Ministry of Defence

Cloud Strategic Roadmap for Defence

Edition 1

The future of Cloud Services

I'm delighted to introduce Defence's new Cloud Strategic Roadmap, 'The future of Cloud Services'.

A critical component of our Digital Backbone is hyperscale cloud capabilities across all classifications. Our roadmap sets out our explicit intent to coordinate and accelerate the most ambitious plans for hyperscale cloud adoption across Defence.

Our future is one that realises data as a strategic asset, that enables us to move faster than our adversaries. Defence will have the unsurpassed ability to consume, aggregate, analyse and exploit data at orders of magnitude more than ever before, it will be fit for our future of integrated global warfighting across all domains.

We are setting out a powerful vision with supporting plans and programmes to cohere and mandate consumption of radically advanced cloud services.

We will consolidate and rationalise existing capabilities, alongside designing and delivering new capabilities to offer a single service across Defence, through the delivery vehicle, the Cirrus Portfolio. We will work with the world's leading suppliers, and those who have delivered these capabilities in the US military.

Thank you for engaging on this work. We look forward to realising this vision together, with modern, fast, coherent and secure cloud services that enable the true value of our data to be exploited throughout Defence.

Charlie Forte, MOD Chief Information Officer, Digital Functional Lead

Preface

Purpose

The purpose of this Cloud Strategic Roadmap for Defence is to state the vision and transformative change required for Defence to consume more world-class Cloud capabilities. Cloud is the key enabler for the realisation of the Digital Backbone and Data Strategy for Defence. Establishing the right cloud platforms will drastically improve the quality of the user experience both within the enterprise and at the tactical edge, accelerating the exploitation of data and providing more sophisticated ways of delivering our Defence products.

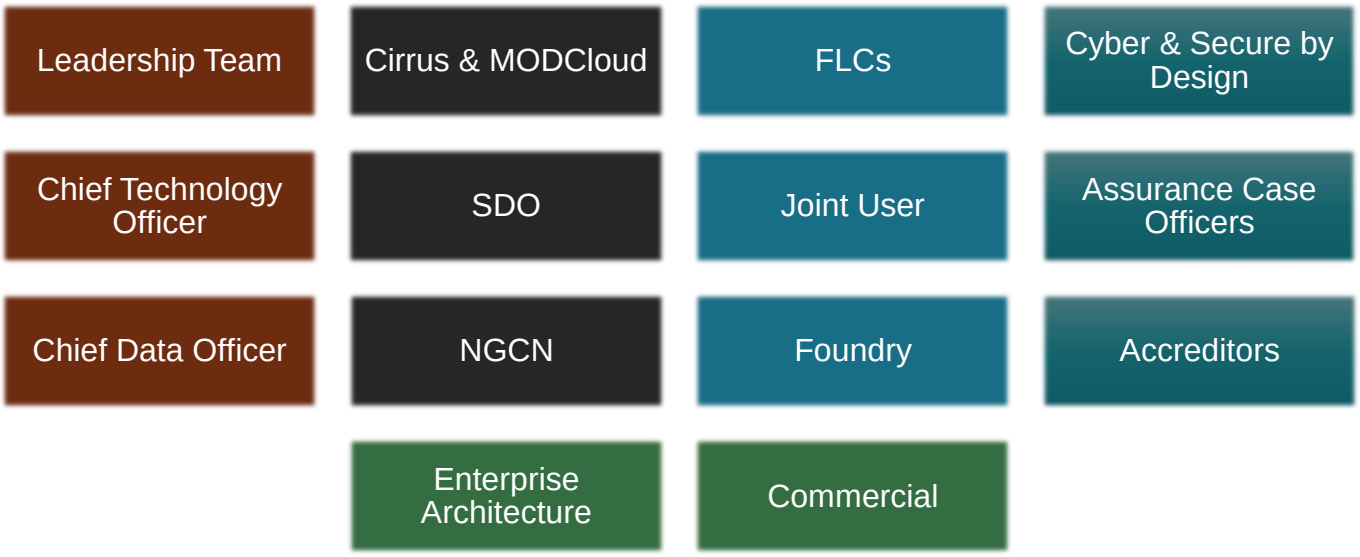
This roadmap articulates the strategic outcomes, the tightly coupled dependencies and the incremental steps to accelerate delivery and exploitation of hyperscale cloud services across Defence. The roadmap aligns the Ways with the Means required to deliver Defence's cloud ambitions, with a focus on consumption of hyperscale Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings, supplemented by MODCloud Software as a Service (SaaS) services. Defence needs to invest in a radical cultural shift, process, and cloud skills, to transform and compete in the digital age and align with our wider Digital Strategy for Defence.

Audience

The document provides clear intent, direction, and guidance for all across Defence – Functions, Commands and Enabling Organisations. This roadmap is aimed at a broad readership including users, owners and customers of Cloud, decision-makers and partners across government and international allies. The roadmap will be of particular interest to Capability Sponsors, SORs, Acquisition Organisations and Operating Authorities; Leaders of FLCs, TLBs and Defence Customers; CIOs and Programme teams realising the Digital Backbone; Defence Digital Architecture & Security teams and Business as usual teams.

Stakeholders engaged

A significant number of Defence stakeholders contributed towards the realisation of this roadmap – this includes Defence Digital stakeholders, Front Line Commands and adjacent programmes.



Map to the Digital Strategies

The Cloud Strategic Roadmap for Defence should be read alongside the other Defence Strategies, including the Digital Strategy, Data Strategy, Cyber Resilience Strategy, Technology Strategy, and any relevant forthcoming Digital Function sub-strategies.

Digital Strategy for Defence

The Digital Strategy for Defence outlines how the Defence Digital Function will transform by delivering a secure, singular, modern Digital Backbone. Cloud is the underpinning technology for it.

Data Strategy, Cyber Resilience Strategy and Technology Strategy for Defence

The Data Strategy states the data vision and transformative changes required for defence to leverage data as a strategic asset.

The Cyber Resilience Strategy states the principles and shift required to build a Cyber Resilient Defence.

The Technology Strategy sets the pan-Defence digital technology vision by directing the transformative changes that will realise Defence's Digital Strategy, and to deliver the Digital Backbone.

This Document

Cloud Strategic Roadmap for Defence

This document serves to outline the journey to adopt more modern Cloud platforms and realise the Digital Backbone.

Digital Sub-Strategies and extant and forthcoming Digital Function sub-strategies.

Roadmap on a page

1. *Diagnosis: Digital age warfare requires us to invest in modern technologies*

Cloud is one of the key building blocks to realise the Digital Backbone, allowing us to unleash the power of data and exploit emerging technologies at pace and scale

- Warfighting at the edge must be amplified through adoption of Tactical Edge Cloud technologies
- Obsolescence must be addressed to realise greater cost savings in the longer term
- We need hyperscale cloud to unleash the power of our Defence Data and to satisfy our user needs
- Our culture, skills and processes must evolve to enable us to drive towards a digital future

We set up CIRRUS and the Digital Foundry - which have already onboarded over 400 OFFICIAL workloads to public cloud. We must now accelerate our estate transformation at SECRET and TOP SECRET classifications.

2. *Ends: Our Cloud vision and Strategic Outcomes by 2025 are clearly defined*

Vision: We will exploit world-class cloud capabilities at all classifications, predicated on Cloud first as a principle

Strategic Outcomes by 2025: the Future of Cloud across Defence

- Delivering a secure and scalable platform to gain strategic military advantage
- Driving innovation through evergreen technologies by default
- Driving exploitation to realise benefits around efficiency and economic value
- Empowering digital age warfighters by maximising the survivability and security of innovative, world-class digital capabilities
- Realising greater benefits by integrating with partners within the cloud ecosystem

3. *Ways: Defence will leverage people and principles to transform Cloud for Defence*

We will adopt a cloud exploitation delivery model, driven by clear guiding principles and underpinned by strong behaviours and responsibilities from our people

Guiding Principles	*Cloud Exploitation Model*	*Behaviours and Responsibilities*
• MODCloud First • Realise Interoperability • Easy to use at the edge • Self-Serve Cloud • Data as a Strategic Asset • Secure by Design	• Exploiting Cloud architectures and hyperscale partnerships to access cutting edge technologies	• Ensuring roles across Defence accelerate and enable cloud adoption through expected behaviours and responsibilities

4. *Means: Key enablers are required to facilitate the exploitation of cloud incrementally*

The enablers and facilitators required to empower Defence's drive to Cloud

Cloud Delivery Model	*3-Year Plan*	*Partners and Suppliers*
• A Delivery model fit for purpose, to truly govern and leverage our skills and talents in Defence	• Based on tangible outcomes, the 3-year plan clearly shows how we will deliver capability at pace	• Partnering with the best suppliers to facilitate and deliver world class outcomes for Defence

Diagnosis

The current technology core is too fragmented, fragile, insecure and obsolescent

Getting greater, near-real-time analysis of rapidly changing data to combat modern threats is forcing us to revisit our approach to cloud as a means to address legacy application shortfalls.

We are not yet exploiting emerging technologies at pace and scale. We have too often traded-out technology refresh and have not driven sufficient integration and commonality.

Continuing down this path will prevent us from exploiting emerging technologies at the pace and scale required to deliver the defence purpose.

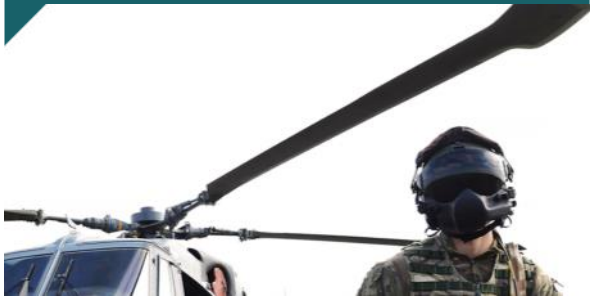
Our commitment to realise the Digital Backbone has already commenced.

So far, we have established hyperscale cloud services at OFFICIAL and increased the maturity and evolution of MODCloud - which now offers a mix of public, private and hybrid cloud services.

We have launched CIRRUS to cohere our cloud deliveries across all classifications, and to guide how the MOD consumes cloud services faster, cheaper and with improved interoperability. CIRRUS includes Data Centre Rationalisation (DCR), to enable the close down of legacy systems and support their migration to cloud.

CIRRUS and the Digital Foundry:

- ✓ Delivering a hyperscale platform to gain strategic military advantage
- ✓ Empowering digital age warfighters
- ✓ Driving benefits to maximise efficiency and economic value
- ✓ Driving innovation through modern technologies by default
- ✓ Reducing and preventing obsolescence



The steps made to date laid the foundations, but we need a step change for a solution to be seamless to deploy, secure by design, and cost-effective at scale.

There are required changes that we can no longer underestimate or delay:

- Warfighting requirements at the edge, as well as strategic capabilities in digital and data strategies, can only be fulfilled by deployable and scalable cloud services. We must extend our hyperscale cloud services available at OFFICIAL to SECRET to provide game-changing capabilities across Defence.
- Culture, standards, capabilities and technology must lead us towards a secure modern enterprise. Our mentality, skills and processes must shift to facilitate this step-change.
- In delivery of the Digital Backbone, we must consider and mitigate wider environmental, ethical and socio-economic risks of our digital technology.
- Legacy obsolescence is an opportunity to invest in our estate to realise greater cost efficiencies in the longer term.
- Foundational investments allowed us to embark upon this journey, but a step change is needed to proceed at scale and at pace with our AUKUS allies[1].

1. PM Statement on AUKUS Partnership, Sept 2021

Contents

Ends

Ways

Means

Appendix

Ends

Our strategic priorities

Strategic Context

"We must work with allies to make the most of new technologies; improve integration across all domains and throughout the spectrum of conflict; and as the NATO Reflection Group recently highlighted, recognise its essential role in cohering how we, as allies, handle this era of great power competition, staying ahead of our rivals and not waiting for them to set the agenda."
– Rt Hon Ben Wallace MP, Secretary of State for Defence

Digital is all-pervasive and is changing the character of warfare and politics

We are becoming increasingly empowered by, and dependent on, digital technology. So are our adversaries. This creates a constant and subtle threat, something that we have not been accustomed to over the last generation.

Today's warfare is populated by assertive authoritarian rivals, who see the strategic context as a continuous challenge. Recognising that they aim to win without going to 'war', as we would define it, we must be ready to respond the same way.

We must therefore adopt a more agile approach to place the latest technologies in the hands of our users, whilst ensuring our people, processes and data keep pace with best practice.

Defence is firmly grasping the challenge of this disruption – both opportunity and threat –and Digital sits at the heart of our developing investment options

Our "Digital Strategy for Defence"[2] outlines our plan to exploit technology, to multiply the national advantages we enjoy: an advanced digital economy; a strong entrepreneurial base; a committed and mobilised Defence workforce and partners across industry and academia.

Its outcome **- a secure, singular, modern Digital Backbone -** is connecting sensors, effectors and deciders across military and business domains, driving integration and interoperability across platforms.

One of the foundational building blocks of the Digital Backbone is the delivery of a secure, hyperscale cloud ecosystem to address the needs across multiple classifications.

It will support increased data sharing and exploitation across security classifications, mobile access to Defence systems and rapid development applications that scale to meet increasing demands and possibilities.

As such, Cloud is not solely an IT decision, but a pan-Defence priority.

The Appendix describes in more detail what is driving these requirements and what this means for our globally deployed forces.

1. Data Strategy or Defence, Sept 2021

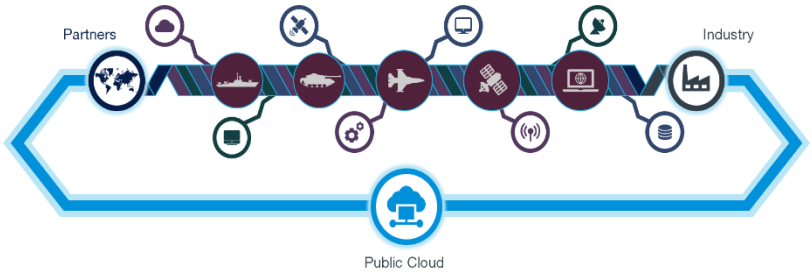
2. Digital Strategy for Defence, Apr 2021

Vision

Our Vision out to 2025:

Predicated on **Public Cloud as a principle**, **Defence will exploit a world-class hyperscale capability at all classifications** – realising the Digital Backbone and unleashing the power of Defence Data. Cloud will enable seamless information and services, available in the right place and at the right time for all Defence users.

Our digital presence will be pervasive and formidable, amplifying our capabilities from the edge to the centre, creating an agile, integrated, data-driven fighting force supported by a digitally empowered enterprise. Cloud is the core enabler and platform to fulfilling this vision.



- **Defence will adopt MODCloud as a principle.** we will transform Defence through our adoption of public cloud. We will continue to move our OFFICIAL workloads to public cloud, complying with governments' Cloud First Policy.
- **Defence will enable multi-classification cloud.** We will build upon Defence's MODCloud services at OFFICIAL by using lessons learnt to deliver SECRET and TOP SECRET cloud requirements, with a view to ensuring the appropriate mix of public, private and hybrid cloud environments. We will explore the use of SaaS in collaboration with the Cyber Defence and Risk (CyDR) service in Defence Digital, to ensure all solutions are Secure by Design.
- **Defence will partner with Hyperscalers.** We will work with leading cloud service providers to obtain access to the required hyperscale cloud services, including but not limited to Compute, Storage, Database, Network, Big Data storage and analytics, Artificial Intelligence, Machine Learning, Robotics and Synthetics.

Multicloud at OFFICIAL Given the complexity of Defence's requirements, one vendor is unlikely to meet Defence's evolving ambition, sudden demand for scalability, and industry advances. MODCloud is delivering multicloud to provide the best fit for mission needs at OFFICIAL, given the varying capabilities that each of the providers bring, alongside other benefits, including:

- ✓ Take advantage of the cloud vendor with the best available technologies matched against the given requirement, to provide the most optimal capabilities and features
- ✓ Increased agility and flexibility, gain the potential to move capabilities between vendors to take advantage of emerging technologies
- ✓ Greater opportunities for operational cost efficiencies, by selecting the most competitive cloud vendor, and via more competitive pricing
- ✓ Avoid vendor lock-in by removing single vendor dependencies

Strategic Outcomes

The following Strategic Outcomes outline Defence's ambition for Cloud by 2025.

Defence Organisations must cohere their efforts to deliver Defence's Cloud vision, accelerating how they currently operate.

Cloud Strategic Outcomes by 2025	Will Achieve
1 **Delivering secure and scalable platforms to gain strategic military advantage**	Pervasively exploiting cloud services enables us to deliver the capability demanded by Defence's Digital Backbone Strategy. By 2025, the services required by game changing military capabilities will be available across Defence, accelerating our level of cloud consumption. We will take advantage of evergreen solutions to prevent future obsolescence, and to ensure immediate access to the latest technologies, driving the pace of modernisation.
2 **Driving innovation through evergreen technologies by default**	Leveraging hyperscale cloud services as a platform enables us to exploit emerging technologies, and consequently allows Defence to stay ahead of adversaries. By 2025, we will use cloud platforms as the foundation on which to build capabilities in big data, advanced analytics, automation, and synthetics. We will spend the majority of our compute expenditure investing in strategic modern platforms, rather than maintaining obsolete legacy platforms.
3 **Driving exploitation to realise benefits around efficiency and economic value**	Concentrating our investment in cloud services will improve the user experience, grows skills, and deliver better products faster. By 2025, we will deliver services from an ecosystem of standardised platforms. We will streamline onboarding processes to these cloud platforms, so that benefits can be seamlessly unlocked by Defence.
4 **Empowering digital age warfighters through our world-class capabilities**	Warfighting technology in the digital age requires capabilities that exist by default within cloud technologies. By 2025, we will enable the deployment, extension and growth of those capabilities, maximising the survivability and security of services, and exploiting data to provide faster access to curated datasets in deployed locations and at the tactical edge. We will exploit cloud services to seamlessly link sensors to effectors via appropriate decision makers,
5 **Realising greater benefits by integrating with partners within the cloud ecosystem**	Collaborating with industry and providers will enable us to tackle our biggest technology challenges and accelerate consumption of emerging cloud technologies across Defence, unlocking greater partner investment and commitment. By partnering with the best across Defence, government, and industry, we will be able to bring different perspectives and skillsets that will facilitate game-changing innovation at a scale beyond what we could achieve in silos.

The Future of Cloud for Defence

The Digital Strategy for Defence outlines a step-change in approach required for Defence to leverage digital and data as enablers to facilitate faster and better decision making. **As a critical enabler of the Digital Backbone**, Cloud is the underpinning platform that will connect 'sensors to effectors, via appropriate decision-makers'.

Cloud will provide the foundation on which we build and deliver the future capability we require. It underpins and enables the advanced applications and services we need at speed, so we can keep pace with, and succeed against, our adversaries. It will enable and deliver on-demand services and applications that are easily accessible and rapidly scalable. In turn, this will enable access for deployed users to retrieve and process data rapidly and securely on the battlefield, as well as enabling access for business users to enterprise systems from anywhere.

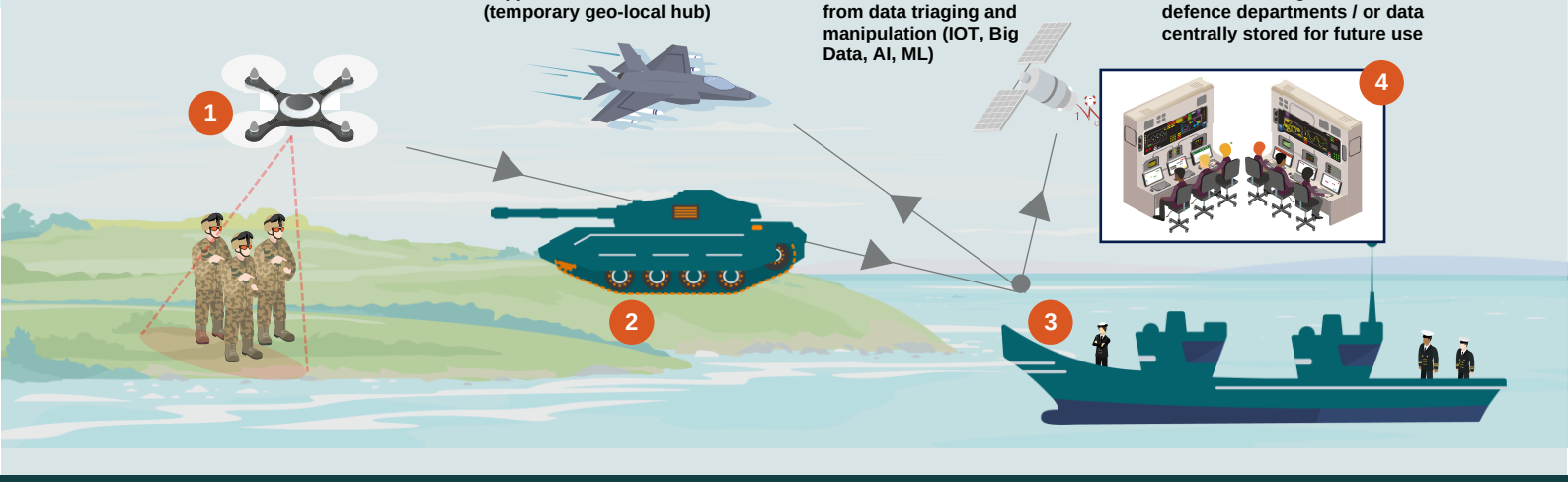
The change at the edge

Sensors & IOT / Edge gateways enable allied drones and support assets to send targeting data to a local UK Force Element HQ

Locally deploy cloud enabled stacks leveraging AI innovation to analyse drone video in response to emerging threat

Local deployed allied forces have immediate situational awareness, simply allocating targets across interlocked platforms

Triaged data sent in real time to central cloud repository to enable coherent decision making and build future AI, ML and Synthetic capabilities



Local Cloud edge computing capability enables quick decision making and data manipulation

Self-serve and automated cloud services will bring a common contract, common definitions, and common ways of doing straightforward accreditation for Defence users.

Self-Serve
Easily consumable and standardised

Automated
Faster for users to exploit and store data

Seamless
Through improved connectivity

"As a military leader I can seamlessly and securely communicate and collaborate with allies and partners without being slowed down by networks and gateways"

"As a decision maker I am able to get quicker, unobstructed access to the technology and services that enable me to analyse data"

"As submariner I can use on-board edge compute services to get better insights from local data even when submerged"

Ways

Achieving our priorities

How Defence will approach Cloud

Accelerating the adoption of cloud must be recognised and valued as a critical Defence activity. The ambition for battlespace advantage will only be realised through significant changes in our culture. To provide a better understanding of what this means for Defence personnel, the section below provides a set of behaviours, stating clearly what we need from our people for our objectives to be realised.

MOD CIO will:	• Responsible for delivering and accelerating Cloud, driving the cloud programmes closely aligned with the FLCs • Drive the cloud transformation under a single integral part of the CIO's Functional Team, ensuring outcomes are achieved and aligned to the overarching strategies for Defence. • Set up Cloud functions and governance within their organisations to drive cloud adoption and consumption, in coherence with all contributing programmes and cloud consumers. • Ensure that data is integral to key decision-making and operational activity, with enduring funding to govern, develop and maintain it locally.
FLC/TLB CIOs will:	• Drive the Digital transformation that cloud brings across Defence, representing the voice of their organisation within the Function; and contributing to the development of standards and processes. • Drive technology transformations as one-team under the CIO's Functional Team, ensuring outcomes are achieved and aligned to the overarching strategies for Defence.
Senior Defence Leadership will:	• Recruit world-class and diverse talent with the cloud skills and capabilities, leveraging common technology architecture standards, automated interfaces and tools. • Foster a cultural shift where cloud is seen as a campaign rather as a project, fostering incremental progress and value-based outcomes. • Inform and inspire Defence personnel and users on cloud matters.
Defence Digital CTO will:	• Contribute to the cloud transformation and innovation and less so for day-to-day technology management. Covering a wide range of technologies to support Cloud from a Digital Enablement and operations angle, i.e. factory automation composable business and cybersecurity. • Foster Technology and process innovation, i.e. 5G, edge compute or microservices. • Optimise and operation of the cloud programme, including commercial decisions.
Programme SROs will:	• Foster cloud exploitation and consumption, ensuring the true exploitation and curation of Data in a secure by design fashion. • Adhere to Defence agreed architecture standards (e.g. Common Technology Architecture, the Rules of the Road etc.) • Issue ongoing comms to celebrate success and marketing Defence's cloud campaign amongst our end-users
Capability Leads will:	• Ensure that cloud consumption is at the core of key decision-making around capability design and delivery, with enduring funding to govern, develop and maintain a seamless platform, easy to use for our Defence customers. • Adhere to Defence agreed standards and management practices with our Hyperscalers • Ensure data is securely exploited and can flow out of platforms for pan-Defence exploitation.
Third Party Providers will:	• Comply with any applicable digital rules, policies and architectural standards. • Work with Defence Digital to ensure the service(s) provided meet requirements for integration and interoperability • Provide excellent partnership and quality services in line with the Defence's guidelines, aiming at optimising the delivery of business value.

Enterprise Architects will:	• Develop and maintain the architectural framework and roadmap • Provide and facilitate an architectural governance process that ensures compliance with standards • Provide a “centre of excellence” to support Solution Architects • Focus on open, loosely coupled Cloud architectures for the future while adapting existing architectures to facilitate integration with legacy systems
Solution Architects will:	• Guide development of a technical solution by providing input on the technical feasibility and architectural direction • Identify and assess high level technical solution alternatives, and choose the high-level technical design • Estimate solution costs and resources and create solution design specifications
Risk Specialists will:	• Develop and implement policies, procedures, and processes designed towards continuous compliance • Apply risk management techniques to determine the effectiveness of controls, and create action plans to track and remediate identified risks
Security Specialists will:	• Set global security policy, support development efforts, and oversee security operations • Define and maintain the Identity & Access Management approach
Service Management will:	• Own and govern service management processes by setting policy and procedures, then managing performance and process adherence. • Provide a transparent, well documented billing model and support for managed billing • A ‘personal shopper’ with TAM experience for MODCloud interactions and requests
Product Managers will:	• Assume end-to-end responsibility for business products and services to ensure they deliver the expected outcomes
Automations Specialists will:	• Automate manual operations processes currently employed in service support, testing, production operations and monitoring • Enable the definition of continuous integration and deployment pipelines • Provide a portal for self-service provisioning of Cloud resources
Infrastructure Operations will:	• Maintain the performance and stability of the production environment for both infrastructure and applications

We must **act as one**, fully embracing cross-domain interoperability and working together to deliver a coherent end state that achieves our strategic outcomes.

The Cloud Guiding Principles

To realise accelerate cloud adoption we have defined the key principles that will serve as a guiding framework. These are aligned with the Technology Strategy for Defence.

MODCloud First

Use MODCloud solutions before alternatives. Where appropriate leverage hyperscale hyperconverged infrastructure and cloud native development practices to grow our elastic, scalable, evergreen technology estate.

Realise interoperability

Reuse available, common patterns and standards across all classifications, akin to the common architectural building blocks defined as part of the Network Reference Architecture that supports commonality of design and solution interoperability.

Easy to use at the edge

Ensure cloud services are customer centric, based on understanding the people who will consume them, what they need to do and why their needs are important.

Self-Serve Cloud

Continue to empower and strengthen the capabilities of cloud services, ensuring that Defence is loosely coupled yet closely aligned. Architect cloud to enable self-serve and workload portability, using cloud orchestration, automation, and tooling to seamlessly provision and manage services.

Cloud is a key technology enabler to realising the following principles:

Data at as strategic asset

New cloud services must align with the Data Strategy for Defence and MOD Data principles to enable delivery of timely, accurate and trustworthy data across domains, enabling sustainable exploitation of data as a strategic asset for modern warfare.

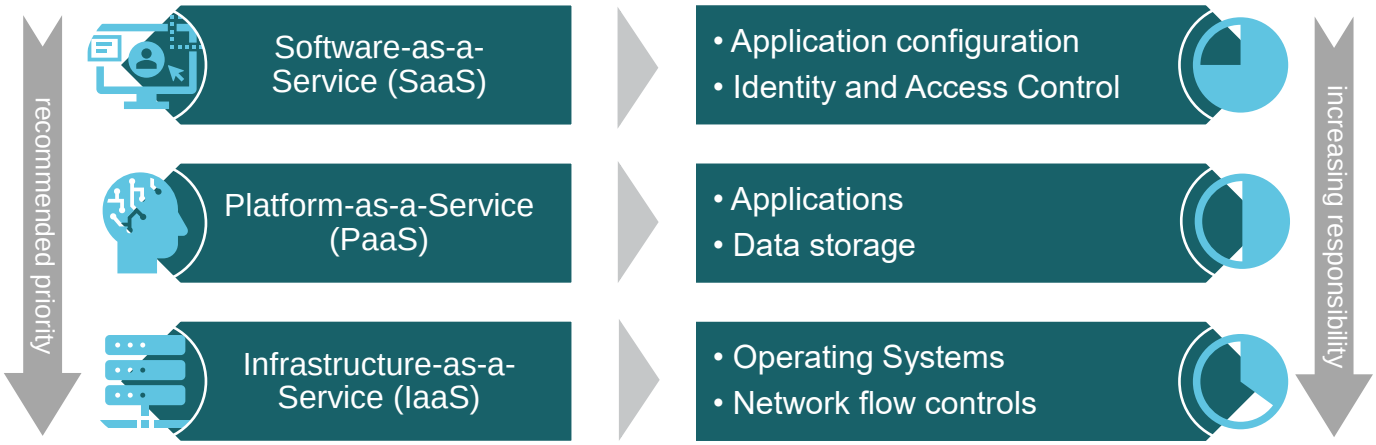
Secure by Design

Secure by Design must underpin all new cloud technologies, enabling security and compliance at scale across defence. Services will have built in safeguards and controls from inception and utilise robust patterns and standards that align to the Cyber Strategy.

How Defence will transition to Cloud

Realising the Digital Backbone requires a true transformation to Cloud, by providing platforms that our end users can exploit at all data classification levels.

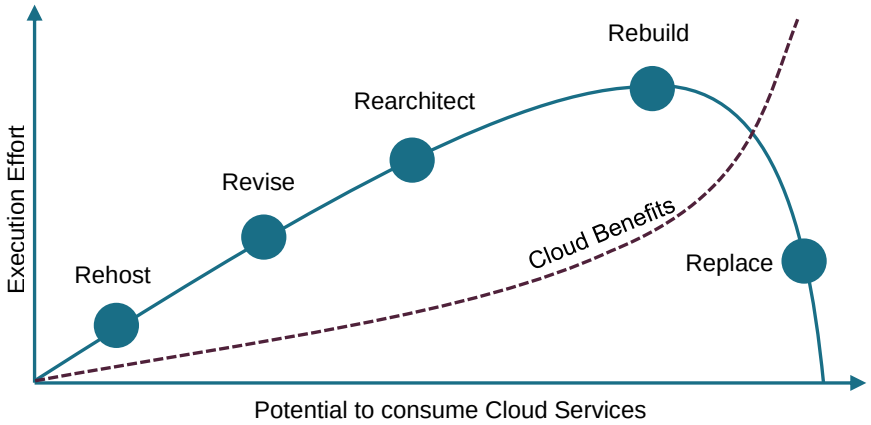
Cloud computing services fall broadly into 3 types, SaaS, PaaS and IaaS, underpinned by a shared responsibility model providing each type with different degrees of benefit, choice and control. We will aim to provide cloud services across all three types, prioritised in the order of SaaS, PaaS and IaaS wherever feasible given the classification and risks assessed, to ensure the lowest barrier to adoption and to delegate as much responsibility to the cloud platform as possible.



Our target is to be ‘cloud native’ as much as possible, focusing on API-centric designs and making the most of cloud native features, rather than trying to implement them ourselves. This approach will naturally include a preference for SaaS, PaaS and serverless components over IaaS, though will accommodate IaaS services when required.

Migration options to the cloud include rehost, revise, rearchitect, rebuild or replace, the option chosen will reflect the benefits sought and investment available.

Applications could migrate as is, or they may require some transformation to ensure compatibility or to maximize the benefits from moving to cloud. The migration path chosen for each App requires varying levels of investment to realise varying levels of cloud benefits.

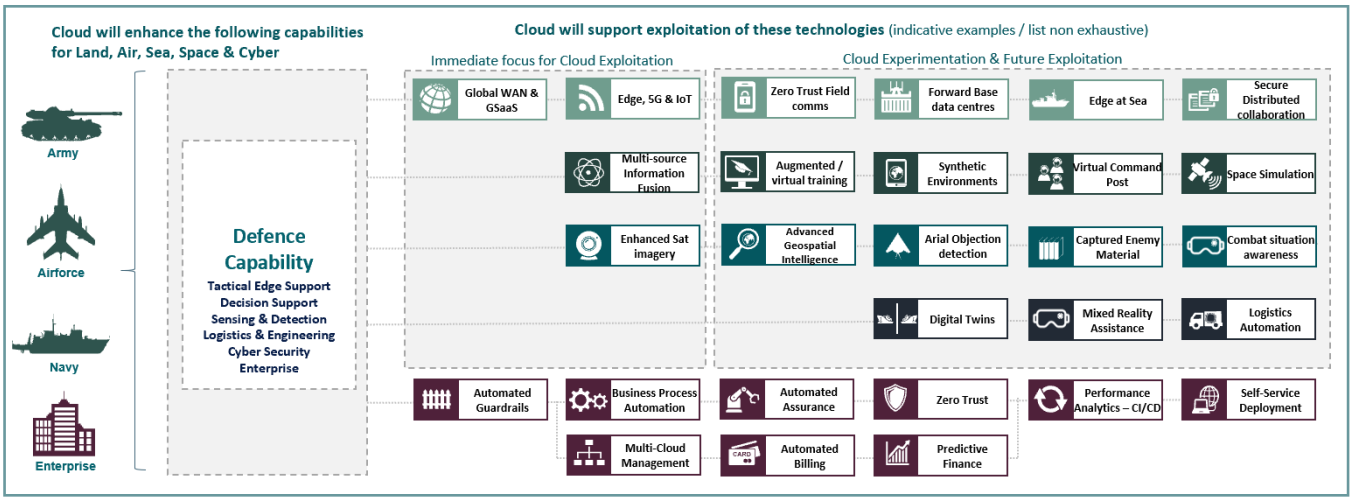


Generally, there is close correlation between the migration strategy and the cloud tier chosen, with “rehost” and “revise” strategies implemented on IaaS, “rearchitect” and “rebuild” on PaaS, and “replace” on SaaS.

Defence's Cloud Exploitation Model

Cloud is not an end state per se - it's the gateway to exploiting cutting edge architecture and technologies that will transform the future of Defence.

Our cloud exploitation model maps technology areas, that hyperscale cloud can significantly impact, to capabilities within Defence. This provides clarity and guidance on technology areas to exploit, in a logical order, that considers the dependencies and requirements for deployment of tightly coupled technologies.

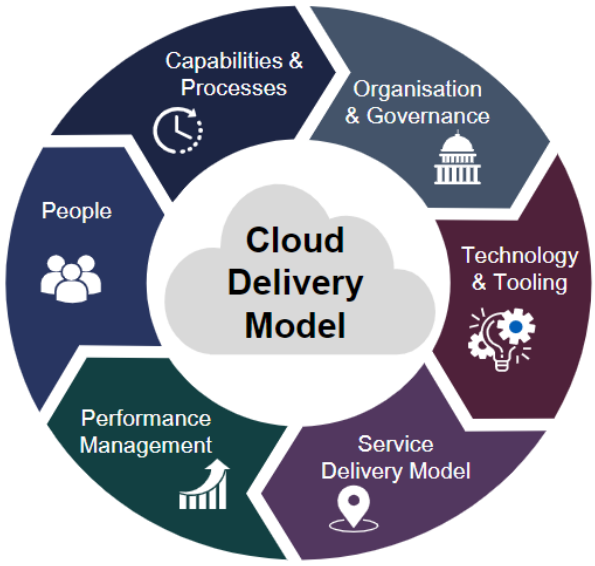


Diverse technologies such as Edge, 5G & IoT have multiple applications across Defence, providing benefit to both to our deployed forces as well as the wider enterprise, and it's imperative that we develop and deploy them efficiently and effectively. Defence will look to gain maturity in these technology areas by focusing on high value use cases derived from direct FLC engagement, and then exploiting this capability pan-defence through re-usable assets to accelerate consumption in a coherent and repeatable manner.

Exploiting cloud technologies will change the way we operate across our estate.

As we progress across the maturity scale, the number of cloud native services we consume will increase and adapting our operational capabilities and the skillsets required to support these capabilities is fundamental to provide the best-in-class capability across Defence. While our warfighters have different requirements, we must provide a consistent user experience for them and the wider enterprise.

An iterative Cloud Delivery Model will ensure we deliver, scale, and evolve cloud services both as new requirements are identified and as demand increases.

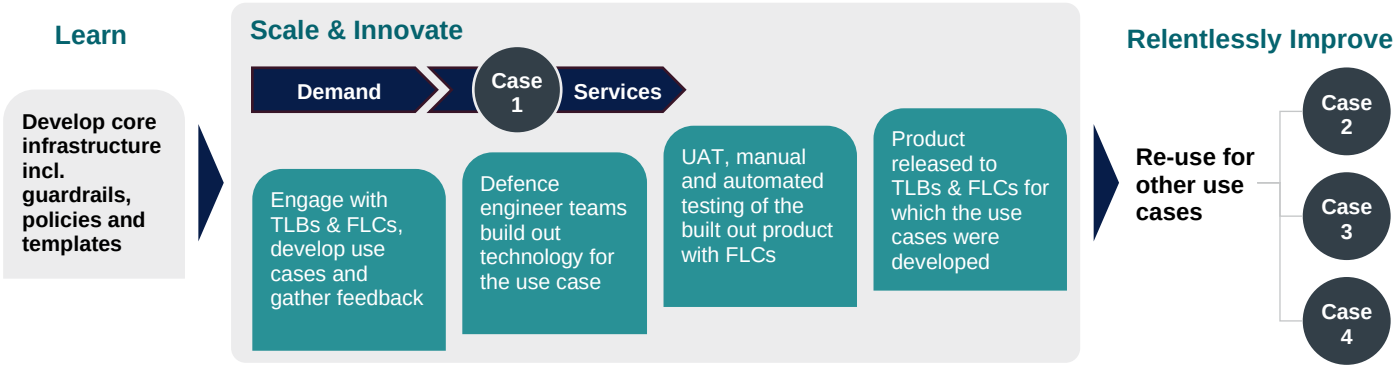


How Defence will exploit Cloud

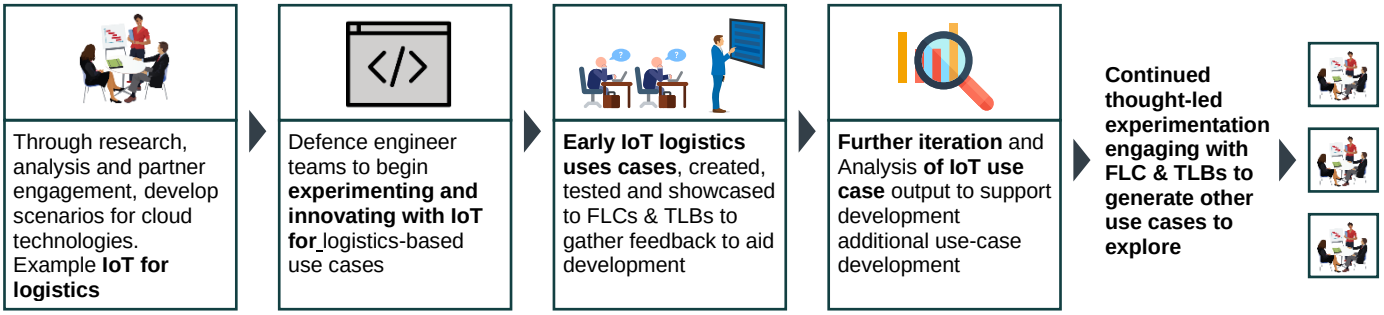
Our approach to exploitation must be diverse and serve the needs of our consumers.

To gain maximum benefit when exploiting these technologies, we will adopt two approaches, Demand-led and Thought-led exploitation. These approaches will be run in parallel, facilitating Defence in gaining critical mass in cloud capability, while encouraging experimentation and innovation as we look to compete with, and surpass our adversaries in digital warfare.

Demand-led exploitation adopts a user centric approach, by engaging with the FLCs and TLBs we will deliver cloud technology solutions based on strong use cases that will resolve their immediate requirements.



Thought-led experimentation will focus on driving innovation through insight led predictions of what technologies will be needed across Defence in the next 5-6 years' time. By engaging with our partners and internal innovation capabilities, we will develop foundational use cases, and through continuous iteration, mature our capability and increase our adoption of these technologies across the enterprise and to the tactical edge.



We must continue to be efficient and reuse our best-in-class assets

Foundational architecture guidelines underpinned by the Common Technology Architecture (CTA) will help dictate how workloads are hosted, which will form the 'core' components of Defence's hyperscale cloud capability.

Defence will leverage technologies such as containerisation, virtualisation, PaaS & SaaS to shift to a more modern deployment model where appropriate, organically promoting innovation and experimentation. As we continue to mature, we will create reusable assets such as blueprints, templates, and standardised components to enable rapid and consistent deployment of cloud solutions across Defence for all use cases.

How Defence will explore the Market

Defence will exploit world-class cloud capabilities at all classifications. From a commercial perspective, this means that we will have a pre-competed environment with selected providers ready to be employed whenever needed.

A cloud compute framework already exists at OFFICIAL through Crown Commercial Service (CCS), that works across the whole of His Majesty's Government (HMG). We are working on a similar framework for SECRET, that will also span across HMG, and timelines with major milestones are shown below.

SECRET Hyperscale Milestones

Q2'22 – Q4'22

- Formal Industry Engagement
- MOD and OGD Customer Engagement Activities
- Formal Supplier Engagement with Shortlisted Suppliers
- Formal Procurement Planning and CCS Internal Approval Processes
- CCS aggregate requirements with OGDs

Q1'23 – Q2'23

- Formal Invitation to Tender (ITT) published
- ITT Responses Evaluated
- Contract Notice Publication

Q3'23 – Q4'23

- Contract Award for **Hyperscale Framework for SECRET**
- Mobilisation and Implementation

Q1'24 – Q2'24

- Initial capability goes live

Q3'24 – Q4'24

- Full capability available

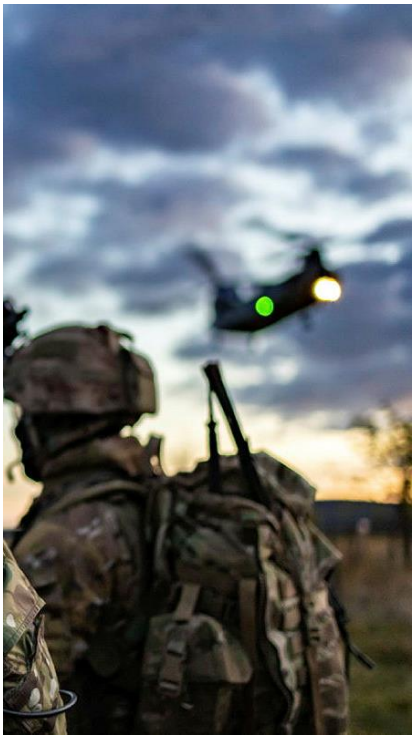
Cloud Procurement Principles

- Cloud will be procured via true Hyperscalers – those suppliers able to provide the computing architecture to seamlessly scale thousands of servers appropriately, as increased demand is added on the system
- Selection is dependent on cloud requirements rather than framework conditions
- The framework is a pre-competed environment
- MOD will buy either directly from, or as close as possible to, the source – avoiding resellers wherever commercially feasible
- Cloud requirements include functionality, skills, and data movement across classifications
- The key market players can be classified as below:
    - **Tier 1:** Leading cloud providers in the market, with the ability to scale as increased unpredictable demand is needed by Defence.
    - **Tier 2:** Significant footprint in the cloud market providing specialised services.
    - **Tier 3:** Challenger provider of cloud services, catering to specific use cases.

Partnering for Cloud

Defence is a coherent fighting force that must be supported by a coherent, interoperable IT estate. Collaboration and partnerships play a critical role in delivering transformative digital capabilities at the pace required to compete with and surpass that of our adversaries.

Across our Organisations



This document, alongside other supporting strategies and initiatives such as the Modernising Defence Programme (MDP), provides the step change in how Defence exploits digital, data and technology, directing our Functions, Commands and Enabling organisations to drive and accelerate Defence's digital future.

Throughout Defence we have exceptionally talented individuals that are producing cloud-based assets that are changing the way we operate in the digital battlespace and wider enterprise, but historically in silo's and therefore reducing the benefits we receive.

Collectively Defence will continue to take action to formalise mechanisms and stand-up forums that embraces a collaborative mentality and multi-use approach, accelerating our cloud maturity in a more coherent manner. We will continue to leverage the approach in programmes such as The Foundry DevSecOps Service that is being delivered by PREDA. This user-centred, cloud-native service provides rapid an agile software development platform that can be leveraged throughout the Defence enterprise and by our industry partners.

Across our Partners

Exploiting cloud technologies brings enormous potential to our enterprise that can be further accelerated through collaborating with government, allies, and industry. Cloud technology is a pivotal enabler for several core initiatives across Defence and is a key asset in operating in the digital age for national governmental bodies. Defence has an obligation to enable and encourage collaboration to support these wider initiatives, using our collective capabilities to drive innovation, scale capability and gain maturity in unison. We must:

- Leveraging existing Defence commercial and supplier relationships to access best in class resources, knowledge, and assets
- Cooperating with wider governmental organisations to share data and assets to provide efficiencies where appropriate (e.g., customs clearance data from department of trades)

We must not be insular in our cloud exploitation journey, but instead continue to leverage our long-standing relationships.

Means

Enablers to achieve

The Enablers for success

Our **cloud enablers** will drive forward and shape the development of a 3-year roadmap, providing clarity on the responsibilities and accountabilities across Defence:

Cohered Delivery Model

CIRRUS has provided a coherent structure from which to drive Defence's cloud activities, connecting together multiple established programmes, projects and activities to deliver and align on similar outcomes – Data Centre Rationalisation, Emporium, Digital Foundry, and other adjacent programmes. CIRRUS realises the Defence need for an effective delivery model to provide clear roles and accountabilities that enable faster decision-making and accelerated delivery of a matured MODCloud platform.

Unconstrained Access to Data

Leveraging the investment on exploitation and innovation capabilities, such as the Digital Foundry and Defence Artificial Intelligence Centre (DAIC), Defence will transform data to become a cloud connected enterprise, underpinned by an optimised business model for data exploitation that ensures data is available and fit for analytics and analysis to drive better insights and outcomes.

Architectural Guidance & Best Practices

Good architecture practice will ensure the right principles, reference architectures, and common patterns are available to ensure consistency and stability across our cloud ecosystem. The Digital Backbone is underpinned by the Common Technology Architecture (CTA), a framework and architectural approach under which detailed technical definitions of the underlying components and services are developed.

Transformation (Culture & Behaviour, People & Skills, Technology)

Changing our culture and behaviours will enable delivery of services that drive the most value from cloud and bring to life a cloud that aims to be the "first choice for Defence". Efficient delivery and consumption of cloud services requires us to transform our workforce, embed cloud capabilities across Defence and adopt appropriate and effective technologies.

Partnerships

Frequent FLC and TLB engagements help us to identify practical issues, pain points and blockers. Partnering with best-in-class suppliers from Industry ensures Defence's requirements are continually addressed, enabling successful delivery against our cloud objectives, and realising our vision of exploiting a world-class cloud capability across Defence.

Cloud Delivery Model & Governance

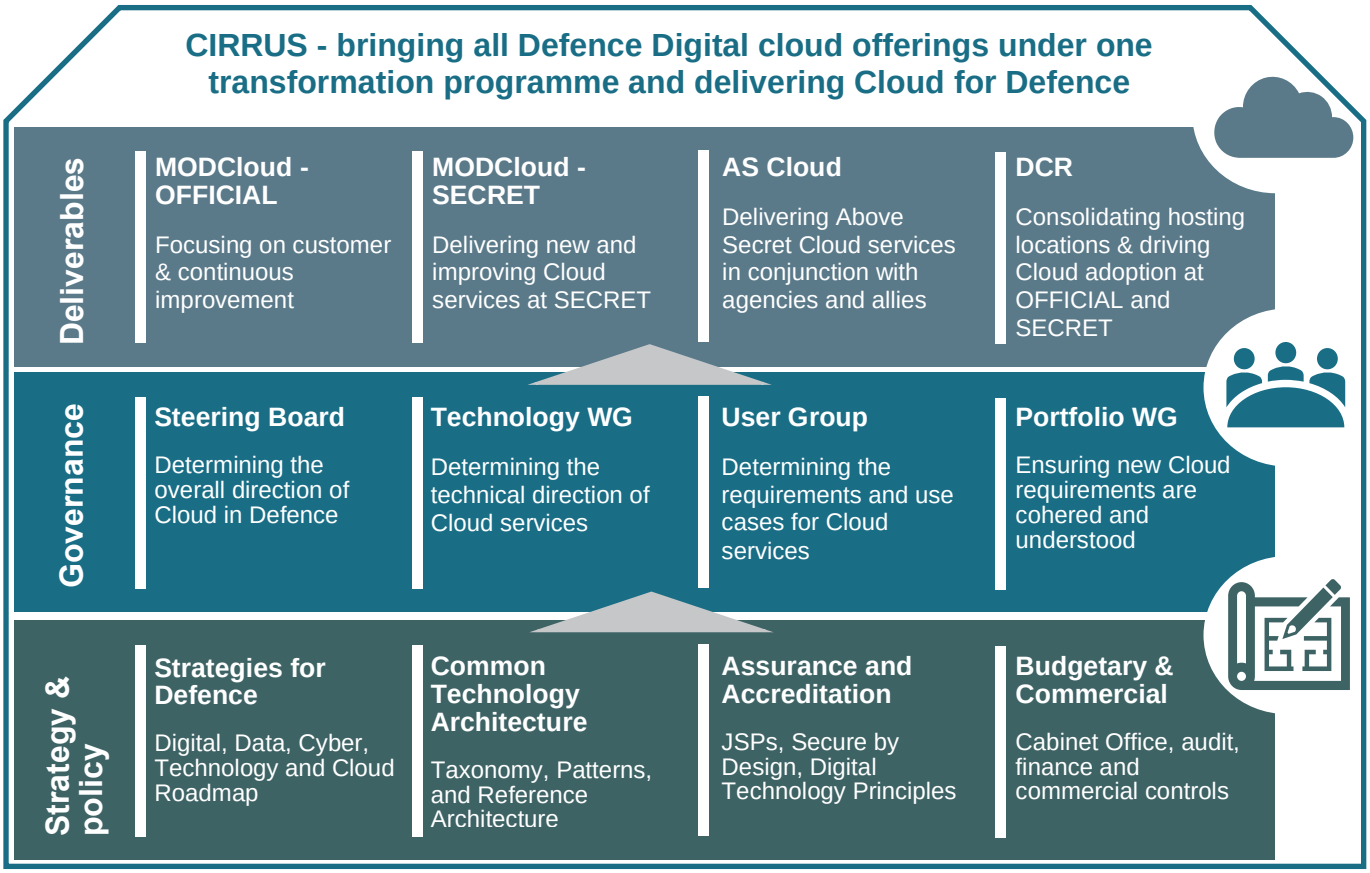
Delivering cloud and realising the Digital Backbone requires a streamlined and effective delivery model.

Slimming down the bureaucratic vehicles

There is nascent coherence amongst Cloud programmes, but the organisation is not yet fully aligned around roles and accountabilities. This mirrors a culture that needs shifting to become more agile and user centric.

CIRRUS will provide an effective delivery model that is coherent across the Digital Foundry, Data, Cyber and other areas to realise the Digital Backbone. **The CIRRUS delivery model will provide faster decision-making, clear accountabilities and accelerated delivery** – "joining the dots" within Defence Digital and across the wider Defence landscape.

The model needs to develop buy-in and shift its existing mentality to celebrate successes of MODCloud, communicating to end-users and key stakeholders (FLCs, TLBs etc.).



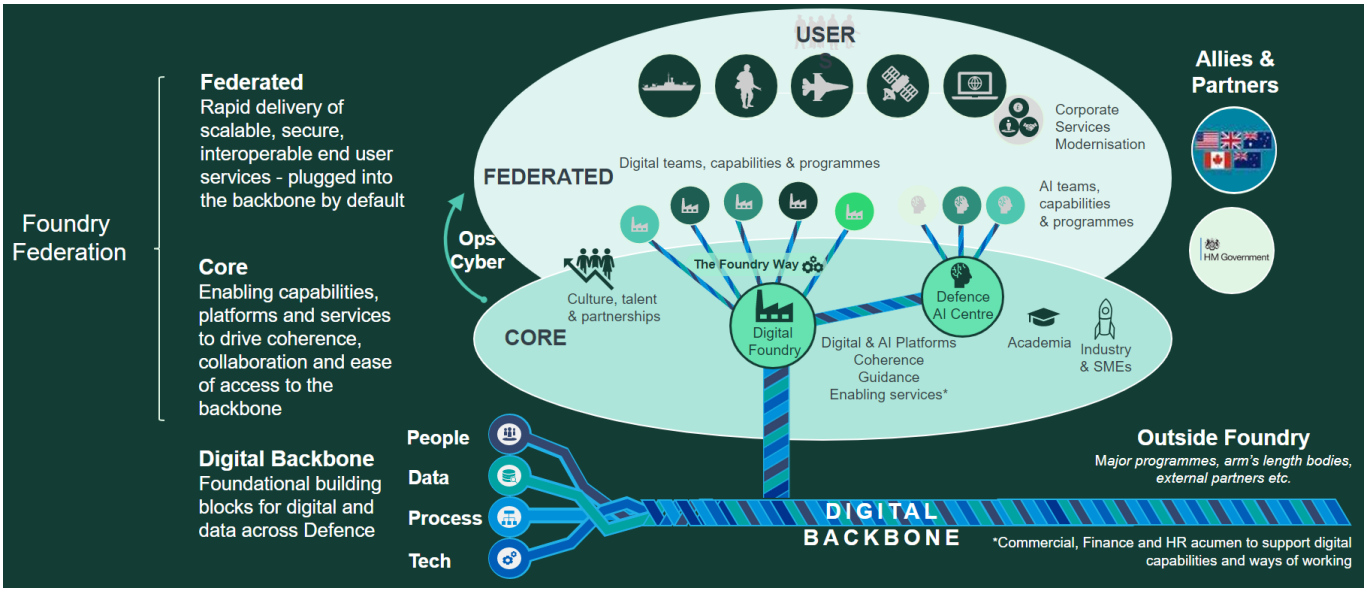
The delivery model will introduce the roles and responsibilities needed to make our cloud services **easy to use** for our defence end-users. Our people will focus on the services, rather than the product, and will collaborate with our front-line commands to deliver cloud.

Unleashing Defence Data

Enabled by the Digital Backbone, the Digital Foundry is unleashing the power of Defence's Data, exploiting Artificial Intelligence and other game-changing technologies.

The Digital Foundry was established in partnership with HMG and the best of British industry and academia, to deliver a unique digital exploitation capability across Defence, and includes the Defence AI Centre (DAIC). The Foundry will leverage all Digital Backbone components (people, process, data, and technology) to rapidly solve problems and deliver operational solutions to Defence users in near real time.

The Foundry is central to the delivery of digital capabilities into the hands of the Armed Forces by leveraging the investment MOD has made into underpinning technology. A key enabler to its successful delivery is the provisioning of accurate, reliable, and interoperable data to power digital exploitation efforts.



Secure data exploitation

Exploiting the amount of data required to support our warfighters means that Defence will be increasingly interconnected via public connectivity.

This requires Defence users to shift mentality towards balancing risks and cloud exploitation.

By combining Defence policy and guardrails, the principles set out in Secure by Design and the significant ongoing investment made into cyber security by the cloud Hyperscalers, we will enable Defence to secure our evolving infrastructure.

We need a modern, agile, and scalable cloud infrastructure to exploit our data

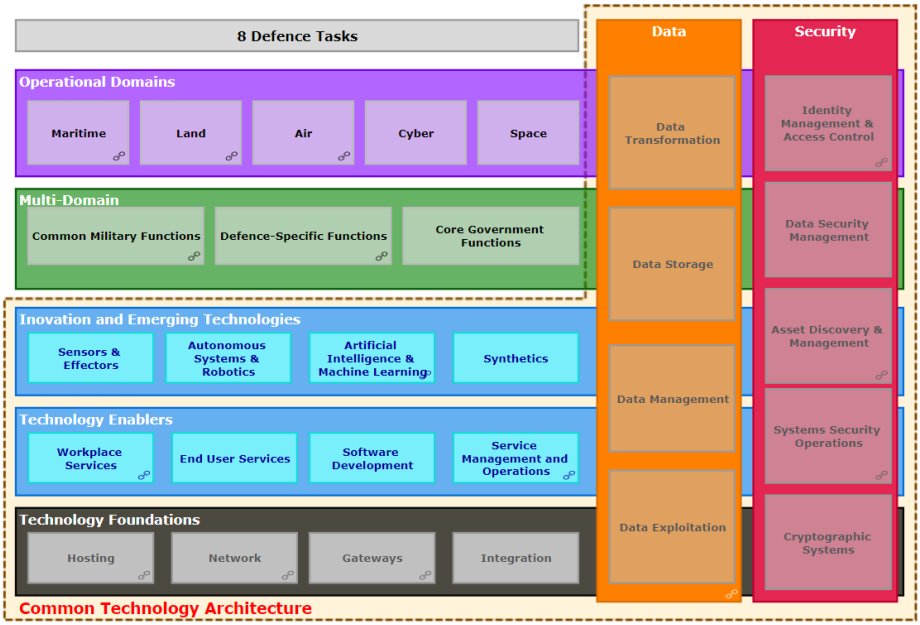
Cloud platforms and services provide the building blocks to achieving the Defence's Data Strategy's ambitions. Defence needs to transform from a "need to know and platform centric" to a "need to share and data-centric" connected enterprise.

As Defence's curated data starts to flow seamlessly between users and across platforms, a truly connected Enterprise will deliver integration, nationally and internationally, across all five domains: Maritime, Land, Air, Cyber and Space.

Defining Defence Architecture

Cloud services underpinned by reference architectures, common patterns and recognised standards that make utilising cloud services more secure, coherent, and interoperable, and providing consistent cloud deployments across Defence.

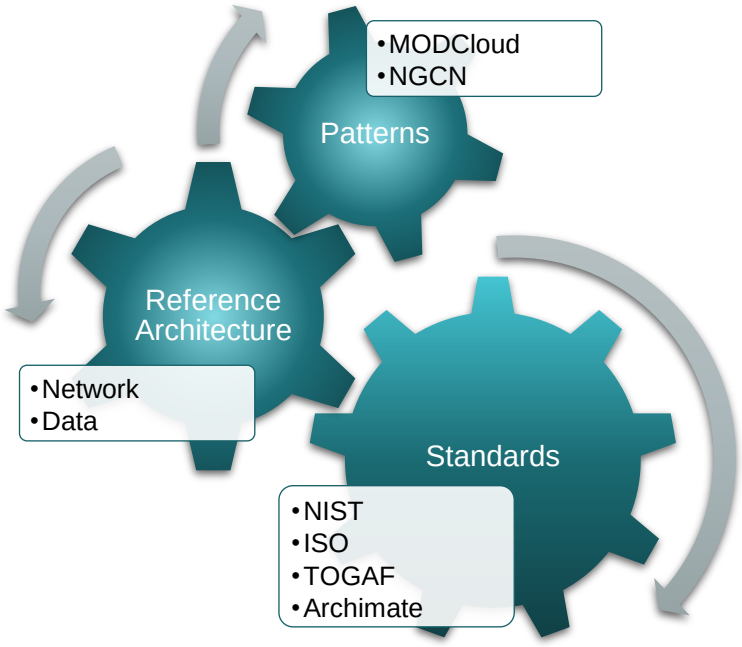
The Common Technology Architecture (CTA) is a framework and architectural approach under which the detailed technical definition of the Digital Backbone and its underlying components and services can be developed. It also serves as the framework of policies, standards, and reference patterns against which the delivery and adoption of the Digital Backbone can be guided and governed.



The policies and standards that will underpin the CTA will set the rules to be followed, both internally and by external partners, to ensure coherence across the technology estate and enable Defence to fully realise its vision for seamless data sharing, integration, and interoperability.

Providing the right architecture at the right time

Due to the complexities of cloud adoption around interdependencies, network integration, data dispersion, security, and assurance, it is essential when designing for cloud to have access to the correct architectural guidance which conveys best practice and signals common pitfalls.



Architects within Defence will work with FLCs, TLBs, and Industry Partners to ensure the correct CTA artefacts are available to support both implementation of appropriate cloud capabilities matched to requirements, and adoption of cloud services by stakeholders on their migration journey to cloud. These artefacts consist of Patterns, Reference Architectures and Standards that will build up over time to provide an evolving reference library of “building blocks” which can be used across Defence.

Culture & Behaviour

Effective delivery and consumption of Cloud services requires us to shift our mentality and streamline our processes.

Our vision is for a more coherent Defence with common standards, governance, and process to exploit Cloud technologies across the enterprise.

We will meet the standards set within the Common Technology Architecture (CTA) to ensure consistency.

We will approach the management of infrastructure in a consistent way, including standardising patching, configuration, change, incident and problem management processes.

Given the exponential rate of technological change across Defence, getting the correct culture to enable design, delivery and operations of Cloud services is critical.

Our vision is for a more coherent Defence with common standards, governance and processes realising the Digital Backbone.

The cultural shift needed will allow us to:

- **Treat Cloud as a campaign,** predicated on a clear vision and pan-Defence communication, making the business part of the solution, identifying decision makers and empowering individuals to execute rapidly
- **Drive seamless procedures,** accelerated accreditation and billing processes that will allow our cloud consumers to establish their environments promptly and easily

What needs to be done?

To achieve our vision of a more coherent Defence that embraces the cloud transformation journey, we must drive consistency, cohesion and integration in a number of key areas:

- **Culture Shift**– A significant culture shift is required that embodies the principles of a coherent, interoperable and collaborative Defence. Leaders across defence will drive adoption of centrally provided cloud services within their areas, encouraging and empowering collaborative teams to innovate and exploit cloud native services in an incremental value driven manner.
- **Communicate Success** – Defence will be brought together in a cohered cloud transformation journey that is clear on its intent, inviting and enticing all personnel to be active participants and contributors to its success. Marketing that depicts this collaborative journey, celebrates success and endorses the use of cloud technologies will be produced.
- **Delivery at pace** – The systems, processes and organisational structures required to support cloud transformation will be adapted to make decisions quicker, delivering cloud deployments using the common templates and by convening multi-disciplinary teams around selected goals

People & Skills

Delivering Cloud capability across defence is as much about the People & Skills as it is about the technologies that underpin it.

Effective delivery and consumption of cloud services requires us to transform our workforce and embed cloud capabilities across Defence.

Realising Cloud's full potential requires us to foster an environment where all personnel are cloud aware.

We will organically embrace cloud services at a greater scale and empower our personnel to explore, innovate and interact with emerging technologies and deliver against our future technology ambitions.

We need to keep pace with the increased capabilities of our adversaries, ensuring we have access to the specialist skills we need and at the scale required to deliver against our ambitions.

Demand for these skills is high and deploying the right skills at the right scale will require us to maximise our brand, offer unique experiences, and most importantly, invest in the development of our people.

Developing the Cloud talent for Defence will involve a step change in the types and volumes of key skills, achieved by:

- **Raising motivation to pursue a mission,** employing the right people and attracting talent
- **Reprioritising skills** and upskilling key talent pools to foster cloud knowledge and expertise
- **Learning from vendors / scaling through partners** via commercial mechanisms that deliver outcomes cost-effectively
- **Acting in a co-ordinated way** so cloud skills are used efficiently across Defence programmes and customers

What needs to be done?

Defence needs to enhance its cloud skills to drive accelerated cloud adoption and exploitation of emerging cloud technologies, by focussing on:

- **Skills Frameworks** – Cloud skills need to be recognised and embedded into Defence's skills frameworks, with clear career and progression cycles and learning pathways. This will provide Defence a means to deliver our cloud-aware workforce and a tangible means to invest in the development of its personnel.
- **Diverse Workforce** – Our people are our most important resource, and innovation and exploitation of emerging cloud technologies will only thrive if there is a diverse mix of skills, experience, thoughts and approaches.
- **Evolved Delivery Model** – Our Defence Delivery Model must continue its evolution to deliver the Cloud capability that Defence needs, which brings coherence amongst cloud programmes and the consumers of cloud.

Technology

Cloud is at the core of a truly integrated Defence organisation.

To support this ambition we must replace our legacy infrastructure with robust cloud services across multiple classifications, utilising public, private and community clouds where appropriate.

We will benefit from a SECRET Cloud fully capable, to enable data sharing across Defence, with similar capabilities considered for TOP SECRET.

Data Centre Rationalisation will address obsolescence, leading to secure and cost-effective hosting.

Hyperscale cloud will provide the foundations to deliver the coherent and secure future capabilities in Defence.

Cloud is fundamental to delivering world-class information and services in the right place and at the right time for all Defence users.

We will adopt a modernised, agile approach to adopting cloud, that is incremental, iterative, and based upon tangible outcomes, delivered through a programme model that suits the infrastructure Defence needs. We need:

- **Technology:** we will realise access to the best of breed cloud capabilities and services available
- **Tooling**: we will drive change by empowering our teams and providing the right management tooling
- **Self-Serve portals**: easily consumable and standardised portals for our Defence end-users

What needs to be done?

Defence needs to accelerate the adoption of cloud technologies, to deliver:

- **Hyperscale cloud** – Provision of hyperscale cloud services across all classifications, consumed everywhere they are required, providing the foundations to deliver future capabilities and drive emerging technology adoption. Cloud services will be delivered across a range of SaaS, IaaS, and PaaS offerings, using public, private and hybrid models, including at the edge.
- **Rapid Deployment** – Common tools, processes and service wrappers that support rapid deployment of cloud accounts and cloud infrastructure in an automated, self-service approach that embraces the “Deliver IT Faster” imperative of the technology strategy for Defence. Access to cloud environments to provision and configure capabilities via standardised portals, and automation of common patterns through delivery of Infrastructure as Code (IaC) – another key enabler that will make cloud adoption user-friendly for Defence Customers.

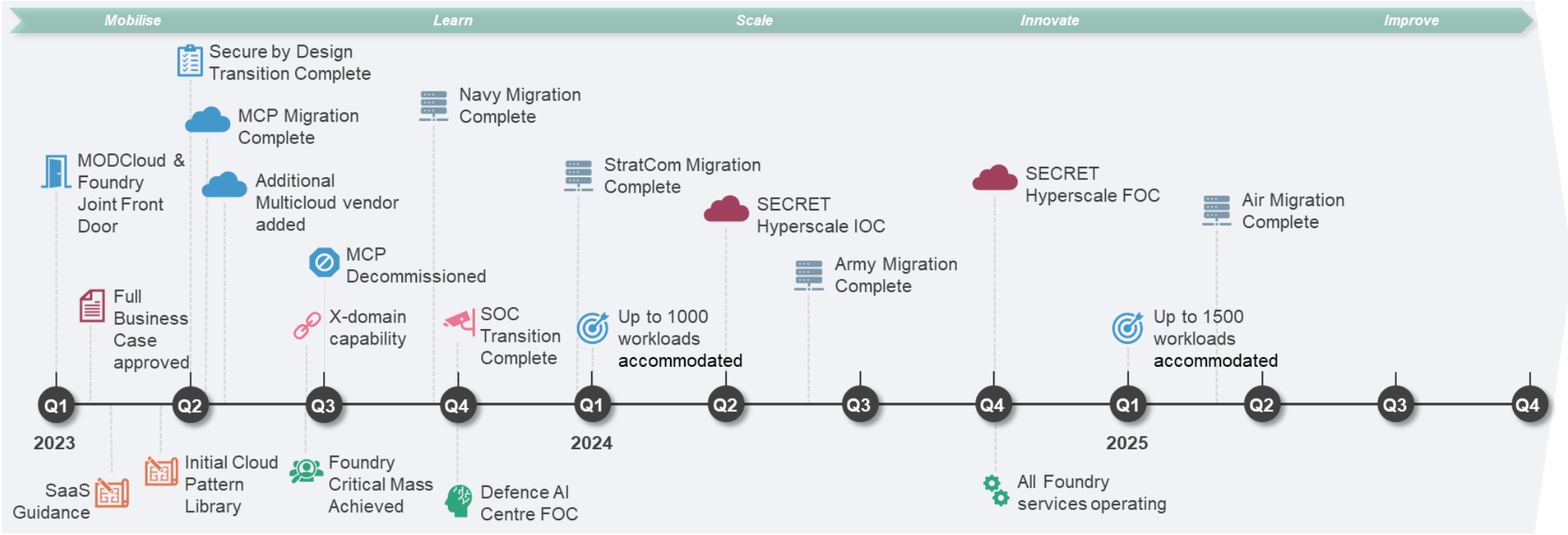
Partnering with the best in the world

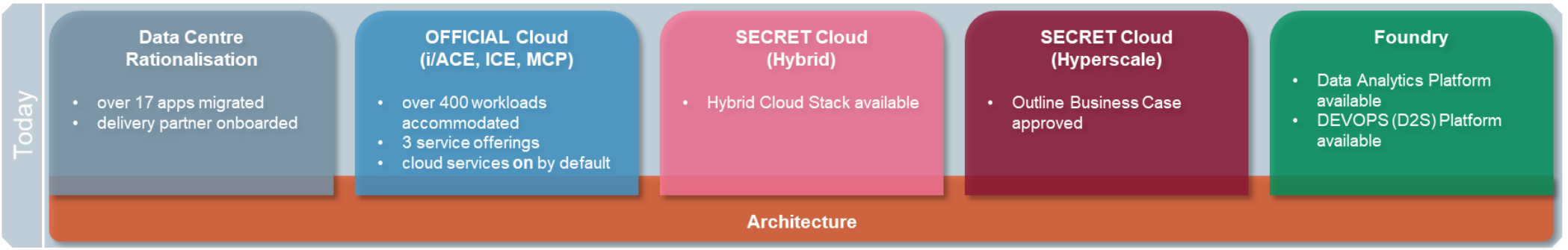
Realising the strategic outcomes requires very specific technical capabilities. Defence will partner with best-in-class providers to take advantage of their cutting-edge service offerings.

We will form a strategic ecosystem of cloud service providers to obtain access to the required hyperscale cloud services at all classifications - including but not limited to Compute, Storage, Database, Network, Big Data storage and analytics, Artificial Intelligence, Machine Learning, Robotics and Synthetics.

	Outcome 1: Delivering a secure and scalable platform to gain strategic military advantage	**Outcome 2:** Driving innovation through evergreen technologies by default	**Outcome 3:** Driving exploitation to realise benefits around efficiency and economic value	**Outcome 4:** Empowering digital age warfighters through our world-class capability	**Outcome 5:** Realising greater benefits by integrating with industry partners within the cloud ecosystem
Technical requirements	• UK footprint, with a number of availability zones and regions • Resilience within data centre, resilience within regions • Scalable services, classified services, choice of service across all aaS model, • Localised platforms and services	• IaaS, PaaS, SaaS broad service offerings to profile core functionality and to realise exploitation of more complex technologies • i.e. (Space Simulation, Synthetic Environments, Virtual Command posts etc.)	• Consumption commitment programmes that provide cost efficiencies as we consume and scale our cloud infrastructure • Incentivisation programmes that provide SME and migration support during transformational activity	• Right services to deliver cutting-edge technologies – i.e. AI, ML, Digital Twins capability • Being able to scale these services to meet demand across all environments, through software and automation • Access to skills and capability to satisfy demand	• Agility to deliver via software (and therefore through public cloud) to establish routes of networks across all environments. • Ability to leverage partner capability • Provide a platform for industry to utilise (especially at SECRET)
Provider considerations	Tier 1 providers are globally recognised, have data centre footprint across a large geolocation, and are already investing significantly in Defence. Tier 2 providers are best suited for niche use cases but may not offer the scale and specific services required by Defence.	Tier 1 suppliers invest in research and development and constantly release new services. They see demand and they innovate through intelligence and demand from customers. Tier 2/3 are more constrained as they provide fixed services with the defined (use tier 1, line in tier 2 if needed).	Tier 1 providers have defined incentivisation programmes with clear timescales for benefits realisation, which makes it easier for Defence to budget. Tier 2/3 providers' fees are subject to negotiations and subject to managed services, incurring a lengthier process.	Size and scale at unpredictable times ingesting volume data, where we're no longer required to configure from new, but must be able to leverage pre-deployed services from the marketplace accelerating time to deliver at the edge. Tier 1 providers have the ability to respond to this requirement.	By leveraging public cloud and Tier 1 suppliers, we build the ability to connect with partner systems, allowing to integrate and share data with the community. Tier 2/3 providers do not have the scale to cater for this requirement.

Cloud Capability 3-year plan






BARCO
NRR3
NO STEP
FOLD DESK BEFORE MOVING SEAT
EMERGENCY EX

Appendix

Defence's user needs

Deployed Persona:

"I support frontline users and those in the Tactical Edge and provide the information and services they need as quickly as possible"

What I need from Cloud:

- Cloud must be available at Mission SECRET
- Common AI/ML and other tools used by commercial cloud services
- Tools for Big Data exploitation
- Process, exploit and disseminate data at point of collection
- To have access to cloud in deployed or disconnected environment
- Process at scale in disconnected environment
- Easy to collaborate with commanders at Tactical Edge

End Users are at the core of Defence's decision making.

While specific FLC requirements (see Appendix) may differ from one another, all Defence users have a set of common requests that help drive the way we shape our cloud ecosystem and our approach to architecture.

Our Defence End-Users need:

- **Innovation at the Front Line** - Take advantage of the latest in AI and Machine Learning technologies
- **Increased Interoperability** - Share data between classification levels, across Defence, and with allies
- **Reduced Costs for TLBs** - Reduce spend on infrastructure & maintenance across Defence
- **Reduced Risks** - Reduce downtime, increase survivability and enhance protection against enemy attack
- **Increased Efficiency at the Tactical Edge** - Increase speed of operations and introduce more automated processes
- **Scalability and Agility** - Rapidly expand volumes of data handled, processed and transmitted to Land, Air and Sea

---

Defence needs common tools and capabilities that users feel hyperscale enables or makes easier to use, including:

- API Management Layer as a Service – particularly Data/API Catalogue and application integration enablement
- Machine Learning, including those for Natural Language Processing and image analysis
- Virtual Apps and Machines
- Cloud databases
- Azure / AWS tools favoured by most with some such as DSTL leaning towards Google Cloud Platform tools
- Along with catalogues and APIs to make it easy to find and use these tools

What is Cloud for Land, Air and Sea?

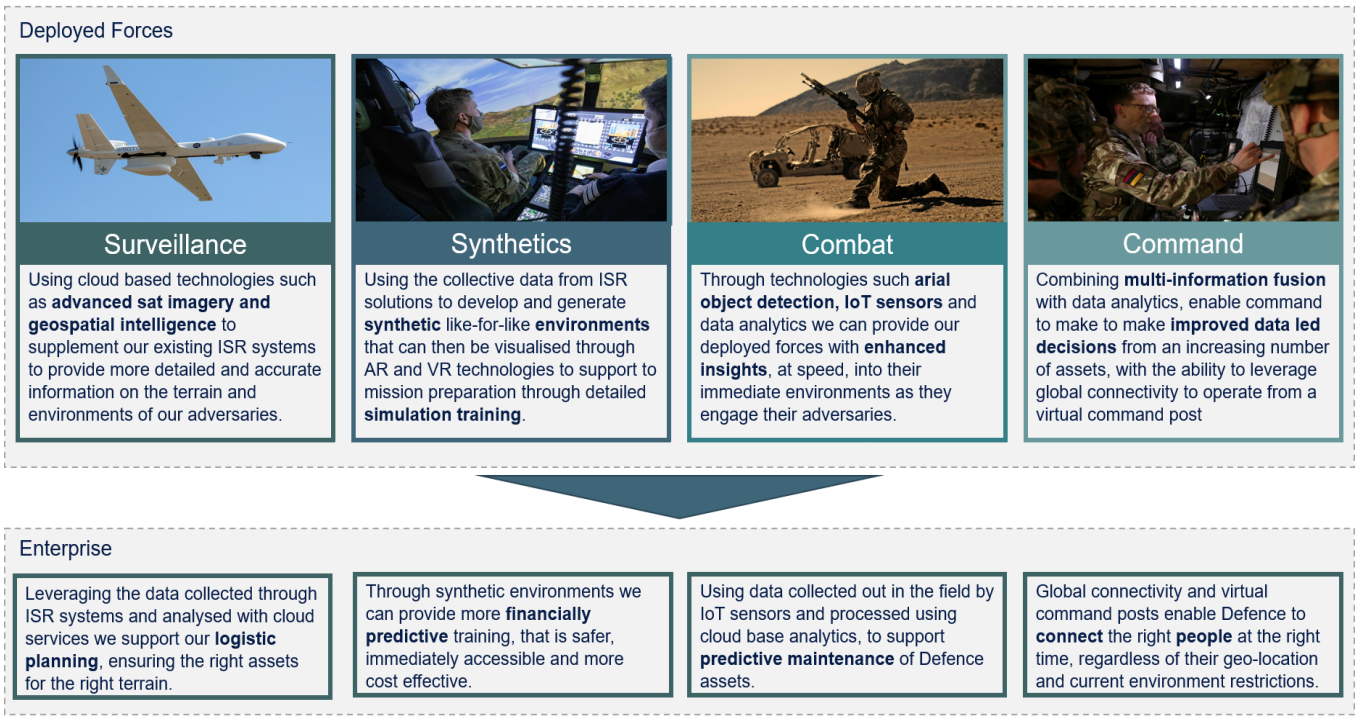
By modernising our legacy estate and fully addressing our technical risks, **Defence users will be working on robust, interoperable and cost-efficient technology infrastructure**. Hyperscale cloud will be available at multiple classification levels, providing the foundation on which new technology services can be rapidly built, adopted and scaled.

Security will be 'baked in' to our technology by design. New architecture standards and smarter governance processes will ensure that our technology remains future-proof, coherent and interoperable across Defence. We will deliver efficiencies by bearing-down on single-use platform designs and rationalising the application-set, building solutions with reuse and portability at the heart. Users will be supported by world-class digital and data services to enable them to rapidly exploit the value of emerging technologies to transform military and business outcomes.

What Cloud Will Enable		
Data Exploitation	Advanced Compute	Edge & IoT
For the soldier on the ground, this is provided as an overlay to augmented reality goggles allowing them to navigate the complex environment and to identify possible threats based on the intelligence provided by the processed data feeds.	**Autonomous UAVs that are able to intelligently identify and locate any threats** in the battlespace using AI while seamlessly transmitting stream data to central mission command.	**Initial intelligence gathered by a combination of satellite, sensors on submarines and human intelligence** identifying enemy areas with initial reconnaissance providing training data for AI pattern recognition.

Game-changing technology deployed pan-Defence.

In all areas of Defence, there are many uses cases where cloud technologies would provide increased efficiencies and enable improved capability, with no area more important than our deployed forces. It's critical that we exploit cloud services that unlock our core assets, such as data, to better prepare our deployed forces in the battlespace.



Understanding the demand signal

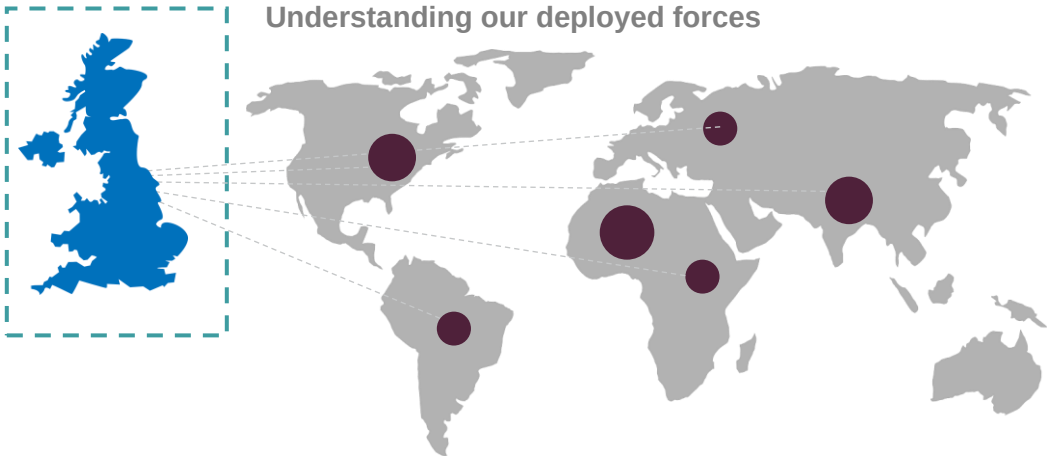
Understanding Defence's demand signal is pivotal to selecting the right cloud solution for Defence. There is a set of characteristics that builds the demand signal. Signals generated by our deployed forces will be very different from those generated from corporate HR or business services, because:

- Deployed forces are typically a smaller user population of military personnel, providing time critical services
- Enterprise organisations are a larger user population, providing less time critical services

One of the examples is from PJHQ. There are 4000 people directly under CJO's command. PJHQ has ~600 people in the headquarters and 25 named operations, the largest of which has 300 people.

Each operation sits in its own data domain. In wanting to establish a services stack, PJHQ will need to look at all of them individually, because the only common denominator is belonging to the UK. For example, there might be a UK domain operation shared with Kenya, and adjacent there might be some activity supporting an EU mission in Somalia. Neither of those share between each other but they have UK domains in common.

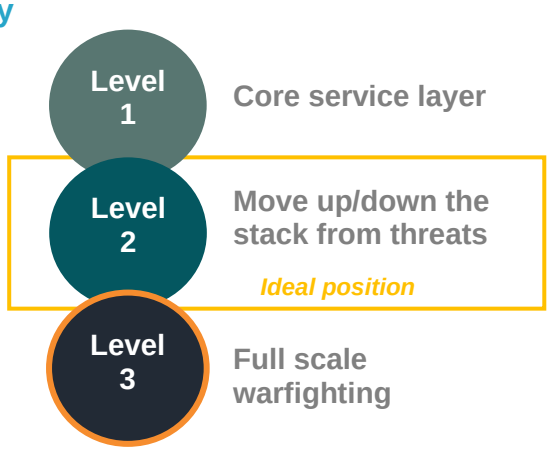
Out of any of those operation environments, Defence must be able to scale – any of those 25 operations could unpredictably escalate to full scale warfighting.



Cloud satisfies the unpredictable need for scalability

Full scale warfighting requires immediate scalability. Transition to full scale warfighting determines the level of resilience needed, and in a Level 3 scenario the networks and core infrastructure will likely be under cyber-attack.

Deploying across the cloud ecosystem - underpinned by the CTA - will provide greater resilience through highly available, fault tolerant services provided by the Hyperscalers. Whatever we build and design will be secure by design, resilient and interruption tolerant.



The voice of Defence's customers

Our "Tour" to understand Defence Users brought to light these requirements:

"We require scalability at unpredictable times. Cloud needs to be secure by design, resilient, interruption tolerant.**"**	**Technology**	**"We need an interim Oracle cloud to cater for our legacy estate (MyHR, Future JPA, 60-80% of DBs)."**
"We urgently require a **Delivery Model** in place to realise the Strategy – with clear roles and responsibilities."	**Delivery Model**	"We need confidence that strategic outcomes are realisable."
"There needs to be a shift to a more **agile approach and mentality."**	**Cultural Shift**	"We have an urgent need for clear onboarding and **end to end process,** including point of contacts."
"We need clear **communication on the landscape** to feel empowered to consume cloud services i.e. security and data sovereignty."	**Comms**	"We want to know how much of the strategy we want the FLCs to own and fund."
"We need clear mechanisms for costs relating to cloud and multicloud deployments."	**Cost Mechanism**	"We have concerns related to pay as you play, OPEX is challenging to fund."
"We need a pool of **architecture blueprints**, to enable streamlined delivery teams."	**Architecture**	"We need architectural patterns to build & deliver services at the edge."

Ministry of Defence · Royal Navy · Army Be the Best · Royal Air Force · de&s · Strategic Command

and more…

Cloud will deliver a “Step Change”

Innovate at the Front Line

Take advantage of the latest in AI and Machine Learning tech

Applications like “Improbable”, a simulation environment at the forefront of wargaming

Increase Interoperability

Share data between classification levels, across Defence, and with allies

Cloud services are at a cornerstone of e.g. NATO Interoperability Standards

Reduce Costs for TLBs

Reduce spend on infrastructure & maintenance across Defence

MODCloud OFF-SEN will deliver ~£52m[1] in cost avoidance across UK Defence over next 5 years

[1] Per Emporium Business Case

Reduce Risks

Reduce downtime and enhance protection against enemy attack

Cloud providers can respond to security risks faster than services from individual TLBs

Increase Efficiency at the Tactical Edge

Increase speed of operations and introduce more automated processes

Automate labour intensive tasks like inventory and supply chain management

Provide Scalability and Agility

Rapidly expand volumes of data handled and processed

Facilitate better use of capabilities at the Tactical edge e.g. F35 jets, can capture gigabytes of data

Addressing some practical issues

Front Door

Our "Personal Shopper" provides a seamless, value driven experience.

The MODCloud front door process focusses on outcomes when engaging with its customers, providing the required direction to which elements of the MODCloud ecosystem are most suitable, underpinned by knowledge of the cloud ecosystem, dependencies across infrastructure and the implications into wider initiatives. Facilitating this approach, a **'personal shopper'** is offered as part of the front door process, providing a dedicated contact point for service owners to interact with. This supports making the customer journey more accessible and informative, driving towards our goal of the MODCloud being the first choice for hosting.

Billing Model

Our billing model will be transparent and easy to consume.

We will require a shift from our traditional centralised billing approach to one that truly embraces a PAYG charging model, providing:

1. **Chargeback mechanisms** - our billing model will automatically enable consumers to understand the TCO for their infrastructure, provide insights into resource usage and shift accountability to consumers, encouraging efficiency and best practice architecture.
2. **Show-back step** - an intermediary step to support our users migrating from traditional on-premises hosting to hyperscale cloud hosting, provides an opportunity for customers to adjust to the new billing model and review their expenditure before being billed in a way they do not yet fully understand – easing accessibility and transformation.
3. **Managed service** – a dedicated point of contact to manage and streamline multiple bills per FLC, by passing queries to the vendors and supporting billing matters. This will enable consumers of MODCloud to focus on delivering business value while the providers of the billing service will support customers with their billing queries and help identify opportunities for cost efficiencies.

Accreditation

Applying new assurance methods as a necessary step in forming our security posture.

Secure by Design is a holistic architectural approach to solving security problems at inception, based on international standards and NCSC guidance. We will shift from the upfront accreditation approach to one of audit and assurance via Secure by Design, enabling rapid deployment of infrastructure while still remaining secure through inflight assurance.

Data Sovereignty

Understanding data sovereignty in a hyperscale cloud environment.

By following the **Data Strategy for Defence**, we will know what data we have, where it is, how it is used, its policy and how to adhere to it, regardless of who has custody over it. Data owners and stewards will be accountable for understanding, maintaining and having control over their data. This approach will support Defence in extracting every drop of value from our data while remaining secure and protected against cyber-attacks from our adversaries.

Ministry
of Defence