# Current Status and Strategies of Enterprise-Wide Security Governance in Quasi-Governmental Organizations

---

## 1. Introduction

The case of KOICA (Korea International Cooperation Agency) is highlighted as a representative example. KOICA, established in 1991, operates as a quasi-governmental organization that supports economic and social development in developing countries and promotes cooperative relationships. With growing cyber threats, KOICA has advanced its security governance through organizational, managerial, and technical strategies.

---

## 2. Organizational and Managerial Security Measures

Initially, KOICA's cybersecurity function was embedded within IT operations and focused primarily on incident response. A turning point came in 2018 after a significant web shell attack, leading to the creation of an independent, dedicated cybersecurity department. Key measures included:

- Establishing a dedicated security team independent from IT operations.
- Recruiting specialized staff, including external cybersecurity experts as department heads.
- Launching a Cybersecurity Control Center to monitor threats continuously.
- Providing strong incentives to attract and retain top-level security professionals.

These changes were backed by active engagement from executive leadership, embedding information security into the agency's governance culture.

---

## 3. Cybersecurity Threat Landscape

The number and complexity of cyberattacks against KOICA have increased significantly. In 2024, overall cyberattack attempts rose by 72% compared to 2023. Key findings include:

- **Increased threats**: website hacking attempts, illegal server access, and denial-of-service attacks.
- **Decreased threats**: PC malware infections, phishing emails, and access to malicious sites.

Attack origins were concentrated in the United States, China, India, Singapore, and Germany. These patterns underscore the need for global and proactive defense strategies.

---

## 4. Evaluation of Security Readiness

Since 2017, KOICA has undergone national cybersecurity evaluations conducted by the National Intelligence Service. Its initial score was among the lowest across public institutions. Through continuous investment and systematic improvements, KOICA's score rose to **87.91 in 2024**, ranking first among quasi-governmental organizations. This improvement was based on the **PDCA (Plan-Do-Check-Act) cycle**, ensuring sustainable information security management.

---

## 5. Capacity Building and Awareness

KOICA has emphasized internal capacity building as a cornerstone of security governance. Initiatives include:

- Regular cybersecurity training for executives and staff.
- Simulation exercises for phishing and hacking mail response.
- Security awareness campaigns to improve organizational culture.
- Cloud-based smart work and network separation to reduce risks.

These activities strengthened both individual and organizational resilience against cyber threats.

---

## 6. Technical Security Framework

KOICA developed a customized information security management framework aligned with **ISO 27001 and ISO 27701**. Its approach combined managerial and technical measures, addressing:

- **Infrastructure security**: separation of networks, cloud and server security.
- **Endpoint security**: protection against malware, phishing emails, and unauthorized access.
- **Security operations**: proactive monitoring, vulnerability assessments, and malware analysis.

In 2024, infrastructure-related threats increased by 272%, while endpoint threats decreased by 91%, reflecting the effectiveness of endpoint protection measures but also highlighting persistent infrastructure risks.

---

## 7. AI and Security Governance in the Digital Era

Recognizing the evolving digital landscape, KOICA has begun adopting AI-driven solutions to strengthen governance:

- AI chatbots for external services (e.g., volunteer program inquiries, procurement regulations).
- AI assistants for internal staff (e.g., HR rules, financial reporting, compliance guidance).
- AI tools for document preparation, data analysis, and automated workflows.

These innovations aim to enhance efficiency, reduce cyber risks, and prepare the agency for next-generation security challenges.

---

# 8. Global Cooperation and ODA Projects

KOICA's mission extends beyond national boundaries, engaging in **cybersecurity ODA (Official Development Assistance) projects** across Latin America, Africa, Asia-Pacific, and the Middle East. By sharing Korea's experience in advancing security governance, KOICA supports developing countries in strengthening their resilience against cyber threats. Cooperation with international organizations such as the UN and OECD further enhances its global impact.

---

# 9. Conclusion

The KOICA case illustrates how a quasi-governmental organization can evolve from a reactive cybersecurity posture to a proactive, governance-driven model. Through dedicated organizational structures, executive support, awareness training, international standards adoption, AI-driven innovation, and global partnerships, KOICA has built a resilient cybersecurity governance system. Its experience offers valuable lessons for other public and quasi-public institutions facing similar challenges in the digital era.