2025 EDITION

EXECUTIVE PERSPECTIVES ON TOP RISKS

for the Near- and Long-Term

protiviti®
Global Business Consulting

Unprecedented change and disruption shaping a new future for the aerospace and defence industry

by David Brand, Managing Director, Global Aerospace, Defense and Federal Leader

Boards of directors and senior executive teams face a complex web of uncertainties. These may generate opportunities for strategic advantage or risks leading to unexpected disruption and performance shortfalls. An ability to anticipate risks that may be on the horizon before they become imminent can help leaders navigate unfolding developments — particularly those that are uncontrollable — that may impact their organisation's value and growth objectives.

Our 13th annual **Executive Perspectives on Top Risks Survey** contains insights from 1,215 board members and C-suite executives around the world regarding their views on the top risks they see on the near- and long-term horizons. Specifically, our global respondent group provided their perspectives about the potential impact over the near term (two to three years ahead) and long term (over the next decade) of 32 risk issues across these three dimensions:

- **Macroeconomic risks** likely to affect their organisation's growth opportunities
- **Strategic risks** the organisation faces that may affect the validity of its strategy for pursuing growth opportunities
- **Operational risks** that might affect key operations of the organisation in executing its strategy

Commentary — Aerospace and Defence industry group

This is Protiviti's first-ever Top Risks commentary focused on the global aerospace and defence (A&D) industry group. Our 2025 survey findings indicate that this industry is in a period of profound transformation driven by mounting geopolitical tensions, technological change and disruption, shifting economic priorities, and evolving workforce dynamics.

While the A&D industry does not always respond swiftly to change, historically it has proven to be resilient in adapting to it — and innovating because of it. But now, it faces an unprecedented convergence of risks that could alter its trajectory and competitive landscape for years to come.

For many businesses in the sector — including some of the largest, most complex and well-established companies — the need is urgent to rethink their traditional processes and modernise their operations so they can move faster and with more agility than ever before. If these organisations want to remain relevant and profitable in the rapidly evolving A&D industry, proactively driving change from within is a must.

Analysis of the top near-term risks for A&D

Cyber threats are top of mind for A&D executives — but not just because of bad actors

Top among the most pressing near-term concerns for A&D executives are cyber threats. This is not surprising, given the vital role the A&D industry plays in promoting national security, public safety and economic stability. Industry organisations are prime — and constant — targets for nation-state actors and cybercriminals aiming to steal classified intelligence and other highly sensitive military and government data, disrupt supply chains, and compromise critical defence infrastructure.

Another likely reason A&D executives cited cyber threats as the top near-term risk for their organisations is the need to comply with the Cybersecurity Maturity Model Certification (CMMC) 2.0.[1] This framework requires certain defence contractors to meet stringent cybersecurity standards to qualify for government contracts. It also presents several challenges for A&D companies, large and small.

The cost of achieving and maintaining compliance with CMMC 2.0 can be substantial, requiring investments in cybersecurity infrastructure, personnel training and continuous monitoring systems. Firms also face a complex certification process that involves third-party assessments and adherence to strict security controls. The evolving nature of cyber threats places particular pressure on larger defence contractors to ensure that their entire network is CMMC 2.0 compliant.

AI and emerging technologies: a double-edged sword for A&D

Implementing emerging technologies can also introduce cybersecurity risks for A&D firms. However, according to our latest Top Risks survey, the leaders of A&D organisations seem more concerned about skills gaps undermining their ability to bring these technologies into their everyday workflows and use them effectively. They cited the "adoption of AI and other emerging technologies requiring new skills in short supply" as their second most concerning risk issue for the near term.

AI has already demonstrated its value in enhancing battlefield intelligence, optimising manufacturing processes, improving maintenance efficiency and more. Yet, despite these benefits, many A&D firms remain cautious about large-scale AI deployments due to concerns about data security and AI governance. Integrating AI into legacy systems also presents technical difficulties and often requires a substantial investment in IT modernisation. (Notably, concerns about the limitations of legacy technology rank fifth among near-term risks for the A&D industry.)

---

[1] "U.S. Department of Defense Updates Cybersecurity Maturity Model Certification Requirements: CMMC 2.0," Technology Insights Blog, Protiviti, November 10, 2021: https://tcblog.protiviti.com/2021/11/10/u-s-department-of-defense-updates-cybersecurity-maturity-model-certification-requirements-cmmc-2-0/.

The A&D sector is in dire need of professionals with expertise in AI, cloud computing and advanced data analytics. However, competition with the private sector — from big tech firms to financial services providers — has made it increasingly difficult for A&D companies to attract and retain top talent. Some organisations have been stepping up investment in internal training programmes and forming partnerships with universities and technology companies to build a pipeline of skilled workers. The question is whether these efforts are too little, too late — especially for firms already well behind the new-tech adoption curve.

The A&D sector is in dire need of professionals with expertise in AI, cloud computing and advanced data analytics. However, competition with the private sector — from big tech firms to financial services providers — has made it increasingly difficult for A&D companies to attract and retain top talent.

Economic pressures and geopolitical uncertainty looming large for the A&D sector

Beyond technological concerns, A&D firms must contend with economic and geopolitical volatility, which also rank among the top 10 near-term risks for these businesses — in third and seventh place, respectively.

Defence budgets are highly sensitive to shifting government priorities, and recent years have seen significant changes in how funds are allocated. In the U.S., for example, there has been a growing emphasis on cyber defence, space security and AI-driven warfare, which has led to reduced spending in some traditional defence areas. The U.S. Department of Defense itself is not immune to the current cost-cutting measures by the federal government. It is worth noting, however, that the Pentagon is also prioritising spending on drones, submarines and other investments, which could benefit many A&D firms.[2]

Meanwhile, rising global tensions, from conflicts in Eastern Europe to increasing competition between the U.S. and China, have created uncertainty around military procurement strategies. Allied nations are planning to invest more in their own defence capabilities and reduce their reliance on U.S.-based contractors. Stricter trade restrictions have also limited market access for some A&D firms.

Inflation has further complicated financial planning for businesses in the A&D industry, with rising material costs and wage pressures squeezing their margins. Many firms are now exploring cost-optimisation strategies, including diversifying supply chains, negotiating long-term contracts to hedge against price volatility and investing in more efficient production technologies.

Disruptive innovations and increasing competition from “defence tech” companies

Ranking fourth on the list of top 10 risks for A&D firms for the near term is the “rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces.” At the heart of this

[2] “Pentagon proposes $50 billion in annual cuts and identifies priorities to expand,” NPR, February 20, 2025: www.npr.org/2025/02/20/nx-s1-5303947/hegseth-trump-defense-spending-cuts.

challenge is the rise of defence tech startups, which have been shaking up the traditional A&D landscape dominated for decades by large legacy companies.

Legacy A&D firms have operated under a business model that prioritises long-term, performance-based milestone contracts that require significant overhead and time-consuming development cycles. In contrast, the new wave of defence tech startups operates with leaner models, lower costs and greater overall agility. These businesses are also able to incorporate AI and other leading-edge technology into their products and services faster and more easily than most legacy firms.

By offering fixed pricing, defence tech companies can also offer government agencies more predictable budgeting, making them an attractive option for procurement. With ongoing pressure to reduce spending and accelerate procurement cycles, it is increasingly likely that agencies will continue turning to more agile firms — thus permanently altering the competitive landscape of the defence sector.

Legacy infrastructure falling short — but modernisation efforts may be at risk

Rounding out the top five near-term risks for A&D is “operations and legacy infrastructure unable to meet performance expectations.” Many large A&D firms continue to rely on aging enterprise resource planning (ERP) systems — often late-generation versions of SAP — alongside a fragmented array of legacy technologies that hinder operational efficiency. Legacy companies are also grappling with disparate data structures that undermine data processing and aren’t optimised for AI integration.

Some A&D companies are pursuing multibillion-dollar technology modernisation initiatives designed to overhaul their IT infrastructure and streamline operations. However, with the current trend towards reduced spending by the U.S. government, there is growing concern in the A&D industry that these ambitious and costly efforts may need to be scaled back or delayed. This could leave legacy firms further behind in the race to innovate and keep pace with more nimble defence tech companies.

Risk category	Top 10 near-term risk issues	Score
O	**1.** Cyber threats	2.98
S	**2.** Adoption of AI and other emerging technologies requiring new skills in short supply	2.86
M	**3.** Economic conditions, including inflationary pressures	2.86
S	**4.** Rapid speed of disruptive innovations enabled by new and emerging technologies	2.84
O	**5.** Operations and legacy IT infrastructure unable to meet performance expectations	2.75

S	**6.** Social media developments and platform technology innovations	2.75
M	**7.** Geopolitical shifts, regional conflicts and instability in governmental regimes	2.72
M	**8.** Access to capital/liquidity	2.70
M	**9.** Talent and labour availability	2.68
O	**10.** Third-party risks	2.68

Each risk was rated in terms of its relative impact using a five-point Likert scale, where a score of 1 reflects “No Impact at All” and a score of 5 reflects “Extensive Impact” to their organization over the near term (next two to three years).

An overview of the top long-term risks for the A&D industry

A&D industry leaders have identified workforce availability as the top strategic risk for their businesses looking out to 2035. The industry’s workforce is aging rapidly, and replacing these workers where needed is proving to be an arduous if not impossible task for many companies, especially in the current climate.

Historically, A&D careers offered stability, pensions and long-term job security, but shifting societal norms and labour market conditions have altered workforce preferences. Combined with increased layoffs in the federal workforce due to budget constraints, the appeal of A&D careers is greatly diminished for new generations of workers. The rise of defence tech startups is also reshaping hiring dynamics for the A&D industry, creating less need for back-office personnel to help support long-term defence contracts.

The A&D industry is changing — fast. The next decade for this sector will be defined by the companies that can anticipate and adapt to the many diverse risks already present or emerging and develop effective strategies that will ensure they are ready to take on what’s next.

While workforce concerns dominate the long-term risk outlook for A&D executives, many also anticipate that disruptive innovations will continue to be a top strategic challenge for their organisations in the coming decade. The adoption of AI and automation will only accelerate, but as we’ve already covered here, many A&D firms lack the infrastructure and personnel to implement these technologies effectively.

Government regulations and ethical considerations surrounding the use of AI in the defence industry are likely to further complicate the adoption of this emerging technology.

Long-term operational risks for the A&D industry remain centred on cyber threats and third-party risks. As companies continue to rely on legacy technologies, cybersecurity vulnerabilities will no doubt persist, while the introduction of AI-driven solutions will introduce new risks. Additionally, supply chain concerns remain high, as government agencies demand greater transparency into lower-tier suppliers, where bottlenecks and compliance challenges often arise.

A&D companies have long enjoyed access to large and long-term contracts, a steady stream of mission-critical work, and workforce stability. But the A&D industry is changing — fast. The next decade for this sector will be defined by the companies that can anticipate and adapt to the many diverse risks already present or emerging and develop effective strategies that will ensure they are ready to take on what's next.

Macroeconomic risk issues

Risk	Percentage
Talent and labour availability	39%
Impact of expected demographic changes	33%
Changes in global markets and trade policies	25%

Strategic risk issues

Risk	Percentage
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces	44%
Adoption of AI and other emerging technologies requiring new skills in short supply	40%
Limited opportunities for organic growth	26%

Operational risk issues

Risk	Percentage
Cyber threats	40%
Third-party risks	33%
Uncertainty surrounding core supply chain ecosystem	25%

Note: Respondents were asked to identify the top two risks in each category (macroeconomic, strategic, operational) separately. That is, respondents identified six risks (two in each category) as "top two" risks. For each category, the three risk issues (including ties) receiving the most responses by percentage are shown.

About the Executive Perspectives on Top Risks Survey

We surveyed 1,215 board members and executives across a number of industries and from around the globe, asking them to assess the impact of 32 unique risks on their organisation over the next two to three years and over the next decade, into 2035. Our survey was conducted online from mid-November 2024 through mid-December 2024. For the near-term outlook, each respondent was asked to rate 32 individual risks on a five-point Likert scale, where 1 reflects “No Impact at All” and 5 reflects “Extensive Impact.” For each of the 32 risks, we computed the average score reported by all respondents and rank-ordered the risks from highest to lowest impact.

We also asked executives to share their perspectives about long-term risks (over the next 10 years to 2035) by selecting the top two risks from each of the three dimensions (macroeconomic, strategic and operational). For each of the 32 risks, we calculated the percentage of respondents who included that risk as one of their two top risks for each dimension.

Read our *Executive Perspectives on Top Risks Survey* executive summary and full report at www.protiviti.com or http://erm.ncsu.edu.

About the author

Dave has extensive experience in the areas of information technology auditing, computer-aided auditing techniques, audit formation, risk assessments, quality assurance reviews, financial controls and board reporting.

Dave is one of the founding members of Protiviti and during his tenure has held various 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®