. Each principle has been developed using the template shown below in Table 3 and is aligned with TOGAF[[2]](#footnote-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. |

**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 [ICT Greening Strategy](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/155098/greening-government-ict-strategy.pdf) |
| **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. |

| **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. |

| **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 and applications) 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. |

| **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 applications, 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](http://aof.uwh.diif.r.mil.uk/aofcontent/tactical/toolkit/downloads/ipr_sal/iprsal_cps.pdf) |

## Information Principles

| **Name** | **IP1: Data shall be delaminated from tools** |
| --- | --- |
| **Statement** | All data shall be able to be exchanged independently of the application it is generated and/or used within. |
| **Rationale** | Data exchange must be a key principle to avoid vendor and application lock-in. This can be done through the use of Open Standards (TP1 applies). |
| **Implications** | COTS 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 application vendor, whereby specific customisations may be in place to “add value” to each specific product, potentially limiting functionality when used in “pure standards” mode |

| **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. |
| **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. |

## Application Principles

| **Name** | **AP1: Use existing services** |
| --- | --- |
| **Statement** | Consume and use existing Application Programming Interfaces (APIs). Don’t try to do everything in-house as the functionality needed could be provided through existing services, whether internal (Private APIs) or external (Public APIs). |
| **Rationale** | Modern applications (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[[3]](#footnote-2) manages the APIs standards across Defence. |

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

| **Name** | **AP3: Configuration not customisation** |
| --- | --- |
| **Statement** | Applications should not be modified beyond the ability to change predefined fields and settings provided within the tool by the application vendor. |
| **Rationale** | So that we can operate independently of applications, 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 application 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. |

| **Name** | **AP4: Build services not applications** |
| --- | --- |
| **Statement** | Applications will be built as a collection of services that expose an Application Program Interface (API) enabling them to be combined to deliver users what they need. |
| **Rationale** | This facilitates reuse, interoperability, and the ability to scale by reducing tight dependencies between components. |
| **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. |

| **Name** | **AP5: User interfaces should be browser-based** |
| --- | --- |
| **Statement** | User interfaces shall be delivered as web-based HTTP applications using HTML5, CSS and JavaScript. |
| **Rationale** | Ensures that applications 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](https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices)” applies. |
| **Implications** | Applications 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. |

## 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](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78892/Open-Standards-Principles-FINAL.pdf) and GOV.UK [Technology Code of Practice](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78892/Open-Standards-Principles-FINAL.pdf) 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 |

| **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.  Applications 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. |

1. [Defence Enterprise Tooling Strategy & Outcomes v1.0](https://modgovuk.sharepoint.com/teams/3114/Shared%20Documents/20171117%20Defence%20Enterprise%20Tooling%20Strategy%20%26%20Outcomes%20v1.0.docx?d=waf8c19fcb7c64a75ad0e1bd30f7ae4f5) [↑](#footnote-ref-0)
2. TOGAF 9.2 https://pubs.opengroup.org/architecture/togaf9-doc/arch/ [↑](#footnote-ref-1)
3. [API strategy](https://modgovuk.sharepoint.com/teams/2433/Artefacts%20101/Forms/AllItems.aspx?id=%2Fteams%2F2433%2FArtefacts%20101%2FCTA%2FTechnology%20Foundations%2FIntegration%2FAPI%20Strategy%20v1%2E1%2Epdf&parent=%2Fteams%2F2433%2FArtefacts%20101%2FCTA%2FTechnology%20Foundations%2FIntegration) [↑](#footnote-ref-2)