Enhancing of evaluation criteria of cybersecurity exercises based on NIST SP 800-84

Eunji Chang*, Hyunjoo Lee
Korea Institute of Nuclear Nonproliferation and Control
**ejchang@kinac.re.kr*

***Keywords : Cybersecurity exercise, Evaluation, Evaluation criteria**

1. Introduction

In accordance with the Enforcement Decree of "the Act on Physical Protection and Radiological Emergency", nuclear licensees must conduct physical protection exercise and cybersecurity exercise to verify its effectiveness and the organization's readiness to execute contingency plan [1]. Additionally, licensees must incorporate detailed plans for the exercising by complying the Radiological Emergency Act's enforcement decree and notifications defined by the Nuclear Safety and Security Commission.

Korea Institute of Nuclear Nonproliferation and Control (hereinafter referred to as KINAC) published regulatory guide for cybersecurity exercise, KINAC/RS-011 "Exercise on cybersecurity incident response in nuclear facilities" (hereinafter referred to as KINAC/RS-011) which gives standards and criteria for evaluation of effectiveness of cybersecurity exercises. Although KINAC/RS-011 provides what should an appropriate cybersecurity exercise contains, it only considers qualitative evaluation criteria.

This paper refers to technical documents, the National Institute of Standards and Technology (NIST) SP 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" (hereinafter referred to NIST SP 800-84) [2], which details the procedures of cybersecurity exercise and suggest to add evaluation criteria in order to develop more detailed criteria to increase effectiveness of cybersecurity exercises.

2. Review of exercise on cybersecurity incident response in nuclear facilities (KINAC/RS-011)

Exercise plans submitted by licensees undergo review of KINAC according to the delegation regulations of the NSSC and can only be implemented after receiving approval from the Commission. The evaluation of exercises is conducted by KINAC evaluators. Through this cybersecurity exercises, nuclear licensees assess the effectiveness of cybersecurity incident response plans and periodically evaluate the response capabilities of their cybersecurity incident response teams. The detailed evaluation items described in table 1 are intended to be assessed during exercises, incorporating threat response scenarios as evaluation criteria.

Table 1: Exercise evaluation criteria of KINAC/RS-011

Category	items
Design	Type of exercise
	Planning of exercise
	Objective of exercise
	Target of exercise
	Range of exercise
	Method of exercise
	Participants of exercise
	Schedule of exercise
	Control and assessment of exercise
	Scenario of exercise
Conduct	Implementation of exercise
	Critique of exercise
Evaluation	Assessment of exercise
	Injecting assessment of exercise
etc.	Corrective action from previous year

KINAC/RS-011 provides a list of items, as it is shown in table 1, however, more detailed criteria can be developed to evaluate licensees' response capabilities and reflect evolving cybersecurity threats, referring other guidance or standards such as NIST SP 800-84. By incorporating the preparedness for zero-day attacks targeting infrastructure and evolving industrial control systems, for example analyzing vulnerabilities in Programmable Logic Controllers (PLCs) and communication-based hardware and software, a more multidimensional evaluation can be achieved.

3. Evaluation criteria from NIST SP 800-84

NIST SP 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" provides guidance on designing, developing, conducting, and evaluating exercise programs for cybersecurity incident response. Among the types of cybersecurity exercise, tabletop exercises and functional exercises, which are commonly conducted in IT-based exercise, are extensively documented regarding the planning and evaluation of exercise programs.

In the case of tabletop exercises, there is the advantage of conducting standalone and joint exercise for senior-level and operational-level groups by forming small groups or multiple groups, which can be an economical exercising method that can reduce costs. Furthermore, by developing scenarios to test and evaluate the existing emergency response plan in an actual exercise, in-depth questions linked to the scenarios can be asked directly to the participants, allowing for a verification process to identify

differences between the emergency response plan and actual scenario response processes and improvement requirements, thereby efficiently enhancing preparedness for effective responses in real situations.

Functional exercises can require more detailed scenarios and roles and responsibilities for exercise supervisors, information collectors, and participants are clearly defined. The Master Scenario Events List (MSEL) is developed to remind participants of the flow of the exercise, branching conditions, activities required for each event or situation, and the exercise objectives, ensuring that participants maintain the timeliness of their roles, authority, tasks, and duties until the end of the exercise.

Fig. I. Master Scenario Events List (MSEL) example from NIST SP 800-84

Master Scenario Events List

Event #	MSEL Key Event Description	Expected Actions Resulting from MSEL Event	Objectives
1	***Example*** The [*insert organization name*] experiences electronic intrusions on critical information systems.	***Example*** Supporting Injects: Day 1, 0900 - 1700 ▪ Activate cyber incident response team ▪ Implement Cyber Intrusion Response Plan ▪ Notify and coordinate with customers and other stakeholders ▪ Take actions to clean infected systems	***Example*** ▪ Familiarize staff with responsibilities under Cyber Intrusion Response Plan ▪ Validate Cyber Intrusion Response Plan ▪ Coordinate with Federal cyber entities, customers, and key stakeholders
2	***Example*** The Homeland Security Advisory System threat level has been raised from an Orange "High" to a Red "Severe" risk of terrorist attack.	***Example*** Supporting Injects: Day 1, 1000 - 1200 ▪ Activate emergency response teams ▪ Initiate backup procedures for all mission critical IT systems ▪ Relocate essential personnel to alternate facilities ▪ Coordinate with the White House and other departments and agencies to inform them of decision to relocate operations	***Example*** ▪ Familiarize staff with emergency activation and notification procedures ▪ Validate IT contingency plans and procedures ▪ Validate relocation plans and procedures ▪ Validate coordination and communications processes with key stakeholders
3	***Example*** A large explosion occurs outside the Office Building.	***Example*** Supporting Injects: Day 1, 1200-1700 ▪ All commercial power to building has been cut ▪ The site reports that some data communications links have failed ▪ Facility managers report the building cannot be repaired	***Example*** ▪ Validate IT contingency plans and procedures ▪ Identify whether additional contingency plans need to be developed ▪ Examine plans to restore data center operations
4	***Example*** Possible threat of terrorism to alternate facility.	***Example*** Supporting Injects: Day 2, 1000-1200 ▪ Explore options if alternate facility is disabled ▪ Prioritize IT system recovery	***Example*** ▪ Identify whether additional contingency plans should be developed for alternate facility

Based on NIST SP 800-83, few items that can be used as evaluation criteria for cybersecurity exercises have been selected as follows.

Table 2: Selected evaluation criteria

Category	Items
Design	Development of MSEL
	Listing of questions based on the exercise scenario
	Duration time
	Setting roles and responsibilities for exercise supervisors, information collectors, and simulators
Conduct/ Evaluation	Injection the message and tracking
	Assessment on MSEL implementation
	Answering questions based on the exercise scenario

The selected detailed items can be utilized in the planning, implementation, and evaluation phases of cybersecurity exercises, and the expected outcomes for each item are as follows:

Through the development and operation of the Master Scenario Events List (MSEL), the traditional exercise scenario, which was based on the passage of time, will branch based on event occurrences, making it clearer to distinguish their roles and responsibilities and tasks when events occur, thus motivating participants to engage more actively in the exercise, enhancing its effectiveness. The development of MSEL can be regarded as criteria in planning, method, scenario of exercise when revising KINAC/RS-011.

By listing questions based on the scenarios, the tabletop exercise can lead to a variety of outcomes. Pre-determined topics shall be provided, and participants can engage in Q&A sessions with segmented questions allowing for a thorough review of their roles and responsibilities, and the operator's emergency response plans.

Setting the exercise duration allows for the quantitative evaluation of participants' preparedness for cyber incidents within a specified timeframe. Duration time and its punctuality can be one of criteria on the goal or objectives of the exercise.

By granting roles and responsibilities for exercise supervisors, information collectors, and simulators, technical support necessary for conducting the exercise can be configured, and various roles can be assigned to enhance awareness of the licensees regarding the exercise.

Evaluation criteria derived in this paper can be used as references for both planning cybersecurity exercises of licensees and revising KINAC/RS-011 in order to enhance effectiveness of cybersecurity exercise evaluation.

4. Conclusion

This paper examines the basic requirements demanded by relevant laws and regulatory standards for conducting cybersecurity exercises, as well as the content of detailed evaluation criteria from the process of performing cybersecurity exercises. The evolving cyber threats to industrial control systems necessitate the enhancing effectiveness of cybersecurity exercises, and evaluation of cybersecurity exercise need to be more multidimensional.

In this paper, by referencing the NIST 800-64 technical standard document, four evaluation criteria applicable to the current exercise evaluation system were derived: (1) MSEL development, (2) development of scenario-based question lists, (3) limiting exercise duration, and (4) assigning roles and responsibilities for exercise supervisors, information collectors, and simulators. In this context, various international technical standards and materials for establishing IT-based or cybersecurity exercises will be referenced for future research.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS), granted financial resource

from the Nuclear Safety and Security Commission(NSSC), Republic of Korea. (No. 2106012)

REFERENCES

[1] Presidential Decree No.26140, “Enforcement Decree of the Act on Physical Protection and Radiological Emergency”, 2015.
[2] Time Grance et al., “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities”, NIST ST 800-84, 2006.
[3] Korea Institute of Nuclear Nonproliferation and Control, “Cybersecurity Regulatory Standard for Nuclear Facilities”, KINAC/RS-015, 2023
[4] Korea Institute of Nuclear Nonproliferation and Control, “Regulatory Standard for Cybersecurity Exercise for Nuclear Facilities”, KINAC/RS-011, 2020.