# Analysis of a Cybersecurity Training Curriculum for Nuclear Facilities and Suggestions for Improvement*

Sooyon Seo[1], Dongmin Kim[1], Damin Kim[1], Jae-Jun Han[2], Junghyun Na[2], Hyun-Kyung Lee[2], Aram Kim[3]†, and Moohong Min[1]

[1] Sungkyunkwan University, Seoul, Republic of Korea
{sooyon1119, ehdals5744, goat0129, iceo}@skku.edu
[2] Korea Institute of Nuclear Nonproliferation and Control, Daejeon, Republic of Korea
{jjhan, njh777, hklee}@ kinac.re.kr
[3] University of Suwon, Gyeonggi-do, Republic of Korea
aramkim@suwon.ac.kr

**Abstract**

Cyberattacks against nuclear facilities pose serious risks, as they can disrupt both information integrity and essential protective functions, leading to severe national security consequences. International standards emphasize continuous, practice-based training; however, earlier study contributed by developing a survey to assess course usefulness and satisfaction, it did not extend to an in-depth analysis of curriculum design. To address this gap, this study applies Stufflebeam's Context, Input, Process, Product (CIPP) framework to an international training course and designs a longitudinal survey covering four stages: pre-course, post-eLearning, post-training, and a 3-month post-training. The approach combines structured curriculum analysis with participant-focused evaluation to examine course organization, difficulty levels, and training outcomes. Results show that practical exercises account for a larger share of the program (55.1%) than lectures (44.9%), the training integrates both attack and defense perspectives, and it is most suitable for practitioners with 2–5 years of experience, offering an advantage over general awareness programs. The proposed survey further captures long-term effects such as knowledge retention and workplace applicability, establishing a foundation for continuous improvement of nuclear cybersecurity education.

**Keywords**: Cybersecurity Training, Nuclear Nonproliferation and Security, International Training Course, Course Design Analysis

## 1 Introduction

In accordance with the U.S. Nuclear Regulatory Commission (NRC) regulations[27] that mandate the design of systems to prevent the theft or diversion of nuclear materials, nuclear facilities have established sophisticated Physical Protection Systems (PPS) to prepare against acts of sabotage. PPS traditionally consists of access control, surveillance, and alarm systems to meet these requirements, but in recent years, their operation has become increasingly dependent on digital technologies[18] such as Closed-Circuit TeleVision (CCTV) and Intrusion Detection and Prevention Systems (IDS/IPS). While this digitalization enhances operational efficiency, it also introduces several cybersecurity vulnerabilities that can compromise or disable core physical protection functions.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 14, December 16-18, 2025, Sapporo , Japan. 
†Corresponding Authors

Incidents in the nuclear sector illustrate the severity of these risks. In 2008, the Hatch nuclear power plant experienced an unplanned shutdown of the reactor when a software update in the business network inadvertently propagated into the control network, directly affecting the reactor control system[6]. And in 2014, Korea Hydro & Nuclear Power (KHNP) suffered a cyber intrusion into its business network that resulted in the leakage of reactor blueprints and other sensitive documents[17]. These cases demonstrate that nuclear facilities are exposed to cyberattacks through both control and business networks, and that such attacks may undermine not only information confidentiality but also operational reliability. Consequently, PPS based on digital devices is equally susceptible, underscoring the need for an integrated perspective that links physical security and cybersecurity.

Achieving such integration requires cross-domain understanding and systematic training. Physical security personnel must recognize that digital-based devices such as access control units and alarm networks are increasingly exposed to cyber threats, requiring at least a foundational level of cybersecurity competence. Conversely, cybersecurity specialists must understand the unique operational characteristics of Industrial Control Systems (ICS), including their operation in environments separated from external networks (air-gapped), to design effective defense strategies. Since training must ensure the capability to respond effectively to real-world situations[26], it must move beyond simple knowledge transfer to incorporate scenario-based, hands-on exercises. International standards and regulatory guidance emphasize this necessity. For example, International Atomic Energy Agency Nuclear Security Series (IAEA NSS) 42-G[1] calls for continuous workforce capacity building through regular training; National Institute of Standards and Technology Special Publications (NIST SP) 800-16[26] highlights role-based, task-specific training; and NRC Regulatory Guide (RG) 5.71[28] recommends the establishment of feedback-driven mechanisms to ensure sustainable programmatic improvement. Collectively, these frameworks highlight that nuclear facilities require cybersecurity education that is systematic, based on realistic practice, and continuously improved.

While a prior study on the International Nuclear Nonproliferation and Security Academy International Training Course (INSA ITC)[20] contributed by developing a survey to assess course usefulness and satisfaction, it did not extend to an in-depth analysis of curriculum design, such as its structure, inter-module connectivity, or difficulty distribution. Building upon this gap, the present study analyzes the ITC operated by the Korea Institute of Nuclear Nonproliferation and Control (KINAC), the Korean governmental organization responsible for nuclear nonproliferation, safeguards, and nuclear security capacity building, to examine its curriculum design, assessing its effectiveness, and identifying opportunities for enhancement.

For this purpose, the study employs Stufflebeam's Context, Input, Process, Product(CIPP) evaluation model[23] as the analytical framework to examine the appropriateness and effectiveness of the curriculum from multiple perspectives. In addition, a longitudinal survey covering pre-training, post-e-learning, immediate post-training, and three-month follow-up was designed to evaluate participant expectations, satisfaction, and knowledge retention comprehensively. The contributions of this study are as below:

- It provides a systematic analysis of PPS-oriented cybersecurity training within the KINAC ITC program.
- It proposes an evaluation framework that incorporates participant perspectives.
- It identifies directions for improving the future development of nuclear cybersecurity education.

The remainder of this paper is organized as follows. Section 2 introduces the KINAC ITC program and relevant international training cases. Section 3 describes the research design

and methodology, including the CIPP framework and survey design. Section 4 presents the curriculum analysis results, while Section 5 outlines the survey structure and item composition. Section 6 discusses key implications and outlines directions for future work, and Section 7 concludes the paper.

# 2 Context & Related Works

## 2.1 KINAC International Training Course (ITC) Program Overview and Objectives

The International Nuclear Security Academy (INSA) was established on February 19, 2014, following South Korea's commitment at the 2010 Washington Nuclear Security Summit to establish a Center of Excellence for nuclear security[15]. INSA began its first international training course in March 2014, with objectives to provide nuclear nonproliferation and security education and support nuclear newcomer countries in developing regulatory frameworks.

The International Training Course (ITC) structure covers three core areas: Nuclear Security, Safeguards, and Strategic Trade Controls[19]. The program has expanded from three annual courses during 2014-2016 to six courses annually from 2017 onwards. By 2024, INSA had conducted 35 International Training Courses with 604 participants from 28 countries.

INSA follows a four-stage development process: material development with US national laboratories, train-the-trainer workshops, dry-run sessions, and course implementation. Course capacity is limited to 2-3 participants per country with a maximum of 30 participants, selected through official government nomination channels.

The Nuclear Security curriculum focuses primarily on Physical Protection Systems (PPS), including basic infrastructure development and advanced courses on Physical Protection System Elements, Security Contingency Planning, and facility cybersecurity[16]. The PPS training combines lectures with practical exercises using security equipment such as intrusion detection sensors, access control systems, and alarm management technologies.

The educational infrastructure centers on the Nuclear Security Research, Training and Test Facility (SETT), occupying 44,329 square meters with a five-story main building. The facility includes classrooms, laboratories, and security training equipment for hands-on PPS education with various detection systems and access controls in operational settings[22].

## 2.2 Related Training Programs & Case Studies

This section examines existing cybersecurity education programs targeting nuclear facilities and industrial control systems to identify effective training approaches, methodologies, and evaluation frameworks. The analysis is structured to investigate four key aspects: specialized nuclear facility programs (2.2.1), broader industrial control system training cases (2.2.2), education improvement models and their effectiveness evaluation methods (2.2.3), and common success factors with identified limitations (2.2.4). This comparative analysis aims to establish best practices and identify gaps in current cybersecurity education approaches for nuclear facilities.

### 2.2.1 IAEA Nuclear Facility Cybersecurity Training Programs

The IAEA has operated specialized International Training Courses for nuclear facility cybersecurity since 2018, developed in collaboration with the U.S. Department of Energy's National Nuclear

Security Administration and Idaho National Laboratory [11]. The training methodology emphasizes adversarial thinking through practical scenario-based exercises where participants experience cyber attacks from an attacker's perspective using models of digital systems representing nuclear facility environments [12].

The program utilizes virtualized training environments where adversaries take control of physical protection systems at simulated nuclear facilities and deploy malware, enabling participants to understand attack vectors and defense mechanisms. In 2023, IAEA enhanced this approach by launching the 'Learners' virtual training platform, which provides realistic facility representations with twelve practical exercises organized into six thematic areas based on IAEA nuclear security guidance [13]. The platform demonstrates scalability by serving over 120 countries and supports customized capacity-building activities tailored to specific national contexts and regulatory frameworks.

### 2.2.2 Industrial Control System Cybersecurity Training Approaches

EC-Council, a cybersecurity certification organization, has developed comprehensive ICS/SCADA cybersecurity training programs specifically addressing advanced persistent threats targeting industrial operational technology, including sophisticated malware such as Triton/TRISIS and Stuxnet [8]. Their curriculum emphasizes practical security architecture understanding through adversarial simulation methodologies, training participants to identify vulnerabilities by adopting attacker perspectives and understanding exploit techniques [9].

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides globally accessible ICS cybersecurity training designed for critical infrastructure protection, offering both web-based learning modules and instructor-led intensive workshops [7]. The SANS Institute's ICS410 course distinguishes itself through hands-on training with actual programmable logic controller (PLC) devices, enabling participants to directly explore cyber-physical interfaces and understand the operational technology environment that characterizes nuclear facilities [21].

Idaho National Laboratory implements a comprehensive team-based training model featuring 7-hour intensive sessions where participants are divided into Red Teams (attackers) and Blue Teams (defenders) to conduct realistic attack and defense scenarios across both IT and operational technology (OT) networks [10]. The program incorporates innovative gamification elements, including escape room puzzles focused on ICS cybersecurity challenges that test participants' teamwork, communication skills, and technical problem-solving capabilities under time pressure, simulating real-world incident response conditions.

### 2.2.3 Education Improvement Models and Effectiveness Evaluation

The 2024 iCAT model proposes an integrated approach using knowledge graphs, serious games, and gamification with micro-learning modules for flexibility and real-time progress monitoring [5]. The CAT framework for remote work environments consists of three levels (awareness, training, practice/evaluation) with 25 core practices to identify organizational weaknesses and measure employee capabilities [2].

A systematic review of 142 studies found positive training effects regardless of cybersecurity topics or methods used, with game-based approaches being most common [29]. Effective cybersecurity awareness programs require continuous processes converting knowledge into practice, measured through participant engagement, incident reduction, and behavioral changes [3]. Key evaluation indicators include post-training assessments, behavioral pattern analysis for threat prediction, and communication effectiveness during security incidents [4].

#### 2.2.4 Success Factors & Limitations

Successful programs share common elements: practical scenario-based exercises [11, 21, 10], regular content updates for evolving threats [13, 4], customized approaches for organizational characteristics [2], and measurable evaluation indicators [3, 4].

Research limitations include small sample sizes, testing on non-employee groups, and focus on short-term effects [29]. Research consistently concludes that special environments like nuclear facilities require customized approaches considering safety regulations, ICS/SCADA systems, and physical-cyber connectivity rather than generic cybersecurity education models [11, 13, 14].

# 3 Research Design & Methodology

## 3.1 Curriculum Analysis Framework

The purpose of analyzing the KINAC ITC curriculum is to examine whether this cybersecurity training program for nuclear facilities sufficiently reflects international regulatory requirements (e.g., IAEA NSS 42-G, NIST SP 800-16, NRC RG 5.71) as well as the practical operational contexts of ICS/SCADA-based environments. To this end, the analysis systematically considers the curriculum's objectives, content, delivery methods, and evaluation system, with particular attention to how these elements incorporate the unique operational characteristics of nuclear facility ICS/SCADA systems. The ultimate aim is to identify potential shortcomings in the program and establish a basis for proposing improvements and enhancements.

For this purpose, this study adopts Stufflebeam's (1971) CIPP (Context, Input, Process, Product) evaluation model as the analytical framework [23]. The CIPP evaluation model is a comprehensive framework widely applied across education, organizations, and programs to support both formative and summative evaluations, and it is structured around four key domains. Context evaluation addresses the guiding question "What needs to be done?" by identifying needs, problems, resources, and opportunities to help establish goals and priorities. Input evaluation asks "How should it be done?" and assesses alternative strategies, implementation plans, and resource allocations to determine feasibility and cost-effectiveness. Process evaluation corresponds to "Is it being done?" by examining whether the program is being implemented as intended. Product evaluation poses the question "Did it succeed?" and measures both short- and long-term outcomes of the program [25].

Stufflebeam emphasized that "the purpose of evaluation is not to prove, but to improve," highlighting the CIPP evaluation model's focus on continuous program enhancement [24]. From this perspective, the CIPP evaluation model goes beyond verifying outcomes and offers particular strengths in deriving the appropriateness of a program and identifying areas for improvement. While recent models such as iCAT and CAT emphasize gamification, micro-learning, or remote-work contexts, they are less suitable for comprehensive curriculum evaluation. In contrast, the CIPP model enables a structured and holistic analysis of training programs, which aligns more closely with the objective of this study to examine the appropriateness and effectiveness of the KINAC ITC program. Accordingly, the CIPP evaluation model is regarded as particularly suitable for analyzing the KINAC ITC curriculum, which not only requires specialized domain knowledge but also aims to ensure the practical applicability of its content in real-world settings. Guided by the four domains of the CIPP evaluation model, this study derived specific evaluation questions to analyze the KINAC ITC curriculum:

- **Context**: Do the curriculum objectives align with international regulatory requirements

and the security needs of nuclear facilities?

- **Input**: Are the curriculum contents and resources designed to reflect the technical and organizational challenges of ICS/SCADA systems?
- **Process**: Are delivery methods (lectures, hands-on exercises, simulations) implemented in ways that realistically mirror operational practices and attacker–defender perspectives?
- **Product**: Does the evaluation system capture both short-term learning outcomes and long-term workplace applicability?

These questions are addressed in Section 4 through detailed curriculum analysis, and in Section 5 through a learner-centered survey design. This ensures that both regulatory compliance and operational applicability are systematically examined.

### 3.2 Survey Design and Target Group

In addition to a systematic analysis of the curriculum's structure and operation, incorporating the experiences of actual participants is essential to evaluate the effectiveness of the program from multiple perspectives. To this end, this study designed a survey targeting learners who had completed the KINAC ITC program, thereby complementing the curriculum analysis with learner-centered feedback on their perceptions and outcomes.

The survey was structured to track changes at four points in time: pre-training, post-eLearning, post-training, and 3-month post-training. This design enabled the assessment not only of short-term reactions but also of longer-term effects, such as whether the knowledge and skills gained were effectively applied in the workplace. By repeatedly surveying the same group, the study could identify gaps between learners' initial expectations and their subsequent achievements.

The primary purpose of the survey was not limited to measuring satisfaction but extended to evaluating learners' changes in understanding and perceptions, the extent of achievement of learning objectives, assessments of instructional methods, and applicability to professional practice. Through this, the study sought to capture a learner-centered perspective that cannot be obtained solely through curriculum analysis, and to determine how well the KINAC ITC program meets the knowledge and competency requirements of real-world contexts.

## 4 KINAC ITC Analysis

### 4.1 Overall Course Overview and Structure Analysis

The International Training Course (ITC) on Nuclear Security Cybersecurity is designed to enhance the cybersecurity capabilities of Physical Protection Systems (PPS) personnel in nuclear facilities. The program aims to provide comprehensive understanding of cyber threats targeting nuclear security systems and develop practical skills for implementing effective defense strategies. Targeting PPS personnel responsible for nuclear facility security operations, the course is structured as an intensive 5-day program that integrates theoretical knowledge with hands-on practical experience.

The program consists of 16 theoretical modules and 6 practical exercises, totaling approximately 28 hours of instruction. The curriculum emphasizes hands-on learning, with 12.5 hours (44.9%) dedicated to theoretical content and 15 hours and 20 minutes (55.1%)

to practical exercises. To support this practical focus, participants are required to complete eLearning courses before attending the in-person training sessions.

The program utilizes specialized training facilities including Security Education, Training and Testing facility (SETT) and Physical Protection System Training Equipment (PPSTE) equipped at KINAC/INSA. These facilities provide realistic training environments that simulate actual nuclear facility security systems, enabling participants to gain hands-on experience with equipment and scenarios they will encounter in their operational roles.

The curriculum follows a carefully structured 5-stage progression that builds knowledge and skills systematically:

- **Stage 1** introduces the program and establishes the importance of cybersecurity in nuclear facility protection
- **Stage 2** explores digital technologies integrated within PPS and provides facility tours to observe systems in operational settings
- **Stage 3** teaches vulnerability analysis and threat assessment methodologies, reinforced through hands-on equipment training
- **Stage 4** provides direct experience with cyber attack scenarios and introduces industry-standard security frameworks
- **Stage 5** focuses on designing comprehensive defense strategies and consolidating learning through group discussions and case studies

This systematic approach ensures participants develop both theoretical understanding and practical skills, while gaining experience from both attacker and defender perspectives, which is essential for effective cybersecurity professionals in nuclear facilities.

## 4.2 Analysis of Module and Exercise Composition

The curriculum content can be organized into five main subject areas. Table 1 and Figure 1 break down the curriculum by topic, showing module assignments, time distribution, and key content areas.

Table 1: Curriculum Structure Breakdown

| **Topic Category** | **Related Modules** | **Training Time** | **Key Features** |
|---|---|---|---|
| Cybersecurity Fundamentals | M1, M2, M4, M6 | 3h 30m | Basic security concepts, threat types |
| PPS Digital Technology | M3, M5, M7, M8, E1, E2, E3 | 8h 50m | System architecture, networking, tools |
| Vulnerability and Threat Analysis | M9, M10, E4, E5 | 9h 30m | Risk assessment, attack simulation |
| Security Framework | M11, M12, M13, M14, M15 | 3h 30m | Industry standards and best practices |
| Course Summary | E6, M16 | 2h 30m | Knowledge integration and review |

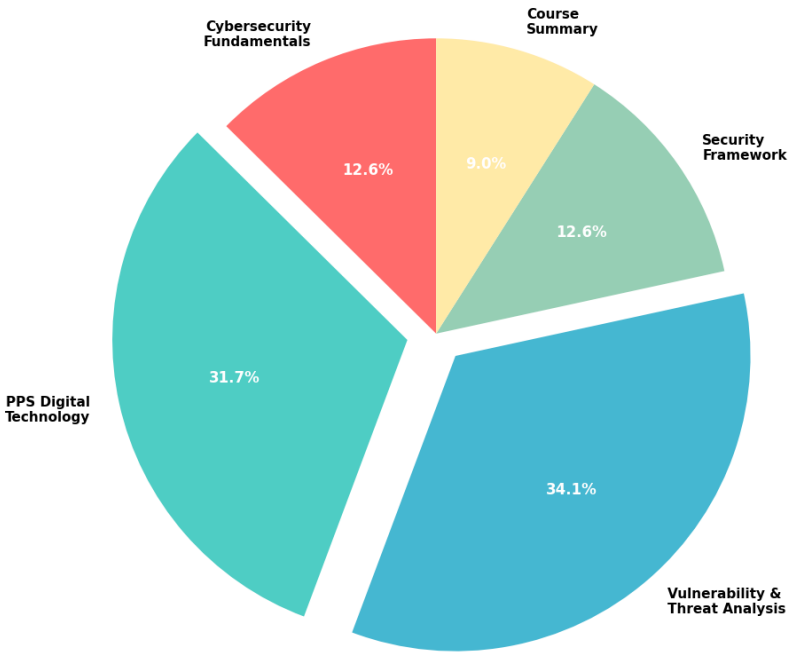


Figure 1: Topic-wise Allocation of Course Hours

Cybersecurity Fundamentals (12.6%) establishes the foundation by covering essential security concepts tailored to nuclear facility environments. This section introduces specialized concepts like blended attacks (combining physical and cyber elements), the CIA triad (Confidentiality, Integrity, Availability), and Design Basis Threats (DBT)—the standardized threat scenarios used in nuclear security planning. The content uses realistic scenarios from the SNRI— a hypothetical nuclear facility used in a training scenario— to make abstract concepts concrete and relevant. However, coverage of current cyber threats such as ransomware and advanced persistent threats remains limited.

PPS Digital Technology, one of the main topics (31.7%), reflects the program's specialized focus on physical protection systems. This section explains how modern security systems work, covering everything from individual devices (sensors, cameras) to network controllers and central management systems. Participants learn fundamental networking concepts including the OSI model and TCP/IP protocols, and gain practical experience with network analysis tools like Wireshark. The hands-on components include tours of simulated security facilities and extensive training with PPSTE equipment, providing real-world context for subsequent vulnerability analysis training.

Vulnerability and Threat Analysis commands the highest proportion (34.1%) and represents the core of the program's practical objectives. This section teaches participants how to identify and assess security weaknesses, covering common vulnerability sources such as design flaws, system misuse, human error, and supply chain compromises. Rather than abstract discussions, the curriculum uses specific examples from actual security equipment (such as WiFi security cameras and network switches) to demonstrate real vulnerabilities. The practical exercises use the previously introduced PPSTE equipment to simulate cyber attacks on physical

security systems, followed by development of appropriate countermeasures. This substantial time allocation reflects the program's primary goal of developing practical threat assessment capabilities.

Security Framework (12.6%) introduces the NIST Cybersecurity Framework, an internationally recognized standard for organizing and managing cybersecurity programs. While this provides important context for professional cybersecurity practice, the relatively modest time allocation may require expansion depending on participants' existing knowledge of security management frameworks.

Course Summary (9%) goes beyond simple review, incorporating structured reflection and collaborative learning activities. Group discussions and presentations help participants consolidate their understanding, identify knowledge gaps, and learn from peers' experiences. This collaborative approach often reveals insights that individual study cannot provide.

## 4.3 Inter-module Connectivity and Learning Path Analysis

The KINAC ITC curriculum is characterized by a sequential structure that systematically links theoretical modules and practical exercises. The learning path begins with fundamental concepts and progresses through applied practice to integrative discussion, as illustrated in Figure 2.

The initial modules (M1, M2, M4, M6) introduce core concepts of cybersecurity and PPS, providing a basis for subsequent in-depth learning. The following modules (M3, M5, M7, M8) focus on digital technologies in PPS and are directly connected to facility tours and equipment operation exercises (E1, E2, E3), bridging theory and practice. Mid-stage modules (M9, M10) focus on vulnerability analysis and asset management, extending into offensive and defensive exercises (E4, E5) using PPSTE equipment. This sequence allows participants to experience both attacker and defender perspectives. The later modules (M11, M12, M13, M14, M15) address the NIST Cybersecurity Framework and supply chain security, leading into a group discussion exercise (E6) and a final summary module (M16). Through this sequence, the curriculum broadens the scope of learning from technical understanding to policy and governance.

The learning process moves from theory to equipment interaction and then to security frameworks. Outcomes of practical exercises are designed to support later modules, reinforcing retention and applicability. The structure aligns with international standards that emphasize practical, role-specific, and continuous training. In summary, the integrated structure of theory and practice enhances learner comprehension and strengthens applicability to operational contexts.

Nevertheless, aspect for improvement remains. As shown in Table 1, later modules addressing frameworks and verification are allocated 3 hours and 30 minutes, significantly less than the introductory and digital technology modules. Furthermore, these later modules are associated with only a single group discussion exercise (E6), whereas the earlier modules are linked to multiple, equipment-based exercises (E1-E5). Therefore, incorporating some simulations or additional exercise components into the latter stages could improve the effectiveness of learning in policy-related domains.

## 4.4 Difficulty Distribution and Learning Load Analysis

Figure 3 shows how difficulty levels are distributed throughout the curriculum. Difficulty levels were determined based on three key factors: (i) conceptual complexity of the module, (ii) technical skill requirements for hands-on equipment use, and (iii) prerequisite knowledge of

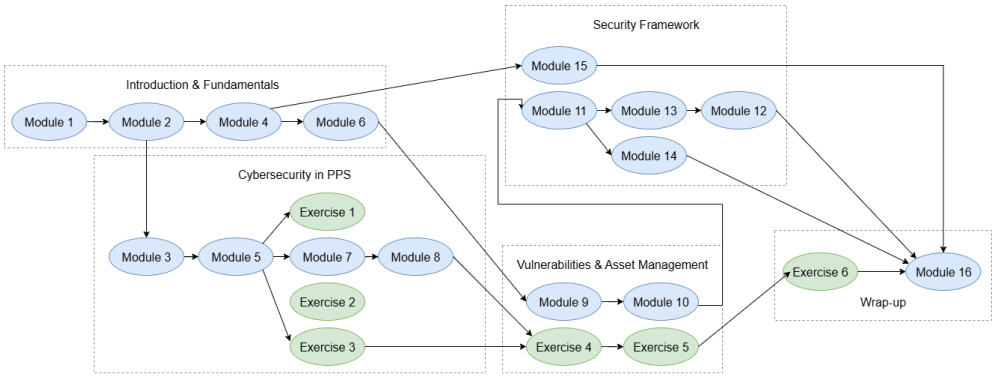


Figure 2: Overall Course Structure and Learning Flow

PPS/ICS systems. Using these factors, three explicit difficulty categories were defined to reduce subjectivity: low difficulty refers to modules focused on basic conceptual lectures or introductory demonstrations without learner interaction; medium difficulty includes lectures that address the same topics in greater depth or practical sessions involving guided discussion and problem-solving; and high difficulty corresponds to advanced conceptual content or exercises requiring independent use of actual equipment to address realistic problems.

Analysis of the components reveals a balanced distribution: low difficulty accounts for 32% (7 components), medium difficulty represents the highest proportion at 45% (10 components), and high difficulty comprises 23% (5 components). This distribution appears well-structured, with medium-level content dominating and challenging advanced content maintained at a reasonable proportion.

However, a closer examination of the practical exercises reveals a concerning pattern. While the overall curriculum maintains balanced difficulty progression, half of the six exercises (E3, E4, E5) are classified as high difficulty. More problematic is the abrupt difficulty transition within the exercise sequence: the initial exercises consist of simple facility tours and equipment introductions (E1, E2), but suddenly jump to advanced-level hands-on operation starting with Exercise 3. This steep learning curve may challenge participants, particularly those with limited practical experience, as they transition from observational activities to complex equipment manipulation without intermediate stepping stones.

Table 2 shows how well the current curriculum serves different experience levels. The mapping was developed by aligning the difficulty distribution of modules and exercises with three typical participant groups, newcomers (less than 2 years of experience), intermediate practitioners (2–5 years), and experienced professionals (5+ years). This approach enabled us to evaluate program suitability for each group and to identify where adjustments, such as prerequisite modules for beginners or advanced specialization tracks for experts, may be beneficial. This mapping was based on expert judgment derived from the earlier difficulty classification. While it provides a useful approximation of suitability by experience level, future empirical validation using learner performance data would strengthen its reliability. The balanced difficulty distribution with medium-level content as the majority makes the program well-suited for intermediate practitioners (2-5 years experience). However, the abrupt difficulty transitions in practical exercises may pose challenges for beginners, while the limited advanced theoretical content may not fully satisfy experts seeking deeper specialization. Accordingly, Table 2 should be interpreted as a preliminary framework rather than a definitive measure.

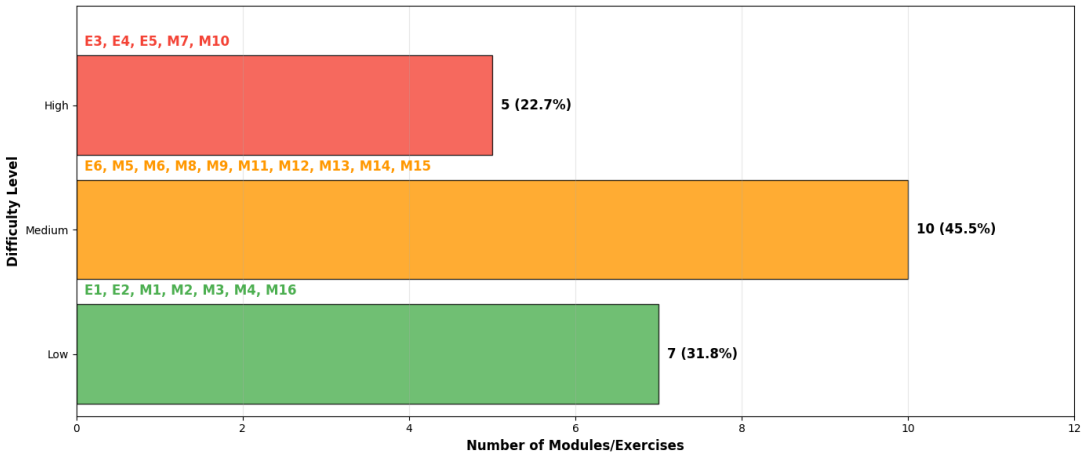


Figure 3: Curriculum Difficulty Distribution

Incorporating actual participant performance and feedback in future studies will enable more objective validation of difficulty classification and audience suitability.

Table 2: Suitability Assessment by Target Audience

| **Target Audience** | **Experience Level** | **Current Suitability** | **Recommended Adjustments** |
|---|---|---|---|
| Newcomers | 2 years | Partially suitable | Add more foundational content, provide optional prerequisites |
| Intermediate practitioners | 2-5 years | Highly suitable | Current design works well |
| Experienced professionals | 5 years | Partially suitable | Allow basic module exemptions, add advanced specialization tracks |

## 4.5 Core Strengths and Enhancement Opportunities

The program's greatest strength lies in its exceptional training infrastructure. SETT provides a full-scale physical protection facility with four operational sectors, complete with integrated access control, surveillance, intrusion detection, and screening systems. This authentic environment allows participants to see how cybersecurity principles apply in real nuclear facility operations. PPSTE complements this with production-quality equipment for surveillance (CCTV systems), access control (biometric systems), and sensor networks (industrial control systems), enabling comprehensive hands-on training.

The curriculum achieves an effective balance between theory and practice, successfully developing skills that transfer to actual work environments. The variety of practical approaches—facility tours, equipment operation, simulated attacks, defense planning, and group discussions—accommodates different learning styles and reinforces knowledge through multiple channels. Particularly valuable is the pairing of attack simulation (Exercise 4) with

defense design (Exercise 5), which provides participants with comprehensive understanding from both offensive and defensive cybersecurity perspectives.

The program's integration of current industry standards, specifically NIST Cybersecurity Framework 2.0, ensures participants learn approaches that align with international best practices. The specialized focus on PPS environments—including unique concepts like blended attacks and Design Basis Threats—effectively addresses the specific cybersecurity challenges of nuclear facilities, distinguishing it from generic cybersecurity training.

Enhancement Opportunities for future development include several promising directions:

- Customization for diverse audiences: Developing prerequisite modules for beginners and advanced tracks for experts would improve accessibility and effectiveness across experience levels.
- Continuous professional development: Post-course programs including regular updates, advanced certifications, and peer networking opportunities would sustain long-term capability development.
- Broader technical coverage: Optional modules covering additional industrial control protocols and specialized security technologies would provide pathways for deeper specialization.

These enhancements would build upon the program's solid foundation while better serving the evolving needs of nuclear facility cybersecurity professionals.

# 5 Survey Design

In this study, questionnaires were developed for four time points, pre-training, immediately after eLearning completion, immediately after main training completion, and three months post-training, to systematically validate the effectiveness of KINAC ITC training from the participants' perspective. The questionnaires were designed to comprehensively examine various aspects including trainees' backgrounds, learning experiences, post-training satisfaction and achievement levels, and actual workplace application.

## 5.1 Purpose

The purpose of the survey extends beyond simple satisfaction assessment to collect comprehensive feedback on learners' understanding and perception changes, educational objective achievement, practical applicability, delivery methods, and evaluation systems, thereby establishing a foundation for multifaceted evaluation of KINAC ITC training appropriateness and effectiveness. Particularly, the design includes a three-month post-training survey to assess the sustainability of training effects. Through this approach, the study aims to establish foundational data for verifying how effectively the KINAC ITC training program provides the knowledge and competencies required in actual field settings.

## 5.2 Targets

The questionnaires were designed for participants who actually completed the KINAC ITC training program. The design enables longitudinal evaluation of the same cohort from pre-training through eLearning, immediately post-main training, and three months post-training, allowing assessment not only of short-term reactions to training but also sustained

effects over time. This tracking structure provides evidence for evaluating not just satisfaction or understanding changes, but also actual workplace application experiences and long-term effects.

## 5.3 Design Principles

Survey items were constructed to be concise to ensure respondents could easily understand and answer without burden. Neutrality of expression was maintained and careful attention was paid to item arrangement and phrasing to minimize response bias. Additionally, a combination of multiple-choice and open-ended questions was employed to secure both quantitative and qualitative data. Multiple-choice items included yes/no selections, 5-point Likert scales, and multiple-response checklists to quantify training effects, while open-ended items utilized free description or numerical input formats to reflect respondents' specific opinions and experiences. These design principles aim to secure instrumental validity for multidimensional assessment of training effects.

## 5.4 Survey Item Composition

The questionnaires were designed to address differentiated themes appropriate to educational objectives and circumstances at each time point. Within this differentiated structure, all four time-point surveys commonly included repeated "Perception and Need Recognition" items to enable longitudinal tracking of changes in identical items. This structure enables longitudinal verification of training effects beyond simple satisfaction dimensions. Specific survey items for each time point are included in Appendix A.

### 5.4.1 Pre-training

The pre-training survey consisted of 16 items total, with 9 multiple-choice and 7 open-ended questions. Given its administration before training commenced, the number of items was kept relatively low to minimize respondent burden, focusing on relatively light topics including existing cybersecurity knowledge levels, PPS-related perceptions, and expected training elements. This established benchmarks for diagnosing learner backgrounds and needs while enabling comparison with subsequent time points.

### 5.4.2 Post-eLearning

The immediate post-eLearning survey consisted of 25 items total, with 17 multiple-choice and 8 open-ended questions. Its primary purpose was analyzing eLearning stage quality and delivery effectiveness. Specifically, it was designed to evaluate understanding and interest changes through online preliminary learning, content difficulty and practical applicability. Additionally, it confirmed satisfaction with the eLearning process and recorded expectations for the subsequent main training stage, identical to the pre-training survey, to examine educational continuity.

### 5.4.3 Post-training

The immediate post-main training survey consisted of 38 items total, with 26 multiple-choice and 12 open-ended questions, containing the most items among all surveys. This utilizes the time point when learners possess the most memories and opinions immediately after training completion. However, to avoid excessive response burden, multiple items were

designed as 5-point Likert scales for quick and intuitive responses. Main content included overall training satisfaction, training operation appropriateness, and educational objective achievement, incorporating scenario-based items to assess actual situation response capabilities. Additionally, perception and necessity items addressed in pre-training and immediate post-eLearning surveys were repeatedly placed to confirm pre- and post-training changes, and items recording training benefits were included to assess how well learners' pre-training expectations aligned with actual achievements.

#### 5.4.4 3-month post-training

The three-month post-training survey consisted of 25 items total, with 16 multiple-choice and 9 open-ended questions. It examined whether expected training elements actually helped in work situations while addressing learning effect sustainability, workplace application experiences, and additional training needs, enabling verification of training outcomes beyond short-term levels to long-term effects.

# 6 Discussion

## 6.1 Implication

This study analyzed the KINAC ITC using the CIPP evaluation model, thereby establishing a foundation for systematic evaluation of cybersecurity training programs. The contribution lies not only in examining the content of the curriculum but also in comprehensively reviewing its structure, delivery methods, difficulty distribution, and overall effectiveness.

In addition, a survey instrument was developed to evaluate expectations, satisfaction, and applicability of training. When implemented in practice, it could generate both quantitative and qualitative data that provide actionable evidence for curriculum improvement.

In summary, the study tried a multifaceted evaluation of the KINAC ITC by combining curriculum analysis with survey development. This dual approach establishes a basis for systematic assessment and continuous enhancement of cybersecurity training for nuclear facilities.

## 6.2 Future Work

Future study would empirically validate the proposed analytical and evaluative framework by administering the survey to participants during actual ITC sessions. As the survey results may be biased toward participants' subjective perceptions, it will be necessary to complement them with performance-based evaluation tools that directly measure learning outcomes.

While this study focused on cybersecurity training for PPS, the same analytical framework could be extended to other ITC programs operated by KINAC, including those on Nuclear Security, Safeguards, and Strategic Trade Controls. Finally, future study will investigate the training needs and perceptions of practitioners in the field through our proposed survey instrument, ensuring that educational programs are closely aligned with operational demands.

# 7 Conclusion

This study applied Stufflebeam's Context, Input, Process, and Product (CIPP) evaluation model to analyze the KINAC International Training Course (ITC) on cybersecurity for Physical

Protection Systems (PPS) in nuclear facilities. In addition, a longitudinal survey instrument was designed to assess participant expectations, satisfaction, knowledge retention, and workplace applicability across four stages: pre-training, post-eLearning, immediate post-training, and three-month follow-up.

The analysis revealed that the KINAC ITC distinguishes itself from lecture-oriented programs by allocating more than half of its total duration to hands-on exercises and by integrating both attacker and defender perspectives. The program effectively utilizes full-scale training infrastructure (SETT and PPSTE) to connect theory with practice, making it particularly suitable for practitioners with 2–5 years of experience. However, certain areas for improvement were identified, including abrupt difficulty transitions in some advanced exercises and limited practice opportunities in framework- and policy-related modules.

Furthermore, the proposed survey instrument provides a means to capture not only short-term satisfaction but also long-term training effects such as knowledge retention and workplace applicability. As such, it can serve as a foundational tool for improving not only the KINAC ITC but also other international training programs operated by KINAC, including those on nuclear security, safeguards, and strategic trade controls.

In conclusion, this study lays the groundwork for systematic evaluation and continuous improvement of nuclear cybersecurity education by combining curriculum analysis with learner-centered assessment. Although empirical validation remains to be conducted, this dual approach provides a practical framework and critical directions for aligning educational programs with real-world operational needs.

# 8 Acknowledgments

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. RS-2024-00403596)

# References

[1] *Computer Security for Nuclear Security*. Number 42-G in Implementing Guide. INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2021.

[2] Cybersecurity awareness and training (cat) framework for remote working employees. *PMC*, 2022.

[3] Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, 8(1):tyac006, 2022.

[4] Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science IT Research Journal*, 5(1):100–119, 2024.

[5] Towards an innovative model for cybersecurity awareness training. *Information*, 15(9):512, 2024.

[6] Jong Gyun Choi, Jae Gu Song, Jun Young Son, Dong Young Lee, Jung Woon Lee, and Cheol Kwon Lee. Development of cyber security test technology for nuclear i&c system. In *Proceedings of the KNS 2018 Spring Meeting*, pages 2–2, 2018.

[7] Cybersecurity and Infrastructure Security Agency. Ics training available through cisa, 2025.

[8] EC-Council. Ics/scada cybersecurity training, 2025.

[9] EC-Council CERT. Ics/scada cybersecurity, 2025.

[10] Idaho National Laboratory. Ics cybersecurity training, 2017.

[11] International Atomic Energy Agency. Iaea launches international training course on protecting nuclear facilities from cyber-attacks, 2018.

[12] International Atomic Energy Agency. Iaea conducts training course on protecting nuclear facilities from cyber-attacks, 2019.

[13] International Atomic Energy Agency. Innovation in virtual computer security training for nuclear and radiological facilities. *IAEA Bulletin*, 2023.

[14] Jackson School of International Studies. Cybersecurity and the nuclear industry, 2019.

[15] H. C. Kim. Kinac/insa international training activities and lessons learned. In *Proceedings of the Transactions of the Korean Nuclear Society Spring 2016 Meeting*, pages 2–2, May 2016.

[16] H. K. Lee. An analysis of international training courses on nuclear security in korea. In *Proceedings of the Transactions of the Korean Nuclear Society 2018 Autumn Meeting*, Oct 2018.

[17] H. K. Lee. Suspected north korean hacking attack... leakage of 720,000 nuclear plant documents [in korean]. Korea Economic Daily, Oct 2024. [Online]. Available: https://www.hankyung.com/article/2024100945185.

[18] S. M. Lim, A. Kim, and I. Shin. Trends in foreign regulations on cybersecurity of digital asset supply chains in nuclear power plants [in korean]. *Review of KIISC*, 26(1):54–60, 2016.

[19] E. B. Park, J. J. Han, B. W. Shin, and H. M. Park. Designing nuclear nonproliferation and security international training course demand survey. In *Proceedings of the Transactions of the Korean Nuclear Society 2024 Autumn Meeting*, Oct 2024.

[20] EunBee Park, Jae-Jun Han, Byung-Woo Shin, and Hui-Min Park. Designing nuclear nonproliferation and security international training course demand survey. In *Proceedings of the Transactions of the Korean Nuclear Society Autumn Meeting*, Changwon, Korea, Oct 2024.

[21] SANS Institute. Ics410: Ics/scada security essentials, 2025.

[22] J. G. Song, J. W. Lee, C. K. Lee, D. Y. Lee, and J. G. Choi. Preparation for cyber security incident response training in nuclear power plants. In *Proceedings of the Transactions of the Korean Nuclear Society 2020 Virtual Spring Meeting*, pages 9–11, 2020.

[23] Daniel L Stufflebeam. The relevance of the cipp evaluation model for educational accountability. 1971.

[24] Daniel L Stufflebeam. The cipp model for evaluation. In *Evaluation models: Viewpoints on educational and human services evaluation*, pages 279–317. Springer, 2000.

[25] Daniel L Stufflebeam. Cipp evaluation model checklist. 2007.

[26] Patricia Toth and Penny Klein. A role-based model for federal information technology/cyber security training. *NIST special publication*, 800(16):1–152, 2013.

[27] U.S. Nuclear Regulatory Commission. 10 CFR Part 73, Purpose and scope. in Title 10, Code of Federal Regulations, April 2023. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html.

[28] U.S. Nuclear Regulatory Commission. Cyber security programs for nuclear power reactors. Technical Report Regulatory Guide 5.71, Revision 1, U.S. Nuclear Regulatory Commission, February 2023.

[29] B. van den Berg et al. A systematic review of current cybersecurity training methods. *Computers Security*, 136:103584, 2023.

# A Questionnaires

## A.1 Pre-training Survey

**Pre-training Survey**

***<Category 1 – Prior Knowledge and Interest Level >***

1. I am familiar with the overall concept of cybersecurity.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

2. I understand the role of cybersecurity within the Physical Protection System (PPS).

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

3. I have previously attended a cybersecurity-related training program.

   [ ] Yes
   [ ] No

   (a) (If Yes) Please specify the name and year of the training you attended. (e.g., IAEA ITC 2024)

4. I regularly explore or keep up to date with trends related to this training's topic (e.g., newsletters, academic papers, applications in your workplace).

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

***<Category 2 – Perception and Need Recognition >***

5. I believe cybersecurity threats can affect the actual operation of nuclear facilities.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

6. The facility where I work considers cybersecurity in its Physical Protection System (PPS).

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

7. I have previously encountered difficulties performing PPS-related tasks due to a lack of knowledge in cybersecurity.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

8. Based on the PPS structure of my facility, I believe the concept of integrating cybersecurity and related training is necessary.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

***<Category 3 – Training Expectations>***

9. What aspects do you hope to gain from this ITC training? **(Multiple answers allowed.)**

[ ] Understanding of basic cybersecurity concepts
[ ] Learning from cybersecurity threat case studies
[ ] Improvement in practical response capabilities
[ ] Understanding the integration of cybersecurity and PPS
[ ] Exploring directions for implementing security policies in the facility

[ ] How to explain cybersecurity concepts to non-experts
[ ] Practical knowledge required in performing tasks
[ ] No particular expectations

10. If you have specific expectations for the training, please describe them:

***<Personal Information >***

11. Please enter your name.

12. Please enter your country of affiliation.

13. Please enter your affiliated institution.

14. Please enter your current area of responsibility.

15. Please enter your years of experience. (Numbers only, e.g., 5)

## A.2 Post-eLearning Survey

Post-eLearning Survey

***<Category 1 – Change in Understanding and Interest>***

1. I am familiar with cybersecurity in the Physical Protection System (PPS).

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

2. I feel that my understanding of cybersecurity has improved through eLearning.

[ ] Strongly Agree

[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

3. I gained an understanding of the role of cybersecurity within the Physical Protection System (PPS) through eLearning.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

4. I recognize the necessity of cybersecurity in PPS through eLearning.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

5. My overall interest in cybersecurity has increased due to eLearning.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

6. My interest in cybersecurity, specifically within the context of PPS, has increased through eLearning.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

***<Category 2 – Perception of Importance / Training Effectiveness and Practical Understanding>***

7. I believe cybersecurity threats can affect the actual operation of facilities.

[ ] Strongly Agree

[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

8. The facility where I work considers cybersecurity in its Physical Protection System (PPS).

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

9. Based on the PPS structure of my facility, I believe the concept of integrating cybersecurity and related training is necessary.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

10. I feel capable of identifying cybersecurity vulnerabilities and considering countermeasures in real-world situations.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

11. I feel confident suggesting improvements in protection systems that are related to cybersecurity.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

12. This training has broadened my understanding and awareness in a way that is helpful to my work.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

***<Category 3 – Training Gains and Expectations>***

13. Which aspects of this eLearning training were helpful to you? (Multiple answers allowed.)

    [ ] Understanding of basic cybersecurity concepts
    [ ] Learning from cybersecurity threat case studies
    [ ] Improvement in practical response capabilities
    [ ] Understanding the integration of cybersecurity and PPS
    [ ] Exploring directions for implementing security policies in the facility
    [ ] How to explain cybersecurity concepts to non-experts
    [ ] Practical knowledge required in performing tasks
    [ ] No especially helpful part

14. Which aspects do you hope to gain from the upcoming ITC training? (Multiple answers allowed.)

    [ ] Understanding of basic cybersecurity concepts
    [ ] Learning from cybersecurity threat case studies
    [ ] Improvement in practical response capabilities
    [ ] Understanding the integration of cybersecurity and PPS
    [ ] Exploring directions for implementing security policies in the facility
    [ ] How to explain cybersecurity concepts to non-experts
    [ ] Practical knowledge required in performing tasks
    [ ] No particular expectations

15. If you have specific expectations for the upcoming training, please describe them:

***<Category 4 – Satisfaction with eLearning and Suggestions>***

16. Please rate your satisfaction with the following components of the eLearning course:

    (a) I am _____ with the content and structure of the lectures (modules).
        [ ] Very Satisfied

[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(b) I am _____ with the delivery method of the lectures.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(c) I am _____ with the difficulty level of the lectures.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

17. Please describe any aspects of the eLearning course that you found especially satisfying:

18. Please describe any aspects that you found lacking or areas you feel need improvement in the eLearning course:

***<Personal Information >***

19. Please enter your name.

20. Please enter your country of affiliation.

21. Please enter your affiliated institution.

22. Please enter your current area of responsibility.

23. Please enter your years of experience. (Numbers only, e.g., 5)

## A.3 Post-training Survey

**Post-training Survey**

***<Category 1 – Change in Understanding and Interest>***

1. I feel that my understanding of cybersecurity has improved through this training.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

2. I gained an understanding of the role of cybersecurity within the Physical Protection System (PPS).

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

3. I recognize the necessity of cybersecurity in PPS.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

4. My overall interest in cybersecurity has increased due to this training.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

5. My interest in cybersecurity, specifically within the context of PPS has increased.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree

[ ] Strongly Disagree

***<Category 2 – Effectiveness and Practical Understanding>***

6. I feel capable of identifying cybersecurity vulnerabilities and considering countermeasures in real-world situations.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

7. I feel confident suggesting improvements in protection systems that are related to cybersecurity.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

8. This training has broadened my understanding and awareness in a way that is helpful to my work.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

9. Read the following scenario and answer the questions below:

   > You have been dispatched as part of a security assessment team to a nuclear power plant to evaluate whether cybersecurity elements are appropriately integrated into its Physical Protection System (PPS). Upon arrival, you discover that some protection equipment is directly connected to the internet and that the access control system has not been updated for a long time. User access requires login credentials (ID: employee ID number, Password: user-set). When asked about the cybersecurity matters, field staff argued that cybersecurity is IT team's responsibility. Also, PPS team was not receiving any training or taking care of issues related to cybersecurity.

(a) What security threats can you identify in the scenario above?

(b) As a security evaluator, what would you prioritize checking or recommending for improvement in this situation?

***<Category 3 – Training Satisfaction and Feedback>***

10. Which aspects of this training were helpful to you? (Multiple answers allowed.)

[ ] Understanding of basic cybersecurity concepts
[ ] Learning from cybersecurity threat case studies
[ ] Improvement in practical response capabilities
[ ] Understanding the integration of cybersecurity and PPS
[ ] Exploring directions for implementing security policies in the facility
[ ] How to explain cybersecurity concepts to non-experts
[ ] Practical knowledge required in performing tasks
[ ] No especially helpful part

11. Please rate your satisfaction with the following training components:

(a) I am _____ with the content and structure of the lectures.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(b) I am _____ with the delivery method of the lectures.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(c) I am _____ with the difficulty level of the lectures.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(d) I am _____ with the implementation of the quizzes.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(e) I am _____ with the quiz format.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(f) I am _____ with the education technology used in the quizzes.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(g) I am _____ with the difficulty level of the quizzes.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(h) I am _____ with the hands-on exercises.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(i) I am _____ with the format of the hands-on exercises.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(j) I am _____ with the group discussion activities.

[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral

[ ] Dissatisfied
[ ] Very Dissatisfied

(k) I am _____ with how the group discussions were conducted.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(l) I am _____ with the overall organization and operation of the 5-day course.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(m) I am _____ with the time distribution across the course.
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(n) I am _____ with the overall flow and structure of the course (module → exercise → group discussion → hands-on, etc.).
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

(o) I am _____ with the additional services provided (e.g., accommodation, meals, etc.).
[ ] Very Satisfied
[ ] Satisfied
[ ] Neutral
[ ] Dissatisfied
[ ] Very Dissatisfied

12. If there was a day during the training that you found most satisfying, please select one and describe the reason below.
[ ] Day 1
[ ] Day 2

[ ] Day 3
[ ] Day 4
[ ] Day 5
[ ] None

13. If there was a day during the training that you found least satisfying, please select one and describe the reason below.

[ ] Day 1
[ ] Day 2
[ ] Day 3
[ ] Day 4
[ ] Day 5
[ ] None

14. Please describe any other aspects of the training you found especially satisfying:

15. Please describe any aspects that you found lacking or areas you feel need improvement:

16. Please share any topics you would like to see added or explored in greater depth in future INSA ITC training courses:

***<Personal Information >***

17. Please enter your name.

18. Please enter your country of affiliation.

19. Please enter your affiliated institution.

20. Please enter your current area of responsibility.

21. Please enter your years of experience. (Numbers only, e.g., 5)

## A.4 3-Month Follow-Up Survey

3-Month Follow-Up Survey

***<Category 1 – Prior Knowledge and Interest Level>***

1. I am familiar with cybersecurity in general.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

2. I understand cybersecurity within the context of Physical Protection Systems (PPS).

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

3. I have attended cybersecurity-related training since participating in the ITC program.

   [ ] Yes
   [ ] No

   (a) (If Yes) Please specify the name and year of the training attended (e.g., IAEA ITC 2024).

4. I regularly explore or keep updated with recent developments related to this training (e.g., newsletters, research papers, application methods in your workplace).

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

5. I feel the cybersecurity knowledge gained through this training has been helpful in my actual work.

   [ ] Strongly Agree
   [ ] Agree

[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

6. Since the training, I recognize the role and importance of cybersecurity in PPS and actively attempt to apply it in my duties.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

7. Based on my awareness of cybersecurity from the training, I am checking or improving the cybersecurity conditions at my facility.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

8. I share the cybersecurity concepts learned through this training with my colleagues and team members and strive to collectively apply them.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

***<Category 2 – Perception and Necessity>***

9. I believe cybersecurity threats can impact actual facility operations.

   [ ] Strongly Agree
   [ ] Agree
   [ ] Neutral
   [ ] Disagree
   [ ] Strongly Disagree

10. I believe my facility considers cybersecurity within its Physical Protection System (PPS).

    [ ] Strongly Agree

[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

11. I have experienced difficulties performing tasks due to insufficient cybersecurity knowledge.

    [ ] Strongly Agree
    [ ] Agree
    [ ] Neutral
    [ ] Disagree
    [ ] Strongly Disagree

12. Considering my facility's PPS structure, I see a necessity for integrating cybersecurity concepts and related training.

    [ ] Strongly Agree
    [ ] Agree
    [ ] Neutral
    [ ] Disagree
    [ ] Strongly Disagree

13. I feel capable of recognizing cybersecurity vulnerabilities in real situations and considering response measures.

    [ ] Strongly Agree
    [ ] Agree
    [ ] Neutral
    [ ] Disagree
    [ ] Strongly Disagree

14. I am confident in suggesting improvements related to cybersecurity in protection systems.

    [ ] Strongly Agree
    [ ] Agree
    [ ] Neutral
    [ ] Disagree
    [ ] Strongly Disagree

15. This training has contributed to broadening my practical understanding and awareness.

[ ] Strongly Agree
[ ] Agree
[ ] Neutral
[ ] Disagree
[ ] Strongly Disagree

***<Category 3 – Training Satisfaction and Recommendations>***

16. Which aspects of the ITC training were helpful to you? (Multiple answers allowed)

    [ ] Understanding basic cybersecurity concepts
    [ ] Learning about cybersecurity threat cases
    [ ] Enhancing practical response capabilities
    [ ] Understanding integration with Physical Protection Systems
    [ ] Exploring implementation of security policies within facilities
    [ ] Methods to explain cybersecurity concepts to non-experts
    [ ] Practical knowledge for performing tasks
    [ ] No particular expectations met

17. Please describe any other aspects of the training you found especially satisfying:

18. Please describe any aspects that you found lacking or areas you feel need improvement:

19. Please share any topics you would like to see added or explored in greater depth in future INSA ITC training courses:

***<Personal Information >***

20. Please enter your name.

21. Please enter your country of affiliation.

22. Please enter your affiliated institution.

23. Please enter your current area of responsibility.

24. Please enter your years of experience. (Numbers only, e.g., 5)