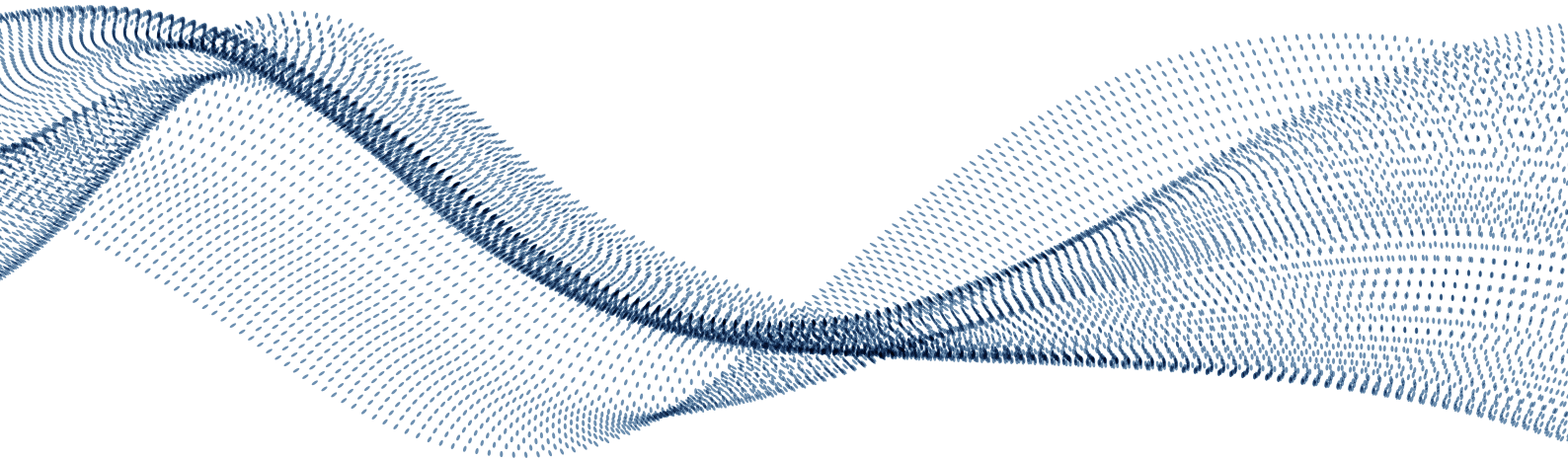
Ministry of Defence

TEAM DEFENCE INFORMATION

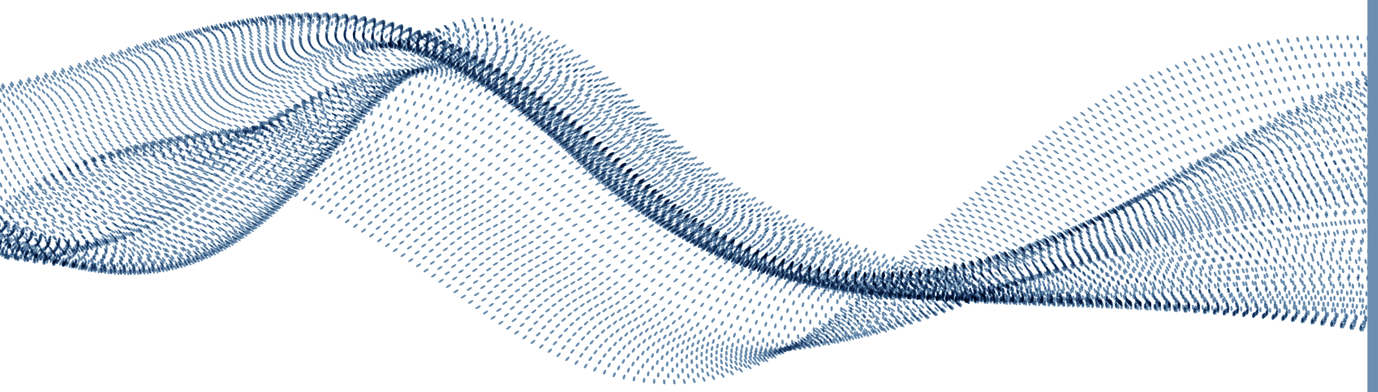


MoD API Strategy Whitepaper for Robotic and Autonomous Systems (RAS)

FCG FUTURE CAPABILITY GROUP de&s

Generate Speed to Value through capability exploration and exploitation.

Ministry of Defence | ROYAL NAVY | ARMY BE THE BEST | ROYAL AIR FORCE | Strategic Command



Ministry of Defence

TEAM DEFENCE INFORMATION

CONTENTS

EXECUTIVE SUMMARY

Robotic & Autonomous Systems (RAS) has the potential to remove people from direct danger, deliver military effect, and enable the UK MoD to outpace, outwit and outfight its adversaries.

To maintain an operational advantage, it is necessary to match and often exceed the rate of change adopted in the commercial sector and by our peer enemies. For many years Defence has looked to adopt open and modular systems architectures to enable technology insertion, accelerate capability development and manage cost through access to commercial solutions. Today's capability is becoming more digital and digitised in nature and as part of the architectural approach, there is a need to understand the potential for Application Programming Interfaces (APIs).

This paper outlines the core challenges that exist today, the resulting impact of these in terms of delivering against strategic objectives, and the opportunity presented by APIs that allow these to be addressed. Consideration is given to wider sector API strategies, industry-leading practices, observations and lessons from the private sector, and the current architectural approach to RAS capability in Defence to provide a number of recommendations and calls for action, namely:

1. **Establish an architecture framework** to ensure strategy, principles, reference architectures, patterns, standards, guidelines, decision-tree matrices, catalogues, and data models are defined, aligned with the business strategy and are available through self-service.

2. **Define and adopt a common functional ontology and data model** to enable better interoperability by allowing data to be linked at the semantic level.

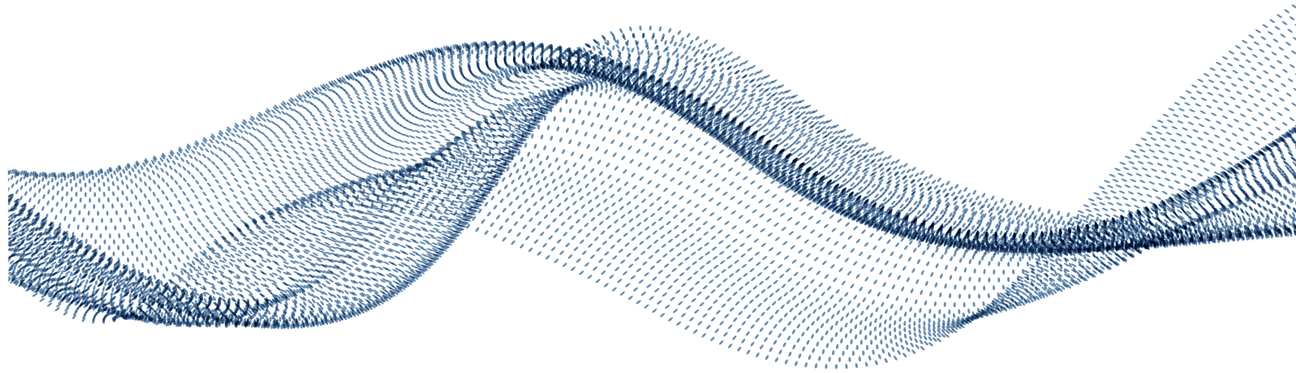
3. **Adopt a composable architecture with levels of abstraction** through an API-led approach to drive delivery agility and reuse while providing separation of concerns.

4. **Expand the logical solution architecture** (outlined in section 5) to define the physical capabilities and technologies, either existing or new, required to deliver against the target architecture.

5. **Create a RAS digital marketplace** consisting of APIs, SDKs, a DevSecOps environment and an online presence offering disruptive technology.

6. **Establish a Community of Interest/Practice** to provide the ability to share and generate awareness of new capabilities across RAS, new frameworks, new Defence/non-Defence related standards, and provide an opportunity for practitioners to showcase work they have undertaken that can be reused in other areas.

Adopting these recommendations will help address the technology, data, people, skills, and talent challenges whereby knowledge is more readily available in terms of open frameworks and standards as opposed to niche custom and closed-system specific skills.



1 CONTEXT & PURPOSE

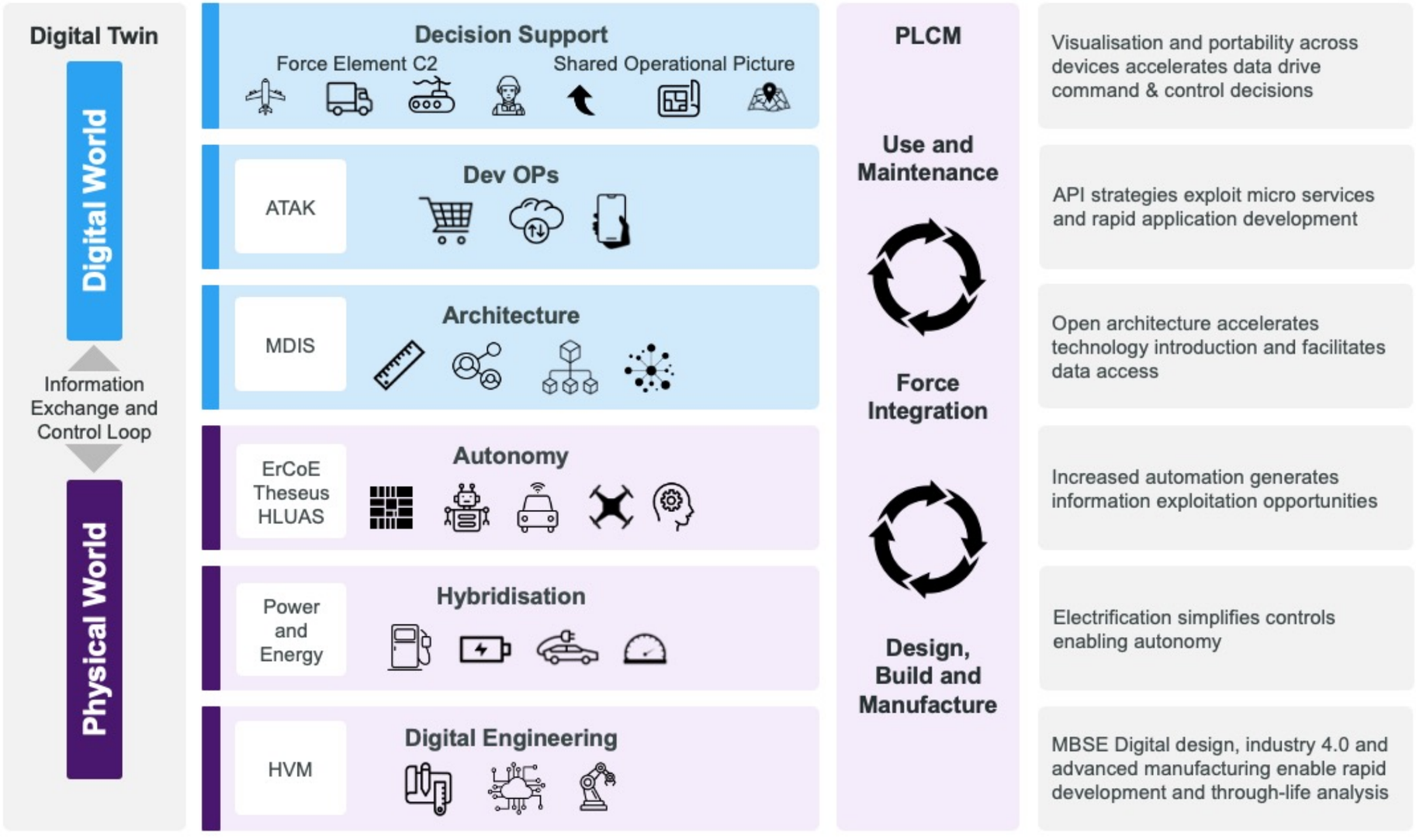
1.1. Context

Integration of Robotic & Autonomous Systems (RAS) in Force Elements, Figure 1, has the potential to remove people from direct danger, deliver military effect, and enable the UK MoD to outpace, outwit and outfight its adversaries. If operational advantage is to be maintained, then we must match (and in some cases exceed) the rate of change adopted in the commercial sector and by our peer enemies. This demands constant step changes to our capabilities however financial pressures dictate that development costs are minimised. Increasingly RAS functionality is delivered by software providing an opportunity for uplift, update, and upkeep of systems at pace.

Within this ecosystem where Modular Open System Architecture (MOSA), DevSecOps and commercial models are key enablers, this paper considers the need for Application Programme Interfaces (API).

Figure 1: *Context Diagram: Force elements comprising of Human Machine Teams operating in a complex, cluttered, contested, and congested threat, and effects environment at reach in all domains.*

Figure 2: *Defence Equipment and Support (DE&S) Centres of Expertise: This paper will assist FCG as it commercialises and integrates disruptive technology into its RAS acquisition and capability development framework.*



1.2. Purpose

The purpose of this document is to consider best practices in the development of API strategies across sectors, identify the value-add activities and artefacts that underpin success then make recommendations for UK MoD to accelerate acquisition and capability development of modular, open, software-driven functionality in RAS, see Figure 2.

2 VISION & STRATEGIC OUTCOMES

Integration of RAS and HMT (Human Machine Teaming) into Land forces will mature over the next decade. Throughout this period and beyond, technological change will continue at pace with the adoption of RAS technologies by Defence and the adoption of advancing technology by our adversaries. To keep up with or ahead of this pace of change, Defence needs to adopt agile approaches to capability development, procuring adaptable systems and solutions enabled by APIs.

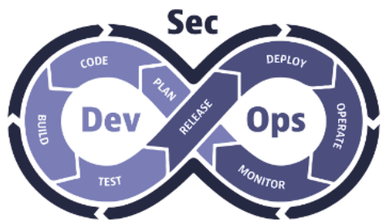
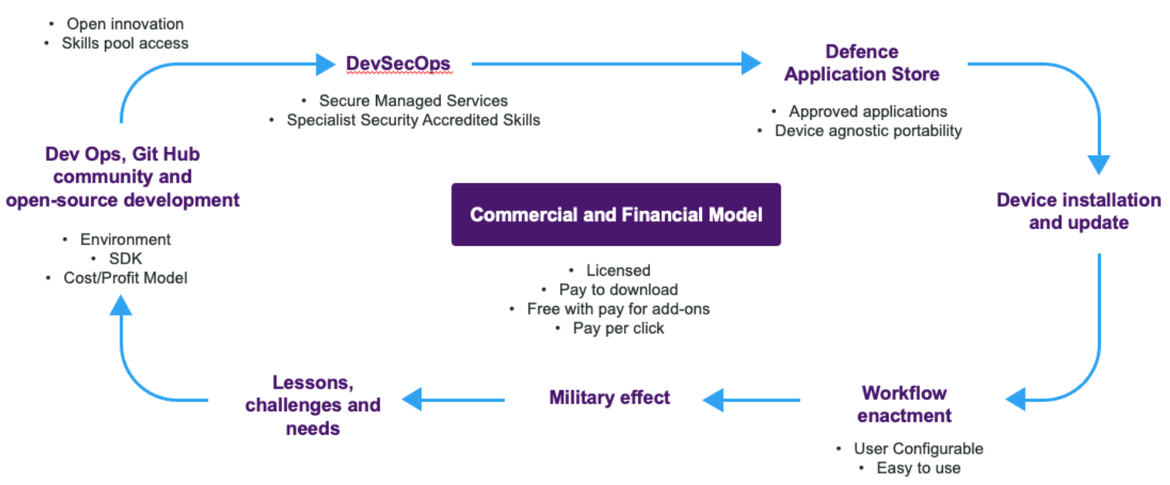


Figure 3: *API DevSecOps ecosystem: Rapid capability development requires a modern value-driven collaborative ecosystem with appropriate security and governance assuring access to talent, development environments and data to enable rapid user-centric capability.*



2.1. Vision

An open API strategy for RAS, coupled with DevSecOps practices, enables rapid update, upkeep, and uplift of RAS systems from a wide ecosystem of cross-sector suppliers providing Defence with access to disruptive HMT capability at pace and ahead of the evolving threat.

Open, modular hardware and software RAS architectures enable multi-function, multi-role RAS to adapt to a wide range of existing and emerging mission requirements. 'Application stores' provide users with access to verified and validated applications delivered using DevSecOps practices as detailed in Figure 3. Rapid delivery of applications utilising open APIs at many layers of abstraction within RAS allows bundling and unbundling of workflows, fostering agility and innovation in the RAS ecosystem while keeping Defence ahead of the pacing threat.

2.2. Strategic Outcomes

Leveraging RAS APIs at all layers of the architecture will enable rapid iteration of capability through continuous integration of new value streams creating revised operating concepts that take full advantage of the latest, more capable systems and components, keep up with and outpacing our adversaries' use of evolving technology.

2.3. Alignment with MoD Vision

The RAS API vision and strategic outcomes align with Defence's direction of travel evident in wide-ranging concept and strategy documentation published by UK MoD since the release of the Defence in a Competitive Age Command Paper[1].

The British Army's approach to RAS[2] demands *"ongoing iterations of experimentation and open Systems Architecture [that] will ensure new technology can be continually added and improved, creating revised operating concepts that take full advantage of more capable systems and sub-systems.* Future Soldier[3] articulates *"integration and spiral development [are] at the heart of all that we do"*. Looking wider, JCN 1/20 Multi-Domain Integration (MDI)[4] states *"MDI is about designing and configuring the Whole Force for dynamic and continuous integration of all global capabilities together, inside and outside the theatre, munitions, and non-munitions, above and below the threshold of armed conflict. The greatest effect will be from drawing in as many capabilities as possible to apply combinations the adversary does not expect or cannot guard against"*.

Opening up RAS by providing APIs at all architectural layers allows agile, iterative, and spiral development of works flow across HMT generating new capabilities in new and unexpected ways.

[1] Defence in a Competitive Age Command Paper, Ministry of Defence, July 2021
[2] British Army Approach to RAS, British Army, March 2022
[3] Future Soldier, British Army, November 2021
[4] JCN 1/20 Multi-domain Integration, Ministry of Defence, December 2020

3 PROBLEM STATEMENT

This section outlines the core challenges that exist today, the resulting impact of these in terms of delivering against strategic objectives, and the opportunity presented by APIs that allow these to be addressed.

3.1. Challenges

The challenges to achieving the vision and strategic outcomes are multi-faceted across people, processes, technology, and data.

3.1.1. People & Culture

The Defence Operating Model is based on the principles of delegated authority between the Head Office, Commands, and 'Enabling' Organisations. It is therefore challenging to ensure coherence across delegated activities using a consistent and joined-up approach. Currently teams operate in silos and/or with the involvement of multiple parties whereby a lack of clarity on accountabilities & responsibilities develops (e.g. data ownership).

Additionally, it is further recognised that the MoD does not have enough people with the right digital and data skills, and it is difficult to fix this skills gap at the pace required. Alongside the need to enhance digital skills, a culture change is also required to create an environment where people can find new ways to reuse existing digital assets and exploit technology through a more agile, risk-taking, flexible, and innovative approach.

3.1.2. Process

It is recognised by Defence that there is a need to rethink long-held mindsets and processes to put the right governance in place in key areas of design, investment planning and programme delivery. Furthermore, changes to the way the information environment is managed is needed to ensure operational integrity and the free, resilient flow of data.

It also demands a change to how services are procured and managed. Currently, based on what's been seen, Defence tends to procure standalone systems over assessing existing capabilities to identify what can be reused and what is missing. This can result in change becoming difficult and expensive. Additionally, lengthy approvals and acquisition processes do not suit the more iterative approach favoured in the private industry for technological change.

The CIO is also currently accountable for the whole Department's use of technology and data but only has direct control of just over 61% of the estimated digital spend. This can lead to misaligned priorities and objectives.

3.1.3. Architecture Framework

Although a number of comprehensive strategies are in place (e.g. Defence Data Strategy[5], MoD API Strategy[6] etc) there is currently no complete overall enterprise-level framework underpinning these strategies in terms of principles, reference architectures, patterns, standards, guidelines, decision-tree matrices, catalogues, data models, roadmaps etc which are available and accessible via self-service. The lack of an effective framework leads to reduced coherence and limited direct line of sight from programmes and projects in delivery mode 'on the ground' in terms of understanding what it means to them while being able to deliver against and conform to these strategies while delivering the business objectives. This limits and hinders conformance to best practice, agreed methodologies, industry standards, interoperability, reuse of digital assets and increases the level of governance.

3.1.4. Technology

Defence's existing IT core has grown organically over many years, with ever-perpetuating technology debt and security vulnerabilities impacting on the ability to exploit emerging technologies at pace and scale[5]. Too often it has proven to be difficult to refresh technology and keep pace with changes due to a lack of integration and commonality.

RAS systems are mostly closed proprietary applications, do not have the ability to talk to one another, do not have open APIs and are therefore not interoperable. The IT legacy estate currently has a mixed ecosystem of different generations of technology ranging from new platforms to closed/black-box systems with either no or a very limited set of APIs. This hinders digital innovation because old and new technologies aren't effectively "meshed" to work together and can only be as fast as the slowest moving part. In addition, there is no ability to effectively discover and reuse digital assets across the application network both within RAS and across wider defence which leads to processes being too slow due to lack of agility, increased technical debt, complexity, costs, and time to deliver.

3.1.5. Data

With a rising volume and complexity of data from an increasingly varied arsenal of sensors and effectors, autonomous and robotic systems, it is harder than ever to isolate the insight from the information. Data is often found to be isolated, inaccessible, not uniformly defined, catalogued, or modelled, not discoverable, not shared, not reusable, held within vertically integrated silos with no clear ownership and inconsistent governance and controls.

Data has particular significance in RAS as data is a design element of the system. Unlike in deterministic applications, where humans code a system's behaviour to react to known pre-determined sets of changes to the environment, RAS systems leverage autonomous models that design themselves based on the training data fed to them. The type, variety, quality, and accuracy of the training data determines how the system evolves in its function, decision recommendation and autonomous behaviour. Data is therefore a prior "design" consideration in addition to traditional post-design considerations such as with "master/transactional" data.

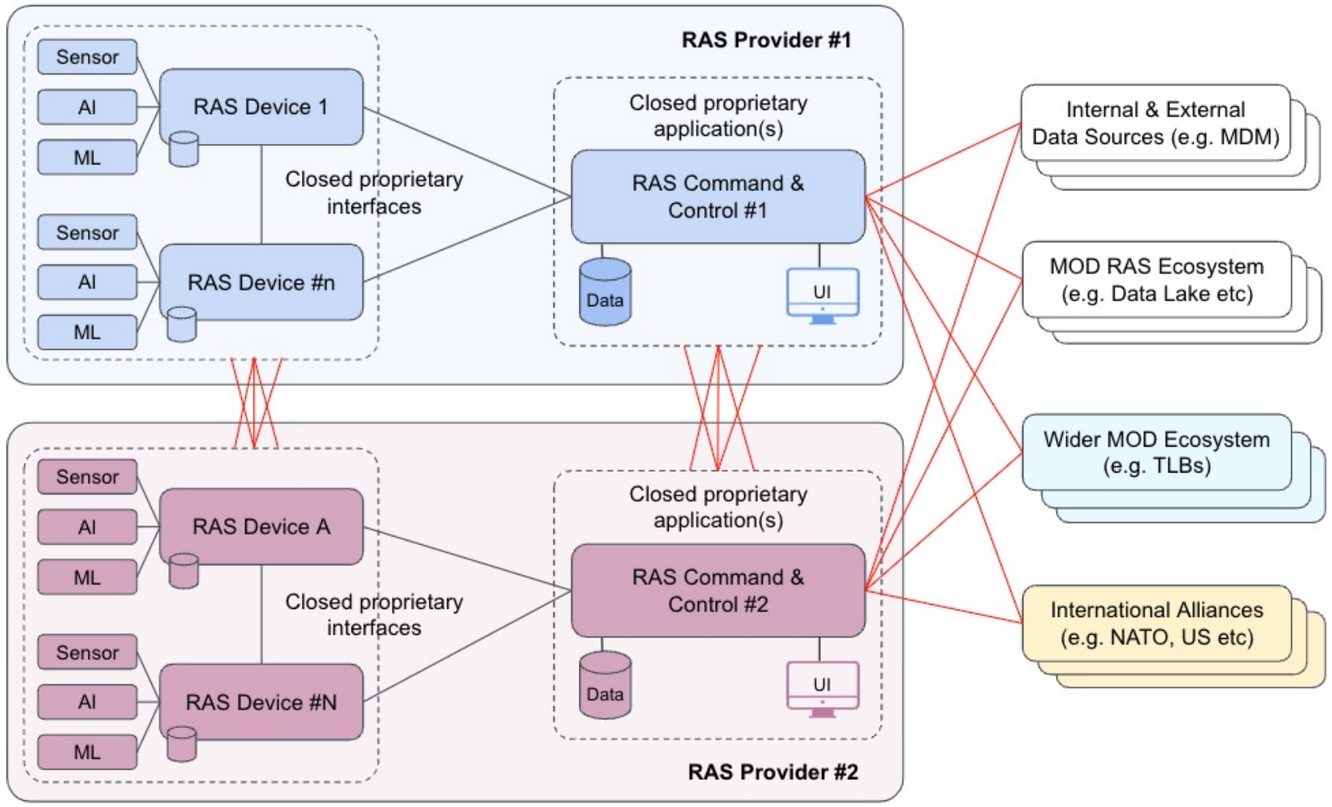
Effective integration is key to enabling the seamless, connected, and secure exchange of data, without which data becomes siloed and isolated and thus loses utility.

3.2. Impact of these Challenges

Effective data management, interoperability, security & integration is hard and complex across the key themes of people, culture, process, data, and technology. These challenges provide a barrier which impacts the ability to deliver against strategic objectives, achieve business outcomes, reduce costs, be responsive to threats and opportunities and innovate and outpace our adversaries through efficiency, speed, agility, coherence and through leveraging best-in-class people, processes, and technologies.

[5] Data Strategy for Defence, Edition 1, September 2021
[6] MoD API Strategy: Data Exploitation in the Modern Age, March 2021

Figure 4: *Outlining the RAS data and integration challenges*



These barriers make it hard to securely & effectively share data across the RAS & wider MOD ecosystems impacting the ability to effectively respond to insights, threats and opportunities in the battlefield

Core Challenges & Impact

1. **Brittle & complex architecture** due proprietary nature of 'closed systems'
2. **Limited 'open' access** to RAS applications, digital services & data
3. **No cross-sharing of data & insights** between different:
   a. RAS devices operating in the field
   b. RAS command & control systems
4. **No single RAS User Interface** for all command & control leading to **no single pane of glass & inefficient operations**
5. **Different end-user training & enablement** needed across multiple RAS systems
6. **High change & operational costs; poor ROI**
7. **Limited ability to share data & insights** with wider ecosystem

Key:

- No/limited integration
- Closed system integration

3.3. Opportunities Offered by APIs

In relation to RAS applications, APIs would typically be provided to support common services such as status monitoring, 3-D control of routes, speed etc., as well as the primary function of recovering payload sensor data. Although different members of the RAS family may achieve these functions in different ways, the users' interfaces with each of them would be common.

To achieve this, the ground-based APIs exposed by battlefield-based RAS devices would be implemented in software and would use the communication link(s) with the RAS Command and Control (C2) to transfer data in both directions. The RAS C2 end of the link would route incoming link messages to activate parts of the RAS onboard functions to, for example, change direction, report status, or send sensor data. Typically, these functions are implemented as a mix of hardware and software, often including addressable hardware registers wired to interact with the mechanical parts of the system (throttle controls, steering mechanisms etc, as well as interfaces with the sensors).

The inherent semi-independence between the API and hardware offers a wide range of technical and commercial benefits, such as:

1. **Improved customer experience**
   The customer can benefit from improvements of in-service performance within the low-level code and hardware without the need to change the interface with it.
2. **Improved automation**
   The hardware, controlled by its low-level software, can perform a range of simple through to complex functions without impacting the API software (user-visible code).
3. **Timescale (cost) reduction**
   Updates, modifications and many fault corrections can be limited to the (user-hidden) low-level software and hardware parts of the system. This can simplify the changes by removing the need to change user-side software.

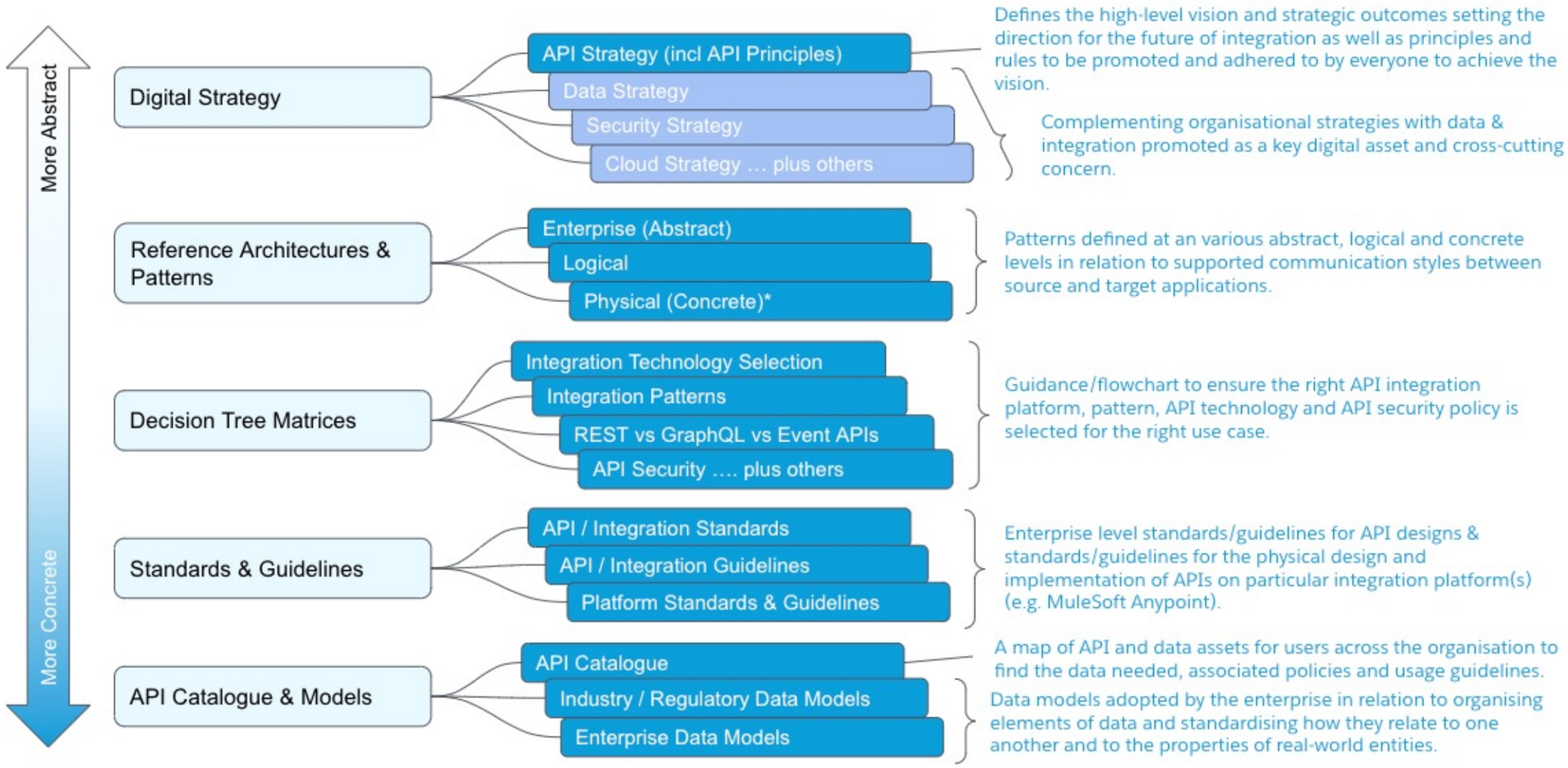
4 INDUSTRY BEST PRACTICES & INSIGHTS

This section provides relevant insights from the private sector which provide a view of how the challenges and problem statements (outlined in section 3) have been addressed elsewhere through effective architectures, approaches, and ways of working.

4.1. Architecture Framework

To provide line-of-sight from programmes and projects to the overarching strategy, it is necessary to define an effective framework which forms the basis of the 'what' of governance. Figure 5 outlines an effective framework which has been used across multiple industries (including Financial Services, Logistics and Distribution) and defines the IT strategy, principles, reference architectures, patterns, standards, guidelines, decision-tree matrices, catalogues, and data models which align with the overall business strategy. The framework provides the artefacts, typically created by an Enterprise Architecture team, required by projects and programmes to make the right technology choices and decisions to align with the strategic vision.

Figure 5: *API Framework providing the ability to govern propositions while enforcing standards & compliance throughout the lifecycle.*

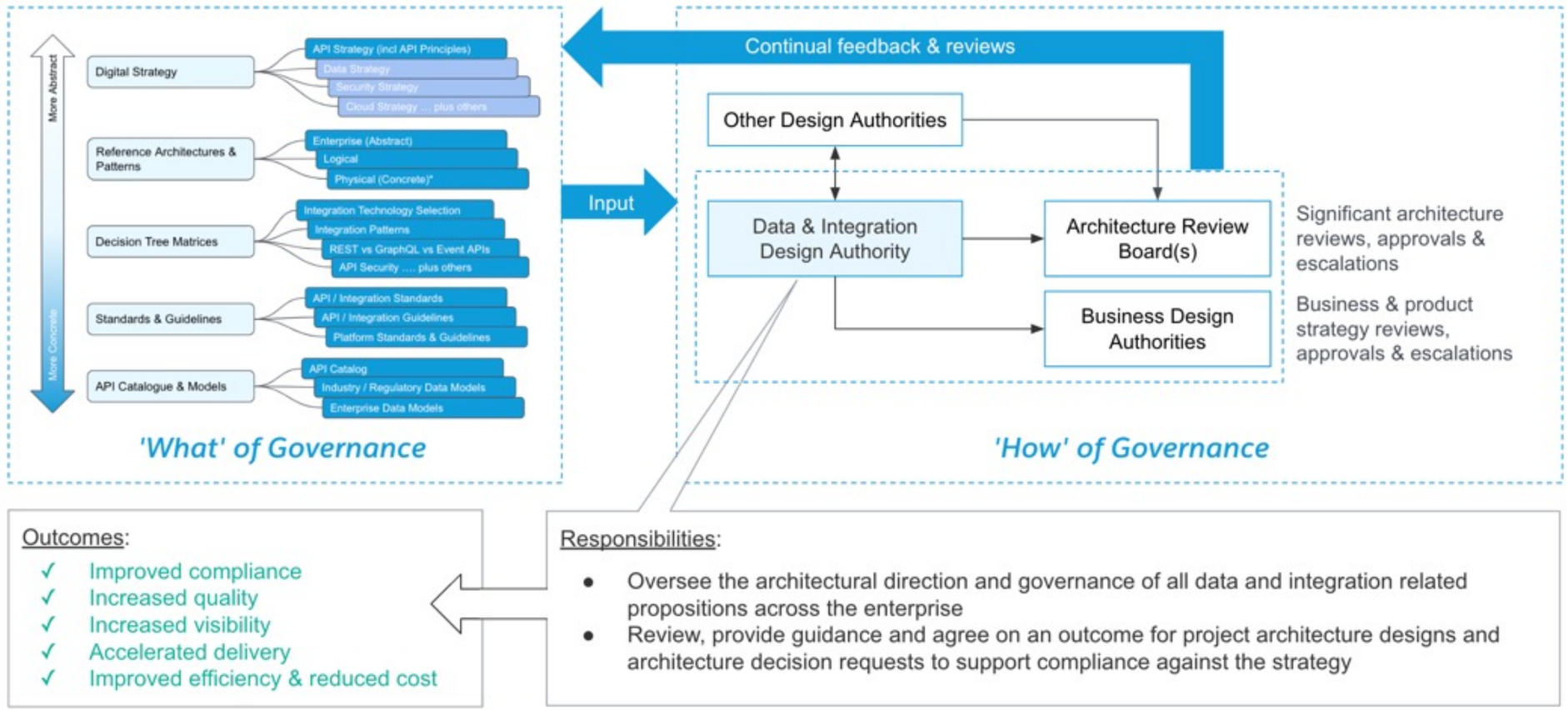


**Delivered by engineering teams with architectural input, support & oversight*

This framework, made available for self-service, can be supported through an effective evangelisation and governance process (i.e. the 'how' of governance) allowing the strategy to be realised through increased compliance, coherence, accelerated solution design and delivery and embedded best practice. Figure 6 outlines a process for governing data & API-enabled propositions while enforcing standards & checkpoints throughout the lifecycle.

Regularly sharing and communicating the evolution of this framework, along with key case studies and success stories through a regular Community of Practice increases community engagement, awareness, interest, and participation.

Figure 6: *An effective operating model for data and integration is needed to provide evangelisation and governance against the strategy.*



4.2. Data Model & Ontology

Organisations that are succeeding in the age of big data are those that have improved data integration and are going beyond simply collecting data. These enterprises are integrating data from isolated systems and data silos to implement a useful data model into business intelligence that can:

-
- Drive vital decision-making through actionable insights.
- Improve internal processes and drive efficiency.
- Indicate service improvement areas and opportunities.

Data integration isn't easy, especially in large organisations where legacy systems and new applications make enterprise architectures difficult to manage, especially due to the different data formats that all these tools support. One solution to this is to define a common data model and ontology to present data entities and relationships in the simplest possible form to integrate processes across various systems and databases. This provides a common language, syntax, and protocol to manage data and for systems to effectively communicate. Effective integration tooling and APIs are needed for this to be successful to provide a layer of abstraction and loose coupling and translate to or from application-specific data models to maximise interoperability.

When defining a data model for an organisation, there are external (i.e. regulatory and industry) as well as internal (customer-defined) data models to consider, as shown in Figure 7. A balanced approach needs to be taken when adopting an industry and/or organisational-specific data model. Fully adopting and implementing a data model across an organisation, while providing standardisation and consistency, is very time-consuming, expensive, and difficult to govern. On the other extreme, not adopting a common data model can lead to a 'wild west' scenario where there is no standardisation and consistency, which often leads to bad experiences. The right balance is to define and adopt a common data model for critical data elements with lightweight, automated governance to ensure delivery agility isn't impacted. Any domain-specific data entities can be owned, controlled, and governed by the domain or federated teams. The approach to a layered architecture (through abstraction and API-led connectivity, see section 4.3) helps to harmonise data models across multiple data sources and provide consistency regardless of where the data is held.

CASE STUDY: Financial Services

Open Banking was created to enable innovation, transparency, and competition in UK financial services. Driven by the regulator, it was tasked with delivering the APIs, data structures, and security architectures that enable developers to harness technology, making it easy and safe for individuals and SMEs to share the financial information held by banks with third parties. This required banks and account providers to securely provide regulated access to account and payment services by exposing REST APIs to the ecosystem.

The Open Banking API Specifications consisted of a number of distinct types of specifications and defined the key data entities, syntax, and relationships to allow the secure exchange of information such as account holder data, residential or location addresses, financial account information etc. All banks participating in the ecosystem were mandated to expose APIs in compliance with these security schemes and data specifications and were responsible for mapping these data structures to their own internal data models. Open Banking has successfully enabled interoperability across the financial service ecosystem and facilitated a data-driven business model.

In addition to Open Banking, banks often adopt BIAN (Banking Industry Architecture Network) as a common industry framework supporting interoperability within financial services. From a data perspective, this framework includes a common vocabulary with unambiguous definitions, data model structures and schemas that concentrate on meta-data (i.e. the meaning and structure of data and information). This common framework helps to standardise and simplify the overall banking architecture while maximising interoperability across the banking ecosystem.

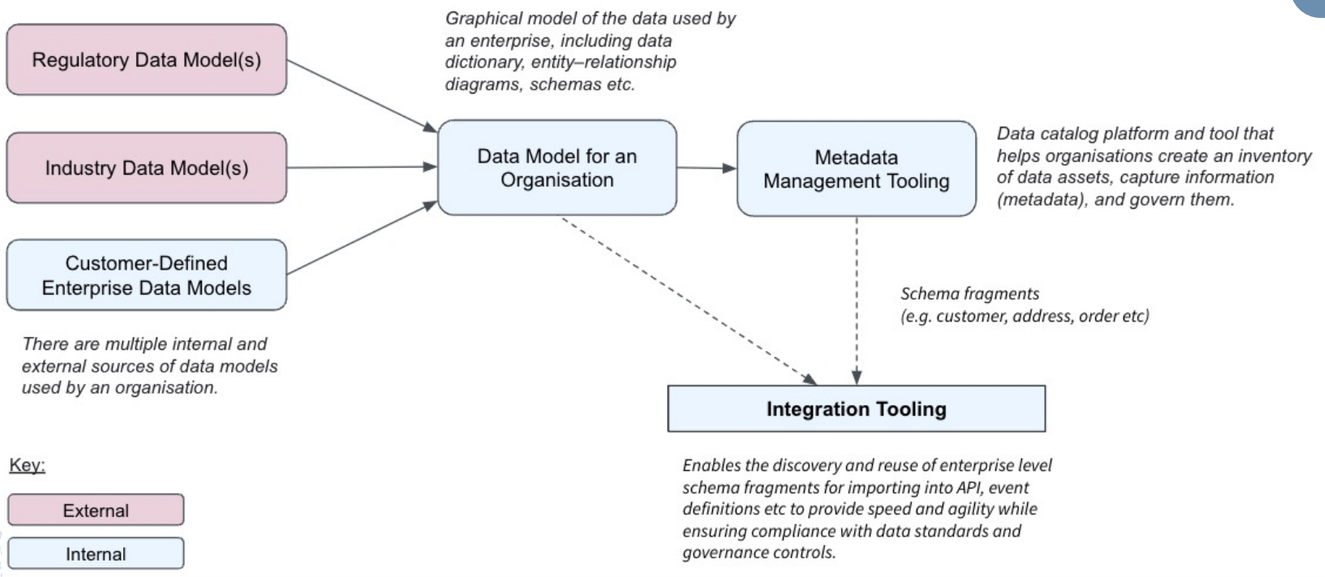


Figure 7: *Organising data elements and standardising how they relate to one another and to the properties of real-world entities.*

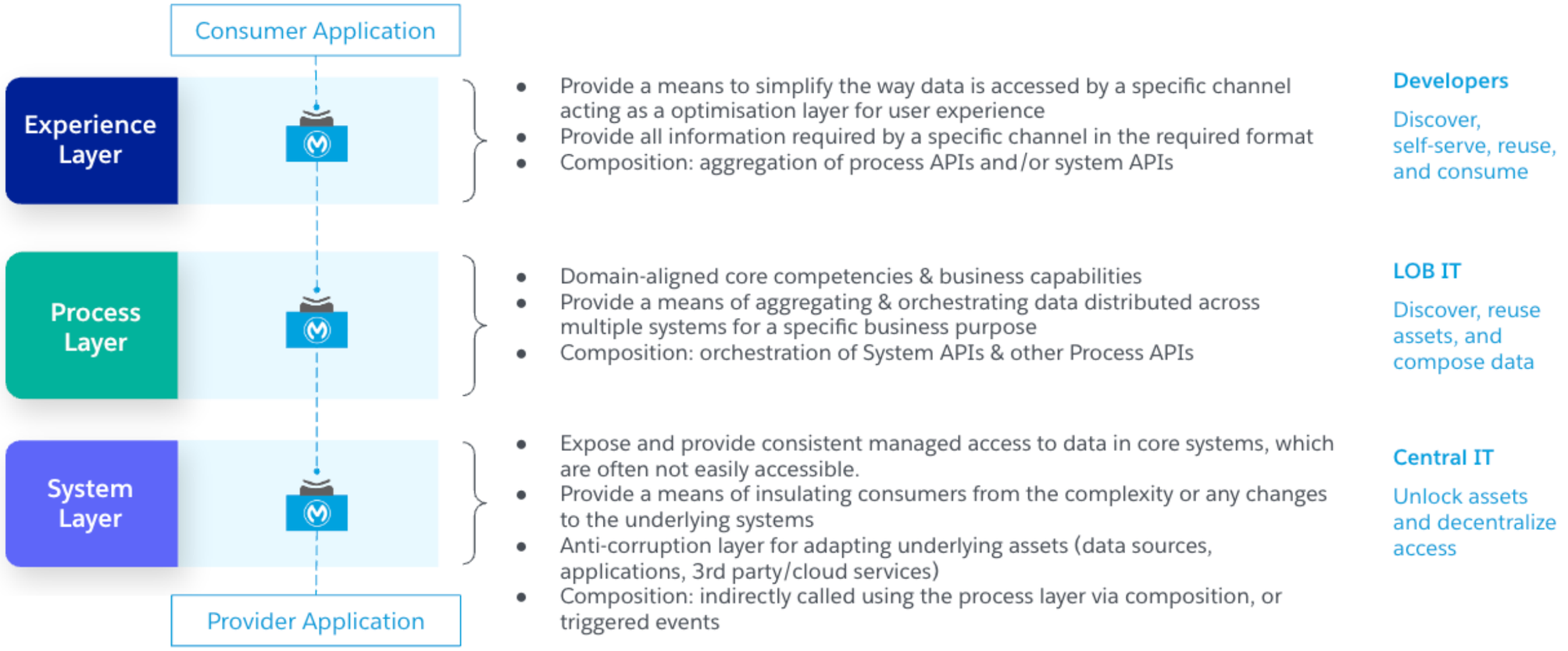
4.3. Abstraction & API-Led Approach

A stakeholder profile rich with third-party entities and an additive approach to IT are just some of the reasons why government and public organisations are more complex than average organisations. In a recent survey, 99% of IT Decision Makers in the public sector admitted that integration challenges hinder digital transformation initiatives[7].

The answer to this, according to Gartner, is to shift towards a composable architecture[8] whereby every piece of data, every application, and every process is a reusable building block that's easily and securely discovered, accessed, and reused. This approach allows new business capabilities to be composed from these reusable building blocks allowing projects to start fast and go faster project by project.

The key to success is applying a level of abstraction and separation by taking an API-led approach (see Figure 8) and exposing every system or application's capability with a well-known and understood set of digital assets or services which are available for discovery and self-service within the organisation.

Figure 8: *API-Led Connectivity is a methodical way to connect data to applications through reusable and purposeful APIs.*



[7] MuleSoft 2023 Connectivity Benchmark Report
[8] Gartner Keynote: The Future of Business is Composable

Breaking this layering down:

- The System Layer offers the abstraction and connectivity layer to all underlying systems and protocols.
- The Process Layer is where the domain-oriented business services are built and where components from the System layer are re-used.
- The Experience Layer is all about driving customer experience by implementing a tailored API for the specific channel that needs to consume the service.

Not all layers necessarily need to be used for all use cases but each should be used for their intended purpose to ensure:

- A loosely coupled architecture which is change-agile and future-proof.
- Digital assets which are highly discoverable and reusable through self-service freeing up more time for innovation.
- Increased business efficiency by unlocking and unifying services and data across underlying systems and processes.
- Speed and agility providing a faster time-to-market for new digital initiatives.
- Delivery of an end-to-end zero-trust security and defence in-depth strategy, where each API can be independently managed and secured through the use of modern security protocols (e.g. OAuth, OIDC etc) to ensure that any sensitive data is fully protected.

The key takeaways of this approach are to:

- Decompose monolithic systems and implement reusable solutions through composable building blocks (e.g. APIs, events etc) to enable agility and connectivity.
- Adopt an API-led approach (i.e. layers of abstraction) to build reusable assets that will save time and money and create a plug-and-play architecture which is designed for change with built-in security, visibility, compliance, and governance.
- Provide support for multiple architectural patterns allowing a seamless transition from vertically integrated monolithic and legacy solutions to an agile API-led and event-based architecture.
- Ensure all APIs are shared via a digital marketplace to facilitate the discovery, promotion, and re-use of digital assets (APIs, events etc) through a unified end-user experience.
- A Centre for Enablement (C4E) is required to enable the business and IT teams to shift from a production-based to a production-and-consumption-based delivery model.

CASE STUDY: Health Service Executive[9]

The Health Service Executive (HSE) provides public health and social services for everyone living in Ireland. It is the largest employer and organisation in the state, employing over 80,000 people directly and an additional 40,000 people through contracts. Its annual budget is over €20 billion, giving them an exceptional amount of fortitude and expertise.

HSE adopted an API-led approach to connectivity, leveraging reusable API building blocks to securely link core data domains such as patient data, GP systems, pharmacies, appointments, and vaccination events. As a result, HSE were able to deliver a solution to the COVID-19 pandemic which was both transformative and strategic. This laid the foundation for delivering the COVAX platform in only 9 days, supporting frontend patient experiences, administering over 11 million vaccinations and being able to adapt and rollout changes quickly in response to changes in vaccine availability and government policy.

CASE STUDY: Financial Services

Open Banking required a number of banks to change the way IT services were architected, designed and delivered through the adoption of a composable, microservice-based 'plug-and-play' architecture, architectural layering to provide separation of concerns, open up legacy mainframe applications through modern standards-based APIs (e.g. BIAN 2.0, ISO 20022 compliant), and leveraging agile methodologies (DevSecOps) to deliver robust and secure applications through effective yet controlled change and release management processes. This required a radical operating model shift across people and processes to effectively manage and govern a set of critical business services with resilient operations, governance, and control in order to comply with the requirements as set out by the regulator.

A number of banks adopted the API-led approach which:

- *Enabled and embraced open innovation allowing banks to accelerate delivery with composability.*
- *Allowed banks to keep relative pace with modern FinTechs in terms of enhancing their web and mobile banking experiences to better meet the needs of their diverse customer base.*
- *Allowed banks to reimagine themselves by transitioning to a banking-as-a-service model.*

[9] https://www.salesforce.com/uk/customer-success-stories/health-service-executive/

4.4. Asset Reuse

Reuse is a key element of Defence's API strategy[10] with the aim of being able to deliver capabilities more quickly and at reduced cost through leveraging existing digital assets both within and outside of RAS through the sharing of standardised and open standards-based APIs, API specifications, API fragments, mock services, SDKs, source code etc. According to the MuleSoft 2023 Connectivity Benchmark Report[11], on average, 47% of an organisation's internal software assets and components are reusable but only 33% of an organisation's APIs are discoverable.

When an organisation has secured, productised, and made their API & integration assets easily discoverable & consumable, this leads to a higher return on IT assets and investments, faster delivery speed, and reduced maintenance & change effort. These benefits are compounded when these assets are available through self-service which frees up more time for collaboration and innovation between teams.

Tying this into the ontology for RAS, a standardised set of common commands, requests and field names should be defined that can return information such as software versions, manufacturer name, model number, firmware version, etc. (even extending to flight/mission duration), which can be augmented by manufacturers for their unique capabilities and sensors. This is a successful approach which has been taken with SNMP (Simple Network Management Protocol), where there are a common set of commands used in all implementations and adopted by all providers with manufacturer extensions built on top of this to allow for extensibility.

Once defined, these common APIs, specifications and data models need to be adopted not only by the industry, manufacturers, and providers but also internally across Defence.

4.4.1 API/Digital Marketplace

Figure 9 shows the vision for an effective API/digital marketplace that facilitates the discovery, promotion, and re-use of digital assets through a unified end-user experience. The marketplace is essentially a portal with an optimised UX where internal and/or external users can discover and understand digital products, APIs, API specifications, API fragments, events, RPA bots, connectors, accelerators, mock services, sample code, SDKs, case studies and success stories. This concept of a marketplace is analogous to a shopping mall which provides a map to discover shops, restaurants, and cafes at a single location and which is easily navigable to discover all of the products which are on offer.

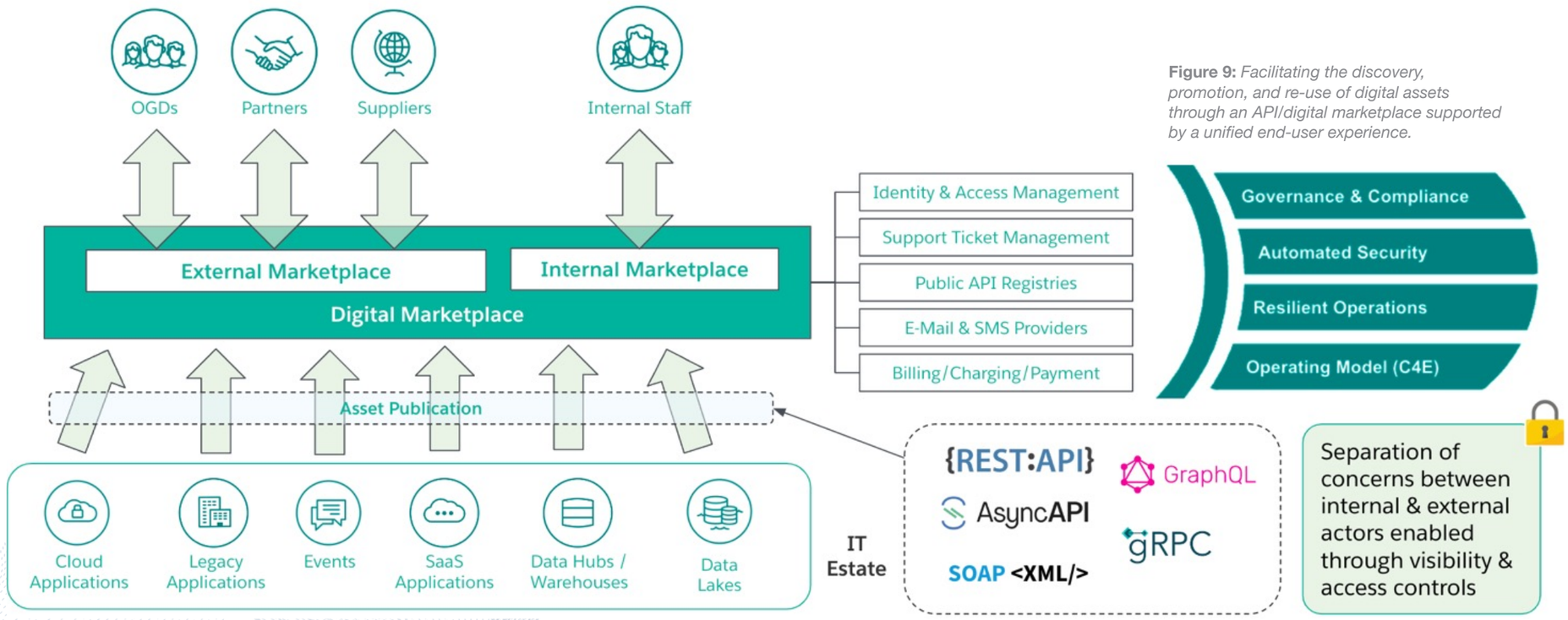


Figure 9: *Facilitating the discovery, promotion, and re-use of digital assets through an API/digital marketplace supported by a unified end-user experience.*

[10] MoD API Strategy: Data Exploitation in the Modern Age, March 2021
[11] MuleSoft 2023 Connectivity benchmark report

From an IT standpoint, this means that the key digital assets offered by RAS and wider Defence, from data platforms, legacy applications, cloud applications, data hubs and warehouses need to be published to the marketplace so that they can be discovered, promoted, and advertised. Separation of concerns need to be addressed through defined identity and access controls between internal and external users, and within these groups in terms of different user group access controls and permissions. The API/digital marketplace needs to be supported through an effective operating model with clearly defined processes and controls, together with governance, security, and resilient operations.

Key benefits of this approach are:

- Digital assets are managed, governed, controlled, promoted & marketed as 'Products' providing opportunities for collaboration and innovation.
- Asset discovery, re-use & self-service enabled through internal and external facing marketplaces.
- Accelerated time-to-market for new propositions through reuse.
- Assets (e.g. APIs, events, API fragments, sample code, accelerators, how-to guides etc) promoted, published, and supported.
- Facility for APIs to be tested prior to onboarding and adoption.
- Consistent branding with a streamlined and unified end-user experience.
- Support ticket management.
- An operating model with cost efficiencies through automation.

CASE STUDY: Financial Services

External API Marketplaces have been more commonly seen across Financial Services to connect creators, consumers, and partners to create innovative solutions. With the adoption of Open Banking and Open Finance through regulation, banks leverage marketplaces to allow their ecosystem to:

- *More easily find, compare, and consume APIs.*
- *Build and deliver seamless digital experiences quickly with access to the latest digital products.*
- *Connect, get help, and learn from other developers and experts to create innovative solutions.*

Please see here for an example of an exemplar API marketplace from the Financial Service industry.

4.4.2 Communities of Interest (CoI) and Practice (CoP)

Having a significant number of well-designed and highly reusable APIs that are discoverable through an API marketplace doesn't guarantee that they will be found, leveraged, and adopted. To advertise, generate awareness and promote adoption requires the formation of a Community of Practice (CoP) and/or Community of Interest (CoI):

- A Community of Practice is a group of people who share a concern or a passion for something they do and learn how to do it better as they interact and practice in the field regularly.
- A Community of Interest, or interest-based community, is a community of people who share a common interest or passion. These people exchange ideas and thoughts about the given passion but may know little about each other outside this area.

Such sessions would have an agreed purpose and objectives, would be run on a regular basis, and would provide the ability to share and generate awareness of new capabilities, new frameworks, new Defence and non-Defence related standards, and provide an opportunity for practitioners to showcase work they have undertaken, what the benefits and lessons learnt were, and how they can be reused in other areas.

4.5. Open Systems Architecture and Open Standards

The UK MoD has recognised that mission systems software is becoming ever more complex and expensive to develop. Technological advances mean software must rapidly adapt to evolving threats and capability needs. The UK MoD is therefore developing a reusable and open mission system architecture, alongside a suite of reusable software components for legacy and future air platforms, known as PYRAMID. This approach will make upgrades simpler and reduce software development costs, as well as the time it takes to implement capability enhancements[12].

See case study on the next page.

[12] PYRAMID Programme - GOV.UK (www.gov.uk)

CASE STUDY: PYRAMID

The PYRAMID programme introduces a paradigm shift to the current method of avionic systems design and procurement. PYRAMID aims to make legacy and future air mission systems affordable, capable, and adaptable through the adoption of an open systems architecture approach and systematic software reuse. The focus of the programme has been to develop the core PYRAMID Reference Architecture (PRA)[12].

Previously, mission systems software was bespoke to each air platform (i.e. Typhoon or F-35 Lightning) and was not designed to be compatible with the wider platform portfolio. PYRAMID aims to break this mould, allowing each software component to be compatible with other platforms that have adopted the PRA12.

Although PYRAMID is not just an API there are key lessons that can be learned from its evolution. PYRAMID's roots are in the Allied Standard Architecture Council (ASAAC) efforts to define a set of open architecture standards[13]. The five Def Stans 00-74 to 00-78 are the key outputs of the ASAAC. Initially established by France, Germany, the UK and the USA, issues began to arise after the USA left the group and invested heavily in their own F-22 Raptor and Comanche helicopter programmes. These platforms use POSIX and ARINC 653 which overlap significantly with the scope of the ASAAC standards. The huge momentum created behind POSIX and ARINC 653 inhibited the business case for industry investment in the implementation of the ASAAC standards and the initiative dwindled until the eventual withdrawal of the Def Stans in 2007.

Lesson 1 – The development and publication of a standard doesn't mean it will be adopted.

Adoption is critical to success and true openness. Select standards with adoption momentum rather than developing your own.In the intervening period between ASAAC and PYRAMID the USA began to develop FACE[14] , to build on ARINC 653 creating a fully featured open avionics environment, and France and the UK developed ECOA[15] to add middleware for software component-to-component communication rather than relying on low-level operating system API calls. FACE continues to develop and PYRAMID is a further evolution from the earlier research conducted within ECOA. Both FACE and PYRAMID initiatives aim to enable interoperability, sustainability, portability, and rapid upgrade of mission systems through the use of reference architectures defining functional breakdowns, standard messaging interfaces, middleware and containerisation enabling independent development.

Learning from 'Lesson 1', the PYRAMID team has recognised that the FACE initiative has significant momentum and therefore industry and our strategic partners will be more likely to adopt PYRAMID-based solutions if there is interoperability with FACE. PYRAMID is collaborating with the US Army and US Navy through the Collaborative Open Systems Architecture (COSA) Project Arrangement.

Lesson 2 – International alignment between standardisation initiatives with a significant overlapping scope is a key enabler in building national and international marketplaces.

[12] PYRAMID Programme - GOV.UK (www.gov.uk)
[13] Allied Standards Avionics Architecture Council - Wikipedia
[14] Future Airborne Capability Environment™ (FACE) | The Open Group Website
[15] Welcome to ECOA — ECOA

4.6. Operating Model

In other sectors, leading organisations drive change through the provision of a development ecosystem. The business models address many of the challenges outlined in previous sections:

- **Platform:** SDKs are provided along with development guides and a list of published APIs. Technology and interface specifications are standardised.
- **Profit:** Payment mechanisms are in place that allow third parties to develop solutions and receive payment. Non-traditional suppliers are incentivised to adopt solutions for Defence applications.
- **People:** Developers with novel solutions utilise the platforms and as their products are downloaded, licenced, and used receive revenue for their efforts. Talent from across sectors is attracted and accessed.
- **Process:** DevSecOps is applied and products are assured prior to being made available in online stores. Users can create digital workflows allowing businesses to optimise and outperform the competition.

CASE STUDY: OSDU WIND FARM SERVICES

The Open Group OSDUTM (Open Subsurface Data Universe) Forum enables the Energy industry to develop transformational technology to support the world's changing energy needs.

The OSDU Forum is enabling new business and operational opportunities for Wind Farm Services. Relevant data from Operational Onshore / Offshore Wind Farm services is loaded in the OSDU Data Platform and made accessible for applications to run on top of the OSDU Data Platform. Data definitions are developing and leading to the establishment of IEC 61400-025 standards; OPC-UA being used to connect Wind turbines to the OSDU Data Platform; Deltalake (Open Source) as the store for near real-time data; Kafka for high-speed streaming data.

- *Data Vendors deliver data in a format that is being adopted by the industry.*
- *Software Developers use the open platform to build newly imagined products that provide both internal and external customers fresh insights, efficiency gains, and innovative interpretations.*
- *Vendors market and deliver or deploy apps to operators which can be delivered via an app cloud marketplace.*
- *Operators access, analyse, and visualise data internally, directly from the OSDU platform.*

5 SOLUTION

Based on industry insights, this section outlines the solution to address the challenges outlined in section 3.

5.1. Solution Architecture

In an ever-complex environment, delegated authority risks producing teams operating in silos, an additive procurement mindset introduces vertically fully integrated standalone systems and data silos and often technology is not supported by a robust architecture framework.

This causes:

- Delivery to be non-conformant to best practice with low reuse.
- Uncontrolled technical debt.
- Increased data held in silos and inaccessible to robotic autonomous systems.

The only sustainable approach to address these challenges is to adopt a set of key/north-star principles which ensure a future-proof and change-agile enterprise architecture which:

1. Is **interoperable** through the adoption of APIs and open standards to ensure interoperability, mitigate the risk of inaccessible data silos, and promote the reuse of strategic digital assets.
2. Is **modular**, providing a microservice-based composable architecture which ensures change agility, speed of delivery and reuse through the creation of digital building blocks across all core domains of the organisation.
3. Promotes **abstraction** to provide loose-coupling and prevent being locked into vendor/system-specific data models allowing a RAS/Defence-based ontology to be adopted.
4. Is **resilient** operationally, ensuring business continuity and availability of all key digital services whatever the conditions or environment.
5. Is **secure** by design and embraces a defence-in-depth strategy.
6. Is **discoverable** through a catalogue of digital assets which are accessible through self-serve to promote reuse and eliminate duplication and technical debt.
7. Is **event-based** both operationally and analytically, providing the ability to share data in real-time enabling actionable insights from RAS devices on the battlefield through to connected decision-making from a command-and-control perspective.

Figure 10 depicts the recommended solution architecture to address the technology and data challenges outlined in section 3.1.5.

Data exchange across RAS & MOD digital ecosystems supported through the adoption of an API framework & north star principles providing the ability to be more reactive, adaptive & responsive on the battlefield

Figure 10: *APIs enable the creation of a secure data exchange network across the RAS and wider MoD digital ecosystems providing opportunities for innovation.*

The key highlights of this target architecture are outlined below:

RAS Command and Control (C2)

- The RAS C2 systems are API-enabled with APIs exposed through an 'Integration and API Management' platform to allow secured and managed access to the API Consumer and API Provider ecosystem.
- Adopting an API-led approach, System APIs would provide a layer of abstraction above each vendor's C2 application to securely unlock siloed data and functionality. This would be joined together through a Process API which would expose access to the RAS systems using a common data model and ontology. Experience APIs can be defined to simplify the way data is accessed by specific channels to optimise the experience.
- This approach allows real-time data sharing from RAS C2 with:
    - Master data systems to provide seamless access to internal data (e.g. resources, military vehicles, equipment etc) and external data (e.g. climate, weather, maps etc) sources.
    - Data Lakes to provide actionable insights from the battlefield and allow effective decision-making based on data collected from multiple trusted data sources (i.e. MoD and our allies). Any military decisions made can be securely shared with key RAS C2 systems via APIs to send to the RAS devices in the battlefield to carry these out.
    - Wider MoD and allied ecosystems to ensure effective collaboration across all areas of Defence both domestically and internationally.
- This architecture also provides an option to move away multiple RAS vendor-specific UIs and allow access to the underlying capabilities of each of the different RAS C2 systems to a single RAS Web App/UI through secured Experience APIs. This will eliminate the need for operators to context switch between RAS provider UIs when multiple vendor RAS devices are operating in the battlefield and reduce the operator training, enablement, and certification needed across multiple technologies.

RAS Devices

- Each RAS provider has its own proprietary protocols for communication between C2 and other devices to share insights from sensors, AI, and ML modules. They would be able to securely share streams of data which any other device can interpret based on its own AI and ML modules to take decisions as a collective group of devices.
- Each vendor's RAS device should be able to securely share data and insights (in read-only configuration) with other trusted vendors' devices and personnel to allow effective collaboration on the battlefield without command-and-control supervision.
- It's critical that all API access points are fully secured with industry-standard mechanisms for both authentication and authorisation before any data is shared. This will ensure that RAS devices and data are protected from cyber-attacks and enemy compromise.

Unlocking the power of RAS in defence is a complex initiative that requires a future-proofed strategy supported by the right people, processes, and technology. It is acknowledged that the solution and approach outlined in this paper requires buy-in from RAS providers to adopt a more open API-based architecture in a controlled and phased manner with commercial incentives to drive adoption and align with this future vision.

6 RECOMMENDATIONS & CALL TO ACTION

The key recommendations and call to action based on the research and insights obtained:

1. **Establish an architecture framework** (see section 4.1) to ensure strategy, principles, reference architectures, patterns, standards, guidelines, decision-tree matrices, catalogues, and data models are defined, align with the business strategy and are available through self-service. This will provide a mechanism to enable effective data and information exchange both within and across the RAS and MoD digital ecosystems and a means for ensuring all projects and programmes align with this vision through an effective governance process.
2. **Define and adopt a common functional ontology and data model** (see section 4.2) to enable better interoperability by allowing data to be linked at the semantic level. Applied against a functional ontology the RAS MOSA systems interface specifications will create the conditions for broad cross-sector development of HMT capability that will outpace our adversaries and position the UK as a leader in RAS technologies.
3. **Adopt a composable architecture with levels of abstraction** (see section 4.3) through an API-led approach to drive delivery agility and reuse while providing separation of concerns.
4. **Expand the logical architecture** (outlined in section 5) to define the physical capabilities and technologies, either existing or new, required to deliver against the target architecture. The focus should be given to elements of the solution which immediately add the most value, resolve existing high-priority challenges and offer a compelling return on investment.
5. **Create a RAS digital marketplace** (see section 4.4.1) consisting of APIs, SDKs, a DevSecOps environment and an online presence offering disruptive technology. The MoD should consider whether the store should go beyond pure software applications and whether this could include modular hardware.
6. **Establish a Community of Interest/Practice** (see section 4.4.2) to provide the ability to share and generate awareness of new capabilities across RAS, new frameworks, new Defence/non-Defence related standards, and provide an opportunity for practitioners to showcase work they have undertaken that can be reused in other areas.

Adopting the above recommendations will help address the people, skills, and talent challenges whereby knowledge is more readily available in terms of open frameworks and standards as opposed to niche custom and closed-system specific skills.

7 CONTRIBUTORS

The following stakeholders have been key contributors to the creation of this whitepaper:

#	Organisation
1	DE&S FCG (MOD Lead)
2	Mulesoft (Industry Lead)
3	Team Defence Information
4	Animal Dynamics
5	Ansys
6	AtechSYN
7	BAE Systems
8	BT
9	Capita
10	Conceptare
11	IBM
12	L3 Harris
13	Maranis
14	Salesforce
15	Real Time Data Company
16	Thales
17	TRL
18	UK AEA
19	UK MOD

Table 1 – *Key Contributors to Whitepaper*

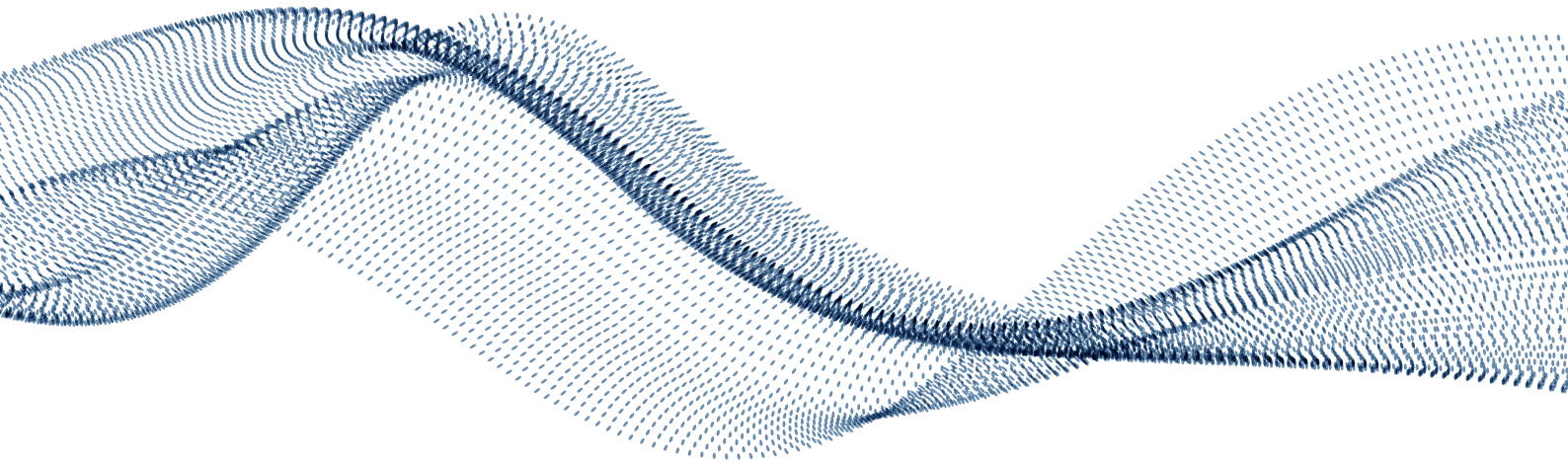
8 GLOSSARY OF TERMS

Please see below for a glossary of terms referred to in this whitepaper to ensure consistency in terms of knowledge and understanding.

#	Abbreviation	Description
1	API	Application Programming Interface
2	ASAAC	Allied Standard Architecture Council
3	C2	Command and Control
4	CoI	Community of Interest
5	CoP	Community of Practice
6	COSA	Collaborative Open Systems Architecture
7	DevSecOps	Development, Security and Operations
8	FCG	Future Capability Group
9	HMT	Human Machine Teaming
10	MOSA	Modular Open System Architecture
11	PRA	PYRAMID Reference Architecture
12	RAS	Robotic & Autonomous Systems

Table 2 – *Glossary of Terms*

8 LICENSING



TEAM DEFENCE INFORMATION

6A Pinkers Court
Briarlands Office Park
Gloucester Road
Rudgeway
Bristol
BS35 3QH

+44 (0)1454 410 550
secretariat@teamdefence.info