Strategy for Promoting a Certification System to Nurture Information Security Professionals

---

1. Introduction

Recent cyber incidents have grown in both scale and severity, causing significant social and economic damage. Large-scale data breaches, in particular, have resulted in not only heavy fines but also serious reputational losses for enterprises. Under these circumstances, information security must no longer be perceived as a cost but rather as a necessary investment.

This report outlines the strategy for promoting a certification system aimed at nurturing information security professionals. It analyzes the current situation and challenges, introduces new certification schemes, and presents directions for their implementation and improvement.

---

2. Severity of Cyber Incidents

2.1 Major Cases

- **KT**: 2012 customer management system breach (8.7M users), 2013 website breach (12M users), fine of KRW 700M.
- **LGU+**: 2014 customer authentication system breach (300K users), fine of KRW 6.8B.
- **SKT**: 2025 core network server breach (27M users), fine of KRW 134.8B.

2.2 Implications

Fines escalated rapidly from KRW 700M to 134.8B, showing how organizational negligence in security management has been factored into severity assessments. This highlights the urgent need for systemic management and professional expertise.

---

3. Status and Supply Issues of Information Security Workforce

3.1 Workforce Status

As of 2023, approximately 50,000 information security professionals were active, with **management roles** accounting for 89.3%. By contrast, incident analysis/response (2.5%) and assessment/diagnostics (2.3%) remain critically understaffed.

Across all cybersecurity roles (approx. 79,500 professionals), management also dominates (71.5%), while technical specializations are in short supply.

3.2 Recruitment Trends

Only 7.6% of organizations hired cybersecurity staff in the past year. Looking ahead, just 33.2% have concrete plans to recruit within the next year, indicating a widening gap in workforce supply.

---

4. Problems and Needs

1. **Lack of proactive threat recognition**: Executives and employees demonstrate limited awareness of information security.
2. **Absence of governance systems**: Strategic threat analysis and systematic access control are insufficient.
3. **Shortage of specialized staff**: Many roles are filled by part-time managers, undermining responsibility and expertise.

Therefore, building organizational governance, securing specialized talent, and expanding budgetary investment are critical.

---

5. Introduction of New Certifications

5.1 Information Security Risk Manager (ISRM)

- **Purpose**: Validate ability to protect assets, operate security management systems, and conduct risk management.
- **Exam**: Written, 5 subjects, 80 questions, 90 minutes. Passing requires ≥40 points per subject and ≥60 overall.
- **Subjects**: Risk management planning, risk assessment, risk response, management system operation (advanced), threat countermeasure management (advanced).
- **Fee**: KRW 100,000.

5.2 Test of Literacy in Information Security (TOLIS)

- **Purpose**: Evaluate basic literacy and foundational knowledge in information security.
- **Exam**: Written, 5 subjects, 90 questions, 90 minutes. Scores assigned to five certification levels.
- **Subjects**: Security overview, security technologies, industry trends, incident prevention/response, ethics.
- **Fee**: KRW 50,000.

---

6. Current Certification Operations

- **Regular Exams**: Three sessions per year, held nationwide (CBT-based).
- **Special Exams**: Conducted upon request from groups of 20+ candidates (iBT-based).
- **Support Measures**: Fee discounts, sample questions, and free candidate guidebooks.

- **First-year Performance (2025)**:
  - Total candidates: ~1,400 (ISRM: 1,209 / TOLIS: 232).
  - ISRM passers: 673 (pass rate 55.7%).
  - TOLIS: Majority awarded Level 2 (72.7%).

---

7. Candidate Feedback

7.1 Candidate Profile

- 82.5% of examinees were employed professionals, with the majority working in the information security field.

7.2 Satisfaction

- Overall satisfaction with new certifications: 64.8% positive.

7.3 Opinions

- **Positive**: Convenience of iBT/CBT testing, helpfulness in ISMS-P preparation, contribution to professional practice, and hopes for national accreditation.
- **Neutral**: Difficulties for those lacking hands-on experience.
- **Critical**: Need for higher difficulty, clearer utilization pathways, mobile certification integration, and more meaningful scoring for TOLIS.

---

8. Improvement Directions

1. **Relax ISRM eligibility**: Open to all candidates regardless of academic/experience background.
2. **Restructure TOLIS**: Replace tiered certification with a score-based system.
3. **Raise exam difficulty**: On-site advanced ISRM subjects; greater focus on practical content in TOLIS.
4. **Digital certification**: Mobile certificates via Naver.
5. **New training programs**: Online ISRM courses launched in cooperation with KISIA.

---

9. Conclusion

As cyber threats evolve in scale and complexity, fostering skilled information security professionals has become a national priority. The new certification system is designed not only to test theoretical knowledge but also to validate practical competencies.

Through continuous improvements and broader adoption, ISRM and TOLIS can become key instruments for producing qualified professionals, strengthening the cybersecurity industry, and elevating national resilience against cyber risks.