Integrating business and technology infrastructures



Strategic autonomy with global interdependence

Defense integration series

To accelerate and secure strategic autonomy, defense leaders must integrate policy intent with industrial execution, technological innovation, and capital formation. This requires design and operationalization of sovereign, interoperable architectures that sustain readiness over decades.

Across the region, defense and national security organizations are investing heavily in new technology, industrial partnerships, and talent. Yet a key question remains unanswered: how can these investments be connected to deliver real capability?

For most defense organizations, the challenge is not a lack of technology but the difficulty of integration. Many ministries, agencies and forces still depend on legacy systems that were built decades ago for single purposes. Logistics, command, procurement, and human-resources systems each operate in isolation. Information cannot easily move between them, and many were never designed for modern interoperability.

Replacing these systems outright is rarely an option. They hold critical operational data and embody years of institutional knowledge, often constrained by political agreements. As a result, many defense leaders face the same dilemma: how to modernize without disrupting mission readiness.

This is where the concept of the fusion layer becomes essential — the framework that connects people, processes, and platforms across the defense enterprise. It allows data, doctrine, and decision-making to flow securely between the business and technology infrastructures that underpin capability. The next capability edge will be architectural, where sovereignty is engineered through interoperable ecosystems, not single programs.

The legacy challenge

Every defense force is built on a foundation of legacy. Systems that once represented cutting-edge innovation are now decades old. They were designed for specific missions, in isolated environments, and often by different suppliers working to different standards.

In the GCC region, defense transformation programs have made impressive progress, yet most still rely on inherited systems for maintenance, logistics, and command. Modern artificial intelligence tools or predictive-maintenance algorithms cannot simply connect to them — they require translation layers, data cleansing, and security accreditation.

Legacy also exists in processes and culture. Acquisition frameworks were written for hardware, not data. Business functions like finance and human resources often operate on separate platforms from operational systems, meaning information about readiness, cost, or risk cannot be viewed holistically.

Integration therefore demands more than new software; it requires aligning the enterprise architecture, the operating model, and the governance that links them. As KPMG's experience across government and industry shows, real transformation happens when business and technology leaders design together — not in parallel.

Sector specificity and safety-critical design

Defense systems are unlike those in many other sectors. They are bespoke, mission-critical, and safety-assured. Every change — no matter how small — must be tested and evaluated to ensure it performs under extreme conditions and does not compromise safety or security.

When an aircraft's mission system or a naval radar network is upgraded, the testing effort can take years. Integrating new digital components means re-certifying interfaces, validating data integrity, and ensuring compatibility with legacy equipment still in service.

This level of assurance makes defense integration complex, but also necessary. The more digital and connected a force becomes, the greater the need for rigorous test, evaluation, and validation.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

The same principles apply at the enterprise level. Integrating business and technology infrastructure — for example linking procurement data with operational readiness — requires controlled testing and trusted governance. Without this, leaders risk introducing new vulnerabilities even as they modernise.

The sensitivity of data and the importance of trust

Defense data is among the most sensitive information a nation holds. It includes troop movements, equipment status, intelligence reports, and industrial production details. Sharing it outside secure boundaries is therefore both a technical and political risk.

In an age of coalition operations and cross-border industry partnerships, some level of data sharing is unavoidable. Governments want to collaborate with trusted allies and enable local industry partners to build capability under national visions such as Saudi Arabia's Vision 2030 and UAE's EDGE ecosystem. Yet every new connection raises legitimate questions about sovereignty, cyber-risk, and long-term control.

Building the fusion layer therefore depends as much on political trust and governance as on encryption or system architectures. Data must be classified, tagged, and controlled according to agreed rules. Industry partners must understand their responsibilities for data protection and export control. Regulators must set frameworks that balance collaboration with national interest.

KPMG's experience supporting government regulators, armed forces, and industrial partners shows that governance frameworks can enable secure collaboration. By defining who owns which data, under what conditions, and for how long, organizations can unlock the value of shared insight without compromising sovereignty.

Designing the fusion layer for sovereign ecosystems

The fusion layer is not a single platform or product. It is a design principle — a structured way to connect business, operational, and technical systems through interoperable, governed, and secure data exchange.

It combines five essential elements:

1. **Data –** standardized, trusted, and discoverable.
2. **Doctrine –** processes and decision rules that define how information is used.
3. **Industry –** partners, suppliers, and innovators contributing to capability.
4. **Innovation –** new technologies that must integrate safely with existing systems.
5. **Capital –** the financing stack that sustains transformation across cycles.



Together these elements form the foundation of future capability. The fusion layer allows a logistics commander to see real-time information from industry maintenance systems, or a policymaker to link budget data with operational readiness metrics.

When designed correctly, it becomes the bridge between business strategy and mission execution — the layer where doctrine meets data.

Integrating business and technology infrastructures

Integration must extend across the entire defense. Business functions such as procurement, finance, and human resources are often managed separately from operational systems. Yet decisions about cost, readiness, and supply all depend on shared data.

In the GCC, several defense organisations are now pursuing enterprise integration programmes that connect back-office data with front-line operations. For example, unified maintenance and logistics platforms can allow both defense forces and local industry to plan spare-parts production more efficiently, reducing downtime and improving readiness.

The key is to build interoperability by design, not as a later retrofit. That means developing shared data models, consistent governance, and secure interfaces from the start of each programme.

KPMG supports this approach through integrated operating model design, enterprise architecture frameworks, and governance solutions that balance agility with assurance.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

Building political and industrial trust

True interoperability requires more than technology; it requires confidence between institutions. In defense, this is both diplomatic and strategic.

When nations, ministries, and industry partners trust one another, they can share information more freely and innovate faster. When trust is absent, even the most advanced systems remain isolated.

Long-term partnerships, localization initiatives, and joint testing programs can all strengthen that trust. For example, GCC countries increasingly host joint ventures where government and private industry share test data under agreed governance rules. These arrangements can build local capability while ensuring that control remains sovereign.

KPMG's work across government, military, and industry gives it a unique perspective on these relationships. By acting as an independent adviser and integrator, KPMG helps partners establish frameworks that balance national security with industrial collaboration.

Practical steps for defense leaders

Building the fusion layer is a journey, not a single project. Defense leaders can begin with a few practical steps:

1. **Assess the legacy landscape –** Map existing systems and dependencies. Identify where integration is technically possible and where replacement is necessary.
2. **Design for assurance –** Embed testing, evaluation, and certification at every integration stage.
3. **Govern for trust –** Establish clear data-sharing policies, access controls, and accountability mechanisms.
4. **Enable the people –** Integration succeeds only when business and technical teams share understanding and language.
5. **Plan for longevity –** Integration frameworks must outlast technology cycles, leadership changes, and vendor contracts.

By taking these steps, defense organizations can move from isolated projects to a connected enterprise capable of adapting to new threats and technologies.

From projects to ecosystems

The future of defense capability will be defined by connection. It is no longer about owning the most advanced platforms, but about ensuring that every platform, system, and partner can operate as part of a coherent 'joint' whole.

Legacy systems, safety-critical assurance, and data sensitivity are not obstacles — they are the realities that make integration both challenging and essential. The fusion layer is how defense organizations can respect these realities while unlocking the value of modern digital capability.

Integration is not a single project or just a technical goal; it is a strategic one. It links the industrial base, the command center, and the policy office into one decision ecosystem. It demands collaboration between business and technology, and between government and industry.

With deep experience across government, the military domain, industry, and regulatory organizations, KPMG helps clients design and govern this transformation — building the trust, assurance, and architecture needed for truly interoperable capability.

Contact us



Chris Moore
Partner, Head of Defense and Security
KPMG Middle East
christophermoore1@kpmg.com



Kev Copsey
Principal, Defense and Security
KPMG Middle East
kcopsey@kpmg.com



Andrew Mellors
Principal, Defense and Security
KPMG Middle East
amellors@kpmg.com

KPMG is the official Knowledge Partner for the World Defense Show 2026

KPMG brings its team of dedicated Defense and Security experts to lead the discussions on defense integration, innovation and localization under Vision 2030 – along many other themes. As Saudi Arabia advances toward the ambitious goals of Vision 2030, the localization of defense industries is becoming a strategic priority. This transformation is about building national capabilities, supporting local talent, empowering SMEs, and fostering innovation. WDS 2026 will showcase cutting-edge technologies, bring together global and local leaders, and spark the collaborations needed to accelerate the Kingdom's defense and industrial ambitions. At KPMG, we are proud to support this transition and to integrate technology and capability development.

Access the **KPMG WDS 2026 resource center**.

© 2026 KPMG Middle East LLP, a Jersey limited liability partnership, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.