

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

Soaring Demand and Budgets Present Opportunities for Aerospace and Defence Leaders

by David Brand

Managing Director, Global Aerospace, Defense and Federal Leader, Protiviti

Successful companies view even challenging times as catalysts for innovation and growth, actively seeking opportunities where others see obstacles.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organisations balancing risk management with a strong focus on seeking growth are better equipped to innovate products and services, enhance their resilience, adapt to change, and achieve top-line growth and strategic differentiation. It is all about unlocking opportunity.

Our 14th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,540 board members and C-suite executives around the world regarding their views on:

- Three specific areas for growth considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organisations;
- The top risks on the horizon for the near term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long term (a decade from now) related to 12 strategic and operational risk themes; and
- A discussion of their organisations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. This paper offers specific insights into these issues from the perspective of the aerospace and defence (A&D) industry.

Where do leaders in the aerospace and defence industry see the greatest opportunities for their organisation over the next two to three years?

A&D leaders are entering a period of profound transformation. Growing demand for advanced capabilities — and ample budgets to support that demand — are facilitating new avenues for growth.

Growth is no longer about scale alone. Governments are demanding faster and more cost-effective solutions, prompting A&D leaders to leverage artificial intelligence (AI) and advanced engineering to accelerate innovation. These leaders prioritise modernisation, speed and integration to create value amid rapid technological and geopolitical change. Rather than relying solely on organic growth, they are boosting progress by compressing design-to-deployment timelines for major systems.

There is optimism for potential growth opportunities



Based on a five-point scale assessing agreement/disagreement. Percentages reflect sum of "Agree completely" and "Agree somewhat" responses.

This emphasis on speed and cost-effective solutions is driving procurement models towards greater “commercialisation,” reshaping competitive dynamics and lowering barriers to entry. Speed is the ultimate differentiator, opening doors for both startups and established primes. As we noted in our 2025 Top Risks survey, defence tech startups introduced leaner models and faster AI integration. In 2026, we expect this trend to continue, reinforcing the imperative for legacy firms to step up innovation and grow partnerships.

Ecosystem development is central to this transformation. No single organisation can deliver the agility and resilience required to compete in today’s volatile geopolitical landscape. Partnerships with technology innovators, advanced suppliers and even non-traditional players such as commercial tech firms are enabling A&D companies to integrate capabilities, reduce development risk and create flexible supply chains that can withstand disruption.

Geographic expansion adds another critical element. With defence spending soaring in Europe and the Asia-Pacific region, A&D organisations are pursuing strategic collaborations tailored to regional requirements. Licensing agreements for local production, joint ventures with domestic manufacturers and technology transfer arrangements illustrate how companies are adapting to regulatory frameworks while capturing growth in high-priority markets. These moves not only strengthen market access but also build trust with local governments, positioning firms as long-term partners in national security.

What will be the organisation’s most significant challenges regarding the impact of AI over the next two to three years?

While AI promises transformative impacts for A&D organisations, adoption hurdles can be daunting. The top 2026 challenges¹ include the inability to deploy AI at a competitive pace and uncertainty about the return on investment (ROI), followed closely by potential risks to third-party partners. Consistent with our 2025 survey findings, concerns around integrating AI into offerings (25%) and ensuring workforce readiness (23%) remain top priorities for 2026.

The pressure is on for A&D organisations not to fall behind in the AI race. Yet, investing heavily in AI can feel like a gamble for firms because it forces them to make difficult choices about priorities and resource allocation when the ROI is uncertain. Adding to this uncertainty, AI deployments tend to ripple across the ecosystem, introducing new dependencies and risks concerning third-party partners, from suppliers to cloud providers, making governance and oversight even more critical.

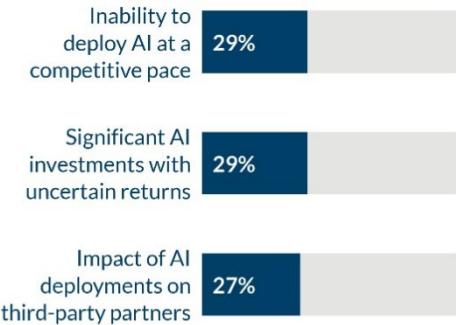
Top challenges for A&D organisations are reflected in the concerns cited in the global Top Risks survey, particularly around data security and deployment speed. That said, these organisations face unique operational stakes. From aircraft to autonomous platforms, AI is central to compressing design cycles for complex systems, and integration delays can undermine competitiveness and mission readiness. Legacy IT infrastructure compounds the problem, limiting data accessibility and slowing AI-driven simulation and predictive analytics. As for cybersecurity exposure (21%), the potential for compromised AI models to threaten national security underscores why this is a critical, high-stakes challenge. Cultural resistance adds another layer of complication, as parts of the workforce remain hesitant to embrace automation.

The mandate for A&D organisations is clear: Failure to operationalise AI swiftly could lead to lost contracts, diminished competitiveness and stalled defence innovation. The race for skilled talent is intense, as these firms vie with tech giants for AI and cloud expertise. In this environment, security and speed are non-negotiable. The successful deployment of AI hinges on modernised infrastructure, robust governance and targeted upskilling.

What are the most significant short-term (two to three years) concerns and risks on the minds of aerospace and defence leaders?

Each of the top 10 short-term A&D risks for 2026 escalated from 2025 levels, signaling an intensification of the risk landscape across the sector. Mitigating cyber threats is the highest priority for short-term risks for

Top 3 priorities – impact of AI



¹ Percentages in the top three priorities — impact of AI chart and commentary reflect frequency with which each area was selected among the top three.

2026. This increase reflects mounting regulatory requirements, most notably the Cybersecurity Maturity Model Certification (CMMC), which imposes stringent standards on defence contractors to safeguard controlled unclassified information. Compliance now demands continuous monitoring, documented security practices and third-party assessments — significantly increasing the operational burden on A&D organisations.

The growing sophistication of state-sponsored cyber threats is shifting the landscape from opportunistic attacks to highly coordinated campaigns targeting intellectual property, weapons systems and critical infrastructure. These adversaries leverage advanced tactics such as supply chain infiltration, zero-day exploits and AI-driven reconnaissance, making traditional perimeter defences insufficient.

Top global near-term risks

2026 rank	Risk issue	Average*	2025 rank
1	Cyber threats	3.90	1
2	Third-party risks	3.51	8
3	Operations and legacy IT infrastructure unable to meet performance expectations	3.36	5
4	Increases in labor costs	3.19	15
5	Increase in global terrorism, crime and violence	3.15	23

* Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."

Legacy IT performance issues continue to weigh heavily, exposing organisations to operational inefficiencies and security gaps. Labour cost inflation and global terrorism/crime add further pressure. Meanwhile, AI-related risks (3.09) are accelerating as firms race to integrate advanced technologies without fully addressing governance, oversight and ethical considerations.

Persistent supply chain fragility — exacerbated by tariffs, export controls and geopolitical tensions — remains a structural challenge for the A&D sector, where production cycles are long, supplier networks are highly specialised and compliance requirements are stringent. Disruptions in the provision of raw materials, precision components and critical technologies can cascade across programmes, jeopardising delivery schedules and contractual obligations tied to national security. The sector’s reliance on sole-source suppliers and geographically concentrated manufacturing amplifies vulnerability.

Collectively, these risks are driving investment in two primary areas: cybersecurity and IT modernisation, with the aim of protecting sensitive data, preparing for AI deployment and maintaining operational continuity. Industry trends indicate growing adoption of advanced analytics for supply chain visibility and tighter alignment of cybersecurity programmes with evolving compliance frameworks such as CMMC. These actions reflect the A&D sector’s response to heightened exposure, where disruptions can quickly affect delivery schedules, contractual obligations and mission readiness.

Based on these near-term risk issues, in what areas is the organisation likely to invest the most over the next two to three years, and why?

A&D investment priorities² align with the sector’s most critical risk exposures, reflecting its unique operational and regulatory demands. Data privacy and cybersecurity dominate spending plans — driven not only by CMMC in the U.S., but also by rigorous European Union (EU) requirements such as the Network and Information Security Directive 2 (NIS2) and the EU Cybersecurity Certification Framework, which mandate robust protection of classified and controlled unclassified information against increasingly sophisticated cyber threats.

Infrastructure modernisation emerges as a critical enabler, laying the foundation for AI integration, advanced analytics and secure digital platforms, while positioning organisations to prepare for quantum computing capabilities that will be essential to mission readiness and programme execution.

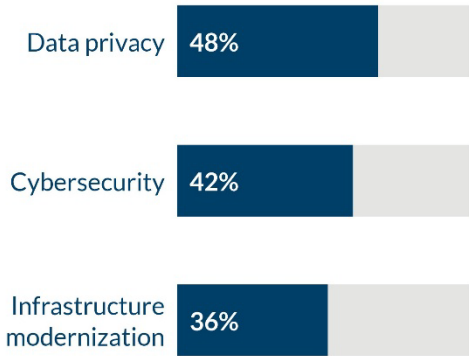
Regulatory compliance infrastructure and third-party management (30% each) remain high on the investment agenda for A&D firms, underscoring the complexity of defence ecosystems where multitiered supplier networks and export controls introduce vulnerabilities. These investments are not discretionary; they are foundational to maintaining eligibility for government contracts, meeting delivery timelines and upholding national security commitments.

These priorities align with broader industry signals, including the Pentagon’s recent acquisition overhaul announced by Defense Secretary Pete Hegseth, which emphasises speed, innovation and industry-led investment. The shift towards the new “Warfighting Acquisition System” and increased use of fixed-price contracting models places pressure on A&D firms to invest their own capital in facility upgrades, workforce upskilling and capacity expansion. Hegseth’s directive to move faster and invest more reinforces the need for agile technology adoption — including AI-driven automation and digital engineering — to meet accelerated timelines and maintain competitiveness in a contracting environment that rewards speed and the use of commercial best practices.

Similarly, in Europe, the Defence Readiness Omnibus introduces streamlined permitting, simplified procurement rules and incentives for joint purchases — fast-tracking timelines and reinforcing the need for agile technology adoption, including AI-driven automation and digital engineering, to maintain competitiveness in a contracting environment that rewards speed and commercial best practices.

While workforce development currently ranks lower on the investment priority list, it’s starting to gain momentum as A&D organisations recognise its critical role in sustaining innovation and addressing acute talent shortages, particularly in areas such as engineering, cybersecurity and advanced analytics. As AI

Top 3 investment areas



² Percentages in the top investment areas chart and commentary reflect frequency with which each area was selected among the top three.

and automation spread across design, manufacturing and finance functions, skill requirements are shifting, creating demand for professionals who can manage AI governance, interpret machine learning outputs and integrate autonomous systems into mission-critical workflows.

Overall, the A&D sector’s investment profile reveals a deliberate focus on security, resilience and speed — priorities very much in keeping with defence imperatives and the realities of operating in an increasingly complex and rapidly evolving global environment.

How do aerospace and defence leaders view the 10-year risk outlook for their organisation?

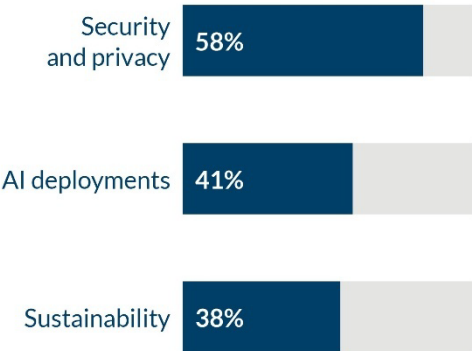
Long-term risk themes for A&D³ centre on technology, security and compliance, with sector-specific nuances shaping strategic priorities. Security and privacy lead the list, reflecting expectations of persistent cyber threats and more stringent regulatory requirements.

These concerns extend well beyond traditional IT safeguards to include data integrity across digital platforms and defence systems, as adversaries employ more sophisticated tactics and regulators tighten disclosure requirements.

AI deployments follow closely behind, indicating both confidence in their transformative potential and heightened awareness of governance, ethical and compliance challenges. As AI is integrated into design, manufacturing and mission-critical systems, new risks emerge around algorithmic bias, data protection and evolving regulatory frameworks for autonomous technologies.

In the A&D sector, sustainability (38%) is viewed primarily through a compliance lens rather than a purely environmental initiative. Regulatory frameworks such as the EU’s Corporate Sustainability Reporting Directive (CSRD) and the Carbon Border Adjustment Mechanism (CBAM) are shaping expectations for disclosure and supply chain transparency. These requirements are influencing how A&D organisations approach emissions mapping, data governance, and environmental, social and governance (ESG) reporting across multitiered supply chains, with implications for market access and contractual eligibility.

Top 3 long-term challenges



³ Percentages in the top three long-term challenges chart and commentary reflect frequency with which each area was selected among the top three.

Guidance/call to action for next two to three years

A&D firms must act decisively to navigate near-term risks and position themselves for sustainable growth. Based on our survey findings and client experience, we recommend the following action items:

- **Modernise legacy IT infrastructure** to unlock AI's potential and prepare effectively for emerging technologies like quantum computing.
- **Strengthen cybersecurity and vendor risk management** to meet regulatory mandates and counter escalating threats.
- **Accelerate digital transformation** by investing in advanced engineering tools, simulation capabilities and workforce upskilling to compress design-to-deployment timelines.
- **Embed robust AI governance frameworks** to help ensure the ethical, secure and effective use of AI across operations and products.
- **Leverage ecosystem partnerships** to enhance agility and resilience in a volatile geopolitical environment.

About the author



Dave Brand has extensive experience in the areas of Technology Auditing, Compliance, Business Leadership, Analytics and Reporting, Risk Management, Financial Controls, and Board Reporting. He has led teams for some of our largest clients and has both published and spoken on various topics.

Dave is one of the founding members of Protiviti and during his tenure has held numerous leadership roles. He now leads our global Aerospace, Defense and Federal practice.

Contact Dave at +1.404.834.6331 or david.brand@protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the **Fortune 100 Best Companies to Work For**® list for the 11th consecutive year, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0126
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®