A study on the RS-015 based Checklist and Acceptance Criteria for Support Consistent Review in Regulation

Jae-Gu Song *, Cheol-Kwon Lee, Jung-Woon Lee
Korea Atomic Energy Research Institute, Yuseong-gu, Daejeon 305-353, Republic of Korea
**Corresponding author: jgsong@kaeri.re.kr*

1. Introduction

As cybersecurity for nuclear facilities has been important, the related laws and regulatory guidelines have been published.

The RG 5.71 was published by the NRC in U.S. and the RS-015 by KINAC in Korea[1, 2].

RG 5.71 and RS-015 describe overall requirements for the licensee. So nuclear industries, such as NEI, in consultation with the regulatory bodies, develop and use detailed implementation guidelines on how to apply the regulatory requirements to their facilities[3].

Despite these efforts, some difficulties still can be met during cybersecurity assessments for nuclear facilities.

In the licensees' point of view, the requirements of cybersecurity assessments are lack of detail, and there exist too many CDAs and also difficulties in implementing security controls in operating facilities.

Meanwhile, from the regulator's point of view, it is difficult to maintain the consistency of acceptance criteria for various types of facilities.

This study develops checklists and acceptance criteria to support consistent assessment in regulatory inspections and suggests methods for using checklists and acceptance criteria.

2. Development of checklist and acceptance criteria

In this study, as shown in Figure 1, the checklist was developed for each requirement of RS-015 technical security controls to confirm the implementation of security controls for critical systems and critical digital assets[4].

The types of documented evidence and the level of information, which are provided as a response to each checklist item, were also defined.

The regulators can identify the status of cybersecurity implementation by examining the documented evidence and information provided by the licensees in accordance to the acceptance criteria for each checklist item.

This approach is a prescriptive-based method and has advantages of reviewing the implementation status than defining what to improve in detail[4].

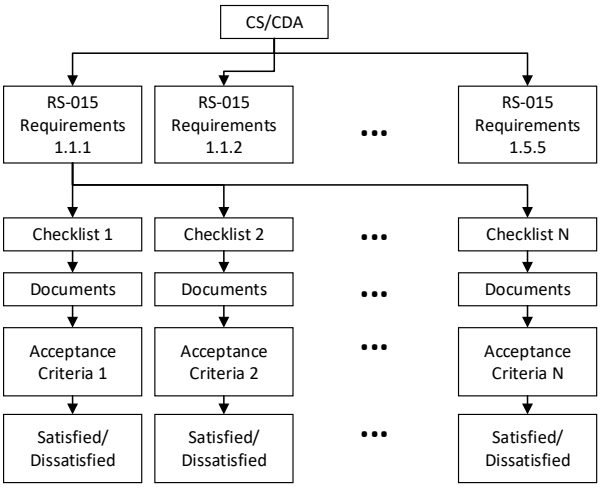

Fig. 1. Development process of checklists and acceptance criteria

2.1 Development of checklists for detailed technical requirements

The technical security controls in RS-015 have a total of 62 items in the following 5 categories: access control, audit and accountability, system and communication protection, identification and authentication, and system hardening.

The 62 items can be divided into a total of 182 basic security control requirements.

The checklist is a set of questionnaire for checking the 182 security control requirements.

The checklist developed can be categorized into the following four types according to the object to be identified[5, 6]:

① Checklist for checking facility-wide top-level policies, guidelines, and procedures,
② Checklist for identifying the target (CDA),
③ Checklist for checking policies, guidelines, and procedures at the level of CS/CDA, and
④ Checklist for checking the detailed implementation status of CS/CDA.

2.2 Analysis of documented evidence for each checklist

To check the compliance with the regulatory requirements, it is essential to submit a checklist response and explanation as well as evidence.

In this study, documented evidence to be evaluated by the regulator is defined at minimum as follows[4, 5]:

- Cyber Security Plan (CSP) for the site,
- User's manual for the target CS/CDA (including system design and operation materials),
- Detailed security guidelines for the target CS/CDA, and
- Detailed security audit data of the target CS/CDA (media access log, physical access log, etc.).

2.3 Development of Acceptance Criteria

Acceptance Criteria were developed to determine the validity, adequacy, and sufficiency of the checklist response and information submitted by the licensee in accordance with the four types of checklist described in 2.1[7, 8].

① Confirm that the CS/CDA data to be reviewed, such as information provided in CS/CDA level policies, guidelines, and procedures, include all the information representing the current operating status.
② Confirm that the CS/CDA data to be reviewed, such as information provided in CS/CDA level policies, guidelines, and procedures, include the information related to the contents of checklist.
③ Confirm that the information provided in the CS/CDA level policies, guidelines, and procedures is enough for checking the contents of checklist.
④ Confirm that the information provided in the CS/CDA level policies, guidelines, and procedures is satisfactory to the detailed requirements of checklist.

2.4 Proposal for use in cybersecurity regulation

The following procedures are proposed for the regulatory cybersecurity assessments using the developed Checklist and Acceptance Criteria;

① The regulator prepares a checklist based on RS-015 and provides it to the licensee. For this purpose, the regulator utilizes the checklist developed in this study.
② The licensee submits to the regulator the checklist response attached the documented evidence.
③ The regulator determines whether to proceed with the assessment by reviewing the checklist response received with the documented evidence. If it is difficult to proceed with the assessment, the regulator sends a written opinion to supplement and requests to resubmit. In this process, the regulatory body references the evaluation points of checklist and the review items of documented evidence listed as examples in this study.
④ Checklist responses and documented evidence are then examined for their validity, adequacy, and sufficiency to ensure that security is maintained in the facility in accordance with the acceptance criteria. In unsatisfactory cases, explain the reasons and request to strengthen the implementation of cybersecurity controls. In this process, the regulatory body uses the acceptance criteria developed in this study.

In order for the security assessment to proceed through the above procedures, the regulatory body and licensee require ongoing communication based on mutual trust.

3. Conclusions

In this study, a set of checklists and acceptance criteria based on RS-015 were developed to support consistency in the security assessments for nuclear facilities. A method of application in cybersecurity regulation was also proposed.

Detailed checklist and acceptance criteria will be included and explained in the N-STAR report of the Korea Foundation of Nuclear Safety.

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. 2003022)

REFERENCES

[1] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.
[2] KINAC/RS-015, Technical standard for the security of computer and information systems in nuclear facilities, Rev. 1, Korea Institute of Nuclear Nonproliferation and Control, 2014.
[3] NEI 13-10 rev.6, Cyber Security Control Assessments, Nuclear Energy Institute, 2017.
[4] NUREG/BR-0303, Guidance for Performance-Based Regulation, U.S. Nuclear Regulatory Commission, 2002.
[5] J. G. Song, J. W. Lee, C. K. Lee, J.S Shin, J. G. Choi, D. Y. Lee, Y. J. Lee, J. Y. Son, Development of RS-015 Regulatory Requirements Evaluation Criteria and Checklist, Nuclear Safety Technology Analysis Report, Korea Foundation of Nuclear Safety, October 2020.
[6] J. G. Song, J. W. Lee, J.S Shin, C. K. Lee, A Study of a Guide Development for Regulatory Acceptance Criteria of Technical Security Controls, Transactions of the Korean Nuclear Society Virtual Autumn Meeting, Korea Foundation of Nuclear Safety, December 2020.
[7] J. G. Song, C. K. Lee, J. W. Lee, J. S. Shin, A Case Study on ESF-CCS TEST-BED Evaluation Using RS-015 Regulatory Requirements Checklist, Nuclear Safety Technology Analysis Report, Korea Foundation of Nuclear Safety, August 2021.
[8] J. G. Song, C. K. Lee, J. W. Lee, J. S. Shin, Development of Acceptance Criteria for RS-015 Regulatory Requirements Checklist, Nuclear Safety Technology Analysis Report, Korea Foundation of Nuclear Safety, September 2021.