Please refer to the original text for accuracy.

Chief AI Officer Guidebook

(Version 1.00)

March 1, 2026

Japan AI Safety Institute (J-AISI)

AISI Japan AI Safety Institute

Table of Contents

1. Introduction

The use of artificial intelligence (AI) has become a critical factor in promoting innovation, advancing and streamlining operations, and creating new customer value in companies. In particular, the rapid development of AI technologies, including generative AI, is bringing significant changes to the way business is operated, to decision-making, and to the planning and design processes for products and services. At the same time, the introduction and operation of AI involve multifaceted issues, including the protection of intellectual property and personal information, the accuracy and explainability of outputs, the fairness and safety of algorithms, cybersecurity, and compliance with reputational risk considerations and legal and regulatory requirements. These issues cannot be fully managed through the efforts of individual departments alone and require decision-making at the management level and integrated governance.

Against this backdrop, the role responsible for leading efforts to maximize corporate value and secure trust by using AI in an integrated manner with data strategy and technology strategy, treating risks in an integrated manner as a management agenda, and realizing innovation and digital transformation is the Chief AI Officer (CAIO). Moves to strengthen AI governance are also advancing in the public sector. For example, governance requirements premised on the designation (or establishment) of a CAIO have been set out for federal agencies in the United States, and in Japan's national administrative organs as well, the establishment of a Chief AI Officer (CAIO) is required under the "Guideline for Ensuring the Appropriateness of Research & Development and Utilization of Artificial Intelligence-Related Technology"[1] pursuant to Article 13 of the AI Act[2], as well as under the Digital Agency's "The Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration"[3]. In companies as well, regardless of size, the importance of developing and strengthening the CAIO function is increasing.

---

[1] Guideline for Ensuring the Appropriateness of Research & Development and Utilization of Artificial Intelligence-Related Technology
December 19, 2025, Decision of the Artificial Intelligence Strategic Headquarters

[2] The Act on Promotion of Research and Development, and Utilization of AI-related Technology (AI Act)
Establishment: May 28, 2025. Partial enforcement: June 4, 2025. Full enforcement: September 1, 2025

[3] Digital Agency: The Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration
Published: May 27, 2025

This guidebook is intended primarily as a practical reference for private-sector business operators to establish a CAIO and ensure that the role can be performed effectively. It organizes and compiles guidance and practical examples concerning the purpose of establishing a CAIO, its roles and responsibilities, the skills required, organizational structures and collaboration with other CxOs, and perspectives on securing and developing human resources. Its purpose is thereby to contribute to sustainable business operations in the age of AI, to improving the quality of products and services provided to customers and users, and to securing trust. However, it does not have legally binding force. The primary intended users are the CAIO and senior executives considering the appointment of a CAIO. This guidebook should also be operated as a Living Document that is revised on an ongoing basis in light of developments in AI technologies, changes in the business environment, and revisions to relevant laws, regulations, and guidelines.

---

2. Purpose of Establishing a CAIO

The adoption and use of AI offer significant potential for more sophisticated decision-making, greater operational efficiency, and improved customer experience. At the same time, however, issues such as uncertainty specific to AI models, data quality and rights clearance, AI-specific security challenges, ethics and legal compliance, reputational risk, and organizational capabilities and talent are emerging simultaneously, increasingly creating complex issues that require a cross-functional response. In such circumstances, existing structures alone, such as the Chief Data Officer (CDO) and Chief Information Officer (CIO), may not always be sufficient to continuously undertake, in an integrated manner, both the promotion of AI use and the control of associated risks. Accordingly, the purpose of establishing a CAIO is to formulate and drive policies for AI use that are aligned with business strategy under specialized expertise and leadership in the AI domain, while also maintaining visibility into AI use across the company and overseeing both risk management and value creation.

Some companies may have positions responsible for the digital domain, such as a Chief Digital Officer. This chapter, however, organizes the purpose of establishing a CAIO from the perspective of integrally undertaking both the promotion of AI use and governance.

3. Roles and Responsibilities of the CAIO

Each business operator needs to actively leverage AI technologies, including generative AI, in its operations while simultaneously achieving the provision of safe and reliable products and services, the protection of the rights of customers and users, and more advanced risk management. As the central coordinating function for these efforts, the CAIO is responsible for formulating and advancing policies, ensuring governance (control), and providing accountability in the following areas. At the same time, final business decisions in individual cases are the responsibility of the relevant business owner, and this does not alter the allocation of ultimate legal responsibility under the Companies Act or other applicable laws and regulations.

3.1 Formulation and Execution of AI Strategy

- **Presenting a vision and formulating a roadmap**
  Formulate a vision for leveraging AI and a medium-term roadmap aligned with management strategy and business KPIs, and, based on an analysis of management and organizational issues, formulate an AI adoption strategy that supports greater operational efficiency, improved quality, and a better customer experience.
- **Investment decisions and value management (including ROI)**
  Organize investment priorities for human, physical, and financial resources related to AI development and AI use, and lead efforts to make value visible and drive improvement cycles through KPIs, ROI, and other indicators.
- **Selection of priority use cases**
  Comprehensively assess expected benefits and risks (such as information leakage and bias) and determine and update the portfolio of priority use cases.

3.2 Oversight of Planning, Development, Procurement, and Implementation Processes

- **Oversight from planning through implementation**
  For use cases that are valuable to the company, oversee the processes for developing AI models or procuring and deploying external solutions based on standards and gates agreed with relevant departments.

- **Selection of technologies and services**
  Keep track of the latest technological and research developments and select models, data, systems, and services appropriate for business operations. Also support the promotion of company-wide cross-functional joint projects and common functions.
- **Advancement of data infrastructure and data management**
  In collaboration with the CIO and CDO, advance data strategy and management, including data collection, preparation, analysis, utilization, quality management, and privacy protection.

3.3 Governance, Ethics, and Compliance

- **Establishment of an AI risk management structure**
  Based on the existing risk management structure, identify and organize potential organization-level risks, cross-functional risks, project-level risks, and clarify the responsible persons and decision-making processes for each. Also establish policies and frameworks to promote data privacy and security.
- **Maintenance of records and evidence**
  Use the AI inventory, risk register, AI Impact Assessment (AIIA), model cards, datasheets, KPI dashboards, and other tools to maintain evidence that can withstand use case review, operational oversight, and audit.
- **Establishment and dissemination of AI use rules**
  For AI systems, including generative AI, maintain centralized visibility over the entire lifecycle, including planning, data handling, procurement, deployment, operation, and responses to incidents specific to AI systems, and establish rules for use. Communicate these rules to employees (including directors, officers, and staff members) and implement education and awareness-raising in a planned manner regarding matters such as the handling of input data and risks such as hallucinations.
- **Continuous review of rules**
  In light of AI technology trends, changes in business conditions, and revisions to relevant laws, regulations, and various guidelines, conduct reviews and revisions on an ongoing basis under the responsibility of the CAIO.
- **Assessment and escalation of high-risk cases**
  Conduct assessments based on the company’s definitions of high risk and determination procedures, and report cases determined to be highly likely to fall under high-risk categories to organizations or committees responsible for risk management, such as an

AI ethics committee or risk committee, and respond based on the advice received. Such reporting should be carried out not only during development and operation, but also as needed when risk cases arise and after responses have been completed.

- **Authority to halt or block deployment**
  For use cases with a high impact on rights and safety, it is desirable to establish a framework under which the CAIO is granted veto authority, including the authority to suspend or block deployment into production, and approval by the Company-wide AI Steering Committee and a final human decision are required. In making such decisions, the CAIO should proceed through review by relevant committees while, in emergencies, taking prompt suspension measures and escalating to senior management and the board of directors as necessary.
- **Regulatory compliance and the practice of AI ethics**
  In collaboration with relevant departments, promote responses, including determining whether responses are required, to domestic and international AI-related laws and guidelines (e.g., Japan's AI Act, the AI Guidelines for Business, the EU AI Act, the Act on the Protection of Personal Information, the Copyright Act, and sector-specific laws), while also advancing the implementation of AI ethics, root cause analysis of algorithmic bias and necessary countermeasures, and the ensuring explainability.
- **Incident response**
  Clearly define major AI incidents (such as misdiagnosis, false positives, and information leakage), and establish a series of response processes covering reporting, initial response, impact assessment, and the formulation of recurrence prevention measures. Where risk cases specific to generative AI arise, respond appropriately in collaboration with the provider or partner of generative AI, according to the level of importance and degree of impact.
- **Use of external conformity assessments and certifications**
  Based on the maturity of the company's AI governance, business strategy, business scale, regulatory environment, and customer requirements, formulate a policy on whether to use third-party certifications (e.g., ISO/IEC 42001) and external assessments.
- **Governance involvement in contracts and procurement**
  In collaboration with operational departments such as procurement and legal, identify risk items and governance considerations at the procurement stage, and confirm and rectify whether contract terms and service specifications are aligned with internal

policies and required standards (including security, data handling, rights clearance, and auditability).

3.4 Organizational Transformation and Talent Development

- **Transformation of organizational culture and operations**
  Drive transformation across overall business operations, including business process redesign, reviews of organizational structures, and performance evaluation systems, without limiting AI use to the mere introduction of tools.
- **Development and securing of AI talent**
  Promote the recruitment and development of AI professionals, improvements in AI literacy among all employees, and reskilling.
- **Promotion of AI adoption across the organization**
  Provide leadership for the adoption and embedding of AI across the organization.

3.5 Internal and External Collaboration and Communication

- **Reporting to senior management and the board of directors**
  Review operational status and AI adoption status, major incidents, major KPIs, and similar matters at the Company-wide AI Steering Committee at least once a month, and report to management meetings and similar forums approximately once every quarter. Report on AI governance maturity, major risks, and important investment decisions to the board of directors at least once a year.
- **Engagement with stakeholders**
  Work with senior management, heads of divisions and departments/sections, employees, external partners, and other relevant parties to advance decision-making and execution with respect to AI policies and measures. As needed, also promote external collaboration with other companies, AI vendors, academic and research institutions, startups, and other relevant organizations.
- **External communication and education**
  Fulfill accountability through external communications regarding the company’s AI strategy and initiatives and through explanations to customers and related parties and share the company’s approach and vision for AI both inside and outside the organization. As needed, also respond as a spokesperson on AI-related issues. In addition, accountability in this context includes not only reporting to senior management and the board of directors and providing explanations to internal and external

stakeholders but also audit response and the recording and evidence management of decision-making processes.

---

4. Skills and Competencies Required for a CAIO

A broad range of skills and competencies is required of the CAIO in order to connect AI-driven value creation to business outcomes, manage and control risks, and strengthen execution capability across the organization. The key skills and competencies expected of the CAIO are organized below. This section does not assume that a single CAIO will possess all of the elements listed here at a high level. Rather, it assumes that the CAIO will build on their own strengths as a core and complement them through role allocation with a team reporting directly to the CAIO described later.

4.1 Technical Understanding and Application Capability

- Has a foundational understanding of machine learning, natural language processing, generative AI (large language models, retrieval-augmented generation, etc.), and MLOps, and can organize key considerations (data, evaluation, operations) when applying them to the organization’s use cases.
- Understands the characteristics and risks of generative AI (hallucinations, bias, lack of transparency, etc.) and can clearly communicate internal points of attention for business use.
- Incorporates perspectives such as cybersecurity, data governance, and privacy protection, and can translate them into requirements for AI systems (data handling, access controls, audit, logs, vendor management, etc.).

4.2 Strategic Thinking and Insight Into Business and Regulatory Environments

- Connects management objectives and business challenges with the characteristics and advantages of AI and can develop an AI adoption roadmap from a company-wide optimization perspective.
- Takes into account marketability, feasibility, and risks, can design and drive performance measurement (KPI/ROI, etc.) and continuous improvement cycles.

- Incorporates external knowledge from government–industry collaboration, academia and research institutions, startups, and other sources, and improves the quality of decision-making for both business and governance.

4.3 Capability to Drive Organizational Transformation and Leadership

- Can lead cross-functional projects and drive them forward while coordinating interests among stakeholders.
- Can implement AI not merely as the introduction of tools, but as a transformation of organizational culture that includes business process redesign, talent allocation, and evaluation systems and related policies.
- Can systematically promote AI literacy improvement, training, and reskilling for executives and employees, and build mechanisms for talent development.
- Maintains a stance of continuously learning about the latest AI technologies and societal trends and agilely reflecting them in measures and rules.

4.4 Ethics, Legal, and Risk Management Capability

- Has an advanced understanding of AI ethics and legal compliance and can operationalize them as internal rules and review and approval processes.
- Can identify and assess potential risks—such as false or incorrect outputs (such as hallucinations) and biases—and design an end-to-end risk management process that covers establishing and executing mitigation measures and continuous monitoring.
- When making decisions on leveraging high-risk AI, can coordinate with organizations and committees responsible for risk management, such as an AI ethics committee or a risk committee, and escalate appropriately.
- Maintains an awareness of accountability and can sustain governance from the perspectives of fairness, transparency, and societal trust.

4.5 Adaptability and a Forward-looking Mindset

- Continuously tracks trends in international standards and state-of-the-art technologies and maintains a global perspective to adapt them to the organization’s environment.
- In the fast-changing AI domain, can flexibly shift direction with agile thinking and make rapid decisions.

5. Organizational Positioning and Structure of the CAIO

This chapter presents key points for designing the CAIO's organizational positioning and structure so that the CAIO can effectively perform the role, taking into account the content of this guidebook.

5.1 Placement of the CAIO and the AI Governance Office (AI Enablement Team)

- **Establishment of the Company-wide AI Steering Committee**
  Establish a Company-wide AI Steering Committee chaired by the CAIO, and handle as standing agenda items such matters as the review of new use cases, review of major KPIs, and the reporting of incidents and complaints and related remediation plans (with at least once a month as a general rule).
  The recommended approach is to establish the CAIO as an independent C-suite position reporting directly to the CEO. In doing so, it is desirable to ensure both a reporting line directly connected to management (e.g., regular reporting to the CEO and management meetings) and an authority structure that enables cross-functional decision-making to proceed efficiently. Even where the CAIO must unavoidably be placed under another CxO, internal rules should ensure direct reporting to the CEO and management meetings, as well as committees or similar bodies that provide oversight of risk-related judgments.
- **Organizational placement**
  The CAIO function should be placed in a department with a company-wide strategic planning function (e.g., corporate strategy, digital strategy, or DX promotion), so that it does not remain merely an extension of the information systems department. Alternatively, it is desirable to grant equivalent authority.
  Note: Even where the function is placed under IT or DX, the organization should be designed together with authority sufficient to involve business departments, legal/compliance, risk management, and other relevant functions, as well as committees or similar bodies that provide oversight of risk-related judgments.
- **Establishment of a core team supporting the CAIO (AI Governance Office/AI Enablement Team)**
  Under the direct supervision of the CAIO, establish an AI Governance Office/AI Enablement Team to support the CAIO (e.g., AI promotion managers, AI data scientists,

and personnel responsible for AI ethics and governance), and supplement the expertise required for AI use in each department. The structure should be designed flexibly according to the size of the organization and the complexity of operations, including the use of external specialized personnel.

- **Connections with frontline operations**
  Appoint personnel responsible for or promoting AI use in each department (e.g., AI leads or AI champions), and, in coordination with the central AI Governance Office/AI Enablement Team, create a structure in which the cycle of identifying candidate projects, implementation, operation, and improvement can function effectively.

5.2 Internal and External Collaboration

- **Collaboration with internal stakeholders**
  As examples, the following should be designated as standing coordination counterparts:
  - Business departments (use case ownership, KPI/ROI, business requirements)
  - Development/operations (model and system design, MLOps, operational quality)
  - Information security (threat analysis, access control, logs/audit, incident response)
  - Legal, compliance, and privacy (laws and regulations, contracts, rights clearance, accountability)
  - Procurement (contract terms, service-level agreements, vendor management)
  - Risk management (risk assessment, approval, escalation)

  On this basis, clarify for each case who makes decisions, who implements, and who provides oversight.
- **Coordination with external experts and institutions**
  As needed, collaborate with external specialized personnel and consulting organizations in order to incorporate best practices, provide quality assurance, and strengthen the ability to respond to the latest risks.
  Also refer to information issued by public institutions that address evaluation methods and standards related to AI safety (e.g., Japan AI Safety Institute[4]) and use it to improve the company's governance.

[4] Japan AI Safety Institute

- **Establishment of an AI lab/sandbox (experimentation and validation environment)**
  To enable rapid evaluation of AI technologies and validation of use cases, establish an "AI lab" or "sandbox environment" within the organization and create a framework that enables frontline departments to safely carry out validation and testing (including controls on data export, use of synthetic data, log collection, and review processes).

---

6. Coordination Between the CAIO and Other CxOs

The CAIO is not merely responsible for technology or individual projects but serves as a leader in advancing AI strategy across the company. To maximize the value of AI, it is important for the CAIO to work in coordination with each CxO while keeping in mind alignment on business objectives, attention to ethics, transparency, and legal compliance, continuous communication, and the visualization of outcomes and feedback. Particularly in the area of AI governance, there are many aspects in which the CAIO's remit is likely to overlap with that of the Chief Data Officer (CDO) in data, the Chief Information Officer (CIO) in IT, and the Chief Information Security Officer (CISO) in security. Accordingly, when coordinating with each CxO, it is desirable to align in advance on role allocation and decision-making approaches from the following perspectives:

- Matters to be agreed jointly (e.g., AI adoption roadmaps, review and approval gates, KPIs, and standards for data handling and vendor management)
- The scope under the CAIO's oversight and the scope executed by each CxO and department (division of responsibilities)
- The frequency of regular meetings and reporting, and escalation routes (major incidents, high-risk cases, etc.)

Set out below are representative examples of roles and key coordination points (to be added to or adjusted according to the company's circumstances).

Role example	Coordination Points
Chief Technology Officer (CTO)	◦ Discuss the selection of AI technologies and implementation approaches and share the technology roadmap. ◦ Consult on how AI will be leveraged in products or production lines.

	◦ Integrate AI systems into existing infrastructure from the perspectives of infrastructure, architecture, and operations. ◦ Coordinate on establishing technical standards, developing technical talent, and allocating AI-related R&D budgets.
Chief Data Officer (CDO)	◦ Jointly drive data collection, quality management, and governance required for AI projects. ◦ Cooperate on establishing and enforcing rules for ethical data use and privacy protection in data use. ◦ Continuously discuss alignment between data strategy and AI strategy, and update priorities.
Chief Information Officer (CIO)	◦ Collaborate on company-wide optimization of IT systems associated with AI adoption, cost management, IT governance, and establishing IT standards. ◦ Share plans for designing integration between AI-related systems and core business operations, as well as the overall plan for advancing digital transformation (DX). ◦ Identify IT-related threats and challenges that increase with AI use and consider mitigation measures.
Chief Information Security Officer (CISO)	◦ Jointly develop security enhancements enabled by AI and risk response measures. ◦ Cooperate on measures for AI data protection and the prevention of model misuse (unauthorized use, data leakage, etc.). ◦ Exchange views regularly on updates to security standards and response measures.
Chief Supply Chain Officer (CSCO)	◦ Collaborate on developing strategy for AI deployment across the supply chain (forecasting, optimization, risk management, etc.). ◦ Discuss supply chain data use and AI and data collaboration with external partners. ◦ Drive training and change management to support the adoption of AI tools in frontline operations.
Chief Human Resource Officer (CHRO)	◦ Jointly plan and execute initiatives for recruiting and developing AI talent, reskilling, and improving AI literacy.

	◦ Work together on work process transformation, organizational design, job role shifts and change management driven by AI deployment. ◦ Exchange views on the impacts of AI deployment on employees, including from the perspectives of ethics, transparency, and fairness.
Chief Operating Officer (COO)	◦ Collaborate on deployment planning for leveraging AI in work process transformation and on setting KPIs. ◦ Drive business process redesign (to-be design) and standardization and agree on operational design to embed use of AI into day-to-day operations (role allocation, procedures, and delineation of responsibilities). ◦ Establish cycles for post-go-live quality and stable operations (service-level agreements: SLA / service-level indicators: SLI, monitoring and logs, performance measurement) and continuous improvement, and coordinate on escalation and remediation operations when deviations or defects occur.
Chief Executive Officer (CEO)	◦ Appoint the CAIO and clarify the CAIO's mission, authorities, and resources (staffing and budget). ◦ Consult with the CAIO on alignment between the company-wide AI strategy, management strategy, and risk appetite and make the final decision. ◦ Receive regular reports from the CAIO and the Company-wide AI Steering Committee and make decisions on matters involving high-risk AI and on significant incidents. ◦ Chair discussions and lead decision-making at the board of directors and executive management committee level on reviews of the AI governance structure and policies.
Chief Financial Officer (CFO)	◦ Collaborate on budget allocation and prioritization for AI investments (CAPEX/OPEX) from a company-wide portfolio perspective.

	◦ Jointly design and operate a balanced evaluation of AI investment ROI/KPI, costs, and risks (value-based management). ◦ Coordinate on designing and reviewing investment decision rules—taking into account financial constraints and risk appetite—including approval gates and evaluation timing.
Business Owner	◦ Collaborate on identifying and selecting critical use cases, developing value hypotheses, and setting KPIs. ◦ Agree on approaches to PoC and evaluation and on scaling decisions (go-live/exit), together with risk assessment. ◦ Organize business and operational requirements (adoption in frontline operations, quality, and delineation of responsibilities) and lead coordination with development, operations, and governance functions.
Legal/Compliance	◦ Collaborate on establishing and updating internal rules (rules for use, review and approval processes, etc.) based on interpretations of AI-related laws and guidelines. ◦ Jointly confirm and remediate matters related to contracts and procurement (vendor management, rights clearance, auditability, clauses related to accountability, etc.). ◦ Coordinate on escalation, regulatory engagement, internal investigations, and corrective measures when matters involve high-risk AI or when significant incidents occur.
Data Protection Officer (DPO)	◦ Oversee data protection design, including the Privacy Impact Assessment (PIA), and coordinate on implementing privacy-by-design. ◦ Organize requirements for handling personal data (purpose, minimization of collection and use, retention periods, data subject requests, etc.) and reflect them in requirements definition and reviews for AI projects and AI use cases. ◦ Coordinate on data protection risk assessment and remediation, including vendor management and cross-border

	transfers, and on incident response when significant incidents occur.

7. Securing and Developing AI Talent

Securing and developing AI talent is a foundational and important measure that supports the advancement of AI use and establishing an AI governance structure in companies. The CAIO should define the talent profiles required from both the business strategy and risk control perspectives, and design and promote “acquisition,” “development,” and “retention” in an integrated manner.

7.1 Acquisition of AI Talent

- **Clarification of required roles and recruitment**
  With regard to AI professionals required in light of business and management challenges (e.g., AI planning and strategy design, system development, data analysis, and AI governance), promote external recruitment after clearly defining the required roles and expected outcomes.
- **Bringing in external expertise**
  Create opportunities for collaboration, such as bringing in personnel with the latest expertise from operating companies, academic and research institutions, and startups, as well as joint research and personnel exchanges.
- **Development of an attractive employment environment**
  In addition to salary and benefits, place emphasis on creating work assignments that enable growth, working arrangements that encourage challenge, and an attractive workplace environment.
- **Supplementing capability gaps**
  In operations and projects where specialized knowledge is insufficient within the company, accelerate launch efforts by utilizing external support such as consulting services, while in parallel designing plans for building in-house capabilities (talent development and transfer plans).

7.2 Development of AI Talent

- **Establishment and focused development of a core team**
  Build an AI Governance Office/AI Enablement Team within the company, select employees with a high level of interest and motivation in AI, and conduct systematic talent development through on-the-job training (OJT), reskilling, certification acquisition, and the use of domestic and international learning materials.
- **Role-based skill design**
  For each role, including AI planning, development and operations, data, and governance (including legal, privacy, and security), define the required skills and target proficiency levels, and link training, OJT, and work assignments in order to enhance the effectiveness of talent development.
- **Use of training resources**
  In selecting learning materials and preparing learning plans, make broad use of available training resources such as portal sites including "Manabi DX[5]" of the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency, Japan (IPA), e-learning, and video content.
- **Strengthening company-wide literacy**
  In collaboration with multiple departments, strengthen AI literacy education (including the safe use of data, protection of confidential information, and measures to address AI risks such as hallucinations).
- **Use of educational institutions and public-private collaboration**
  Promote collaboration with educational institutions such as universities and encourage participation in AI education programs developed through public-private collaboration.

7.3 Continuous Learning and Talent Retention

- **Fostering a learning culture and supporting mechanisms**
  In light of the rapid advancement of AI technologies, foster a culture and mechanisms (such as regular training and communities of practice) that enable employees to continuously learn the latest knowledge and best practices.
- **Providing opportunities for practical experience**

[5] Manabi DX (Japanese site)

Utilize AI labs, sandbox environments, and similar arrangements to establish a structure that enables motivated frontline employees to more easily engage in proof-of-concept activities, validation, and experimental challenges.

- **Compensation, career paths, and evaluation**
  Along with devising compensation and career paths and providing appropriate evaluation of outcomes, provide training and opportunities for relearning that bring out individual motivation for growth and specialized skills.
- **Encouraging internal and external exchange**
  Promote talent exchange and information sharing among internal and external subject-matter experts, as well as across companies.

---

8. Conclusion

The CAIO is a “strategic leader for the AI era” who positions AI not merely as a technical means, but as a core technology for business transformation and value creation within the company, and who drives both business growth and AI governance in a balanced manner. To effectively fulfill this role, the CAIO is required to possess not only technical understanding and a strategic vision, but also strong leadership to promote responsible decision-making, including ethics and legal compliance, as well as advance governance and transformation throughout the organization.

Based on the perspectives organized in this guidebook (strategy, process oversight, governance, organizational structure, coordination with other CxOs, and talent development), it is important to advance the provision of trusted products and services and sustainable use of AI that takes into account diverse customers and users. It is hoped that this guidebook will contribute to the appointment of a CAIO and to the establishment and continuous improvement of AI governance structures centered on the CAIO.