

Emerging Risk I: Edge AI Application Scaling Challenges

Subject	Description
Description of the Risk	The significant difficulty and inherent risks associated with transitioning diverse artificial intelligence (“AI”) applications from successful pilot stages to reliable, manageable, secure, and commercially viable deployments at scale across heterogeneous industrial edge environments. Successfully scaling AI from pilot projects to widespread, reliable deployment across diverse industrial edge environments presents significant emerging risks for technology providers like Advantech. These challenges include: • Integration and Management Complexity: Significant obstacles to reliably integrating diverse AI models, various edge hardware, and OT/IT systems across large-scale and heterogeneous edge deployments, compounded by the lack of mature MLOps practices to efficiently manage the entire AI lifecycle, and a lack of consistent and reliable data sources, all hindering high performance and reliability, which creates major obstacle for Edge AI Development. • Security & Compliance Burdens: Exponentially increased difficulty in securing the vast attack surface of distributed edge AI systems and ensuring compliance with complex, evolving global AI/data regulations as deployments scale. • Technology Velocity & Ecosystem Gaps: Rapid evolution of AI/edge technologies risks obsolescence, while gaps in ecosystem standards and specialized skills hinder the creation and scaling of robust, interoperable solutions and create talent bottlenecks. • Blurring Value Chain Roles & Disintermediation Risk: The complexity of scaling enables players at different layers to offer more vertically integrated solutions, potentially disintermediating traditional hardware or platform providers who cannot effectively bridge the scaling gap for customers.
	Failure to effectively address the challenges of scaling Edge AI and assist customers and partners in overcoming these obstacles could have a significant impact on Advantech: • its products may be less competitive compared to solutions that are easier to integrate and use. This could diminish the value of its hardware or result in a loss of pricing power, thereby hindering revenue growth and leading to a decline in market share.

Impact to Advantech	• Due to the complexity of scaling, any inability to ensure reliability or maintain high performance in large-scale AI deployments could severely damage customer trust and Advantech's brand reputation in industrial reliability. • Failing to effectively facilitate scalable AI solutions could prevent Advantech from seizing market opportunities driven by advanced edge intelligence, limiting expansion into high-value application domains. • If partners perceive building and scaling solutions on Advantech's platform as overly complex or costly, ecosystem engagement may slow down, reducing market coverage and ultimately jeopardizing Advantech's leadership in providing Edge AI solution.
Mitigation actions	Advantech is focused on providing advanced Edge Computing Platform (WISE-Edge), with high degree of hardware and software integration to help customers accelerate large scale deployment, reduce ROI cycle. These tools and ecosystem support will help industry users to confront the industrial AI scale challenges: • Develop Enabling Platforms and Solution Frameworks: Heavily invest in the WISE-Edge platform to provide unified management, hardware abstraction, optimized software components, and vertical reference architectures, thereby simplifying scalable deployments and reducing risks. • Build Strategic Partnerships and Ecosystem: Actively collaborate with system integrators, AI experts, silicon vendors, and cloud platforms to provide more complete, pre-integrated solutions and navigate the evolving value chain. • Embed Security and Ensure Compliance Readiness: Build robust, scalable security features into platforms and hardware, and proactively design for compliance with emerging global AI and data regulations relevant to large-scale industrial deployments. • Enhance Internal Competency and Talent Development: Invest in internal training programs, cross-functional team development, and strategic hiring to build the specialized, integrated skill sets necessary to support customers and develop scalable solutions. • Strengthen Customer and Partner Enablement: Provide comprehensive training, documentation, scalable support models, and potentially professional services specifically focused on guiding customers through the challenges of deploying and managing Edge AI solutions at scale.

Emerging Risk II: Operations & Talent Risks Derived from Agentic AI Technology

Subject	Description
Description of the Risk	Agentic AI technology erupted in 2025 as cutting-edge AI agent solutions. They can autonomously plan, create, and execute tasks, which is fundamentally different from previous AI agent technologies. If the company fails to timely adopt such technology into internal operations and to develop or acquire required talent, operational efficiency and organizational competitiveness will be impacted. Key challenges include: • Computing Infrastructure and Cost Management Complexity: The new technology requires employees with new skills to manage on-premise computing server clusters, ensuring sufficient computing power at a reasonable cost. Such talent is scarce in the market; we need to hire through the right channels, retain them well, and also grow such talent internally. • Shift in AI Agent Management Approach: Agentic AI Agents automatically create tasks and execute them, requiring a management approach fundamentally different from before. AI Harness (the control framework for AI agents) becomes a critical topic; we need to hire and grow people capable of AI Harness to keep agent behaviors safe, controllable, and auditable. • Business Transformation Mindset: Agentic AI Agents need to be defined jointly by AI engineers and business users. The company needs business users with the right mindset for this transformation; hiring such people externally is difficult, so we need to grow them internally through training programs. • Multi-Agent Orchestration: As Agentic AI Agents proliferate, they need to be connected and orchestrated with each other, which requires employees with new types of AI agent skills. • Data Governance and Security: Agentic AI Agents require broad access to internal systems and data, significantly increasing the complexity of permission management, data security, and confidentiality protection; talent with AI security governance capability is required. • Rapid Technology Iteration: Another new type of AI agent technology may emerge in the near future. The company must have people who can quickly learn new AI technologies to ensure we keep up with the latest developments.

Impact to Advantech	1. Falling Behind in Operational Efficiency: If competitors adopt Agentic AI Agents to automate internal processes first, their cost and speed advantages will erode Advantech's operational competitiveness. 2. Talent Gaps Delaying Adoption: Inability to recruit or retain talent with new skills such as computing cluster management, AI Harness, and multi-agent orchestration will delay AI adoption and limit operational efficiency gains. 3. AI Governance Failure: Without proper control, autonomous agents may automatically execute wrong tasks, make erroneous decisions, or improperly access data, causing operational disruption, data leakage, or compliance risks. 4. Cost Overrun Risk: With dramatically increased token consumption, adoption costs may exceed benefits without a sound computing strategy and cost management, making return on investment uncertain. 5. Stalled Organizational Transformation: If business users lack the right transformation mindset, AI remains isolated point tools and cannot scale, weakening both organizational competitiveness and attractiveness to next-generation talent.
Mitigation actions	1. Establish AI Governance Organization and AI Harness Framework: Define the Autonomous AI Agent adoption roadmap, control standards (AI Harness), and permission and audit mechanisms, ensuring agents remain safe and controllable. 2. Computing Infrastructure and Cost Management: Plan on-premise computing server clusters and a hybrid-cloud computing strategy to ensure sufficient computing power at reasonable cost; recruit and develop talent capable of managing computing clusters. 3. Strategic Talent Recruitment and Retention: Define key new roles (e.g., AI infrastructure engineer, AI Harness engineer), recruit through the right channels (specialized headhunters, tech communities, industry-academia collaboration), and retain scarce talent with competitive compensation and incentives. 4. Internal Talent Development and Transformation: Build business users' AI transformation mindset and engineers' new AI agent skills through training programs. 5. Business-AI Co-creation: Establish mechanisms for AI engineers and business users to jointly define Agentic AI Agents, expanding from pilots to scaled deployment to ensure adoption fits business needs and delivers real benefits. 6. Continuous Technology Sensing and Fast Learning: Build a technology radar and partnerships with external players (AI vendors, academia), and develop fast learners of new AI technologies so the company can promptly master and adopt next-generation AI agent technologies.