

원자력 사이버보안 검사를 위한 성능측정 활용사례 소개

Introduction of Performance Measure Cases for Nuclear Cyber Security Inspection

'21.5.13

핵안보본부 사이버보안실

권국희 선임연구원/PM

vivacita@kinac.re.kr

목 차

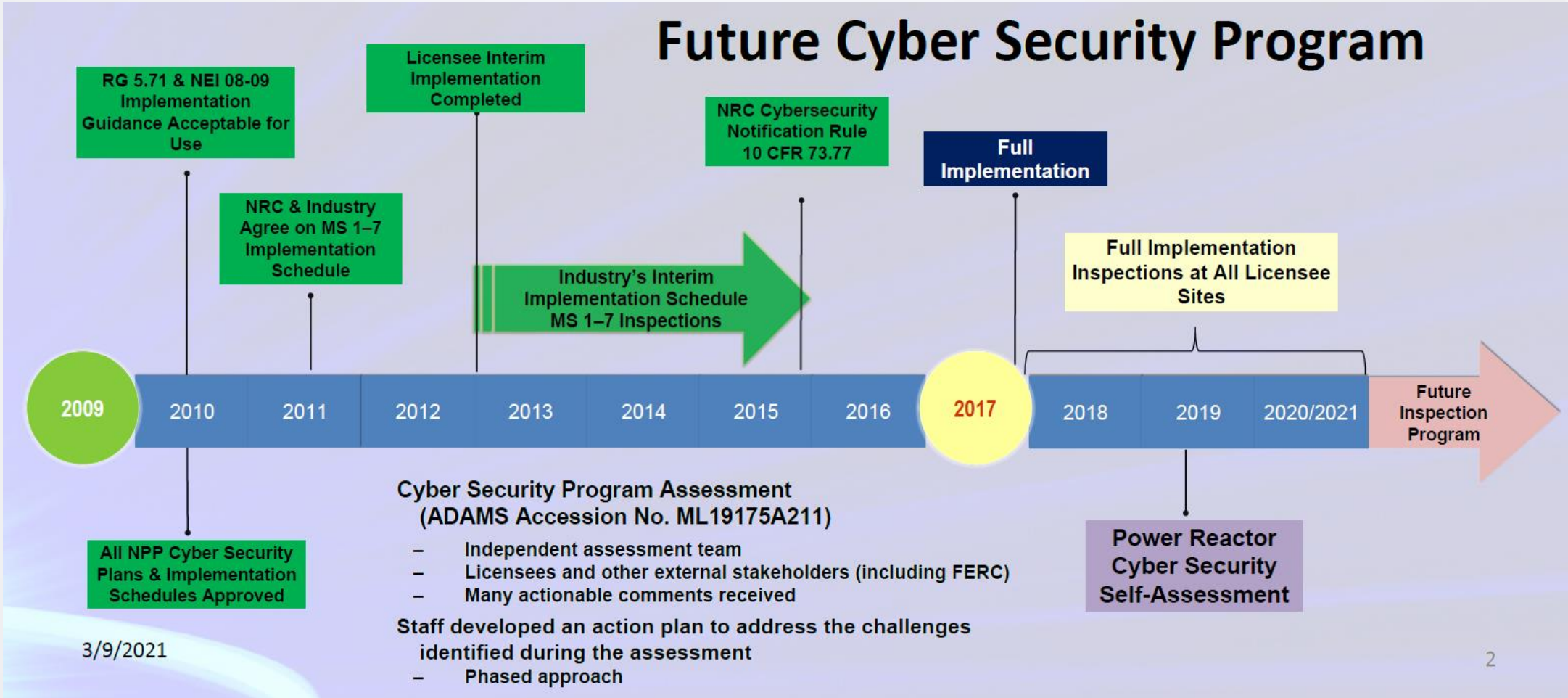
01 NRC activities

02 Performance Measure Cases

03 결언

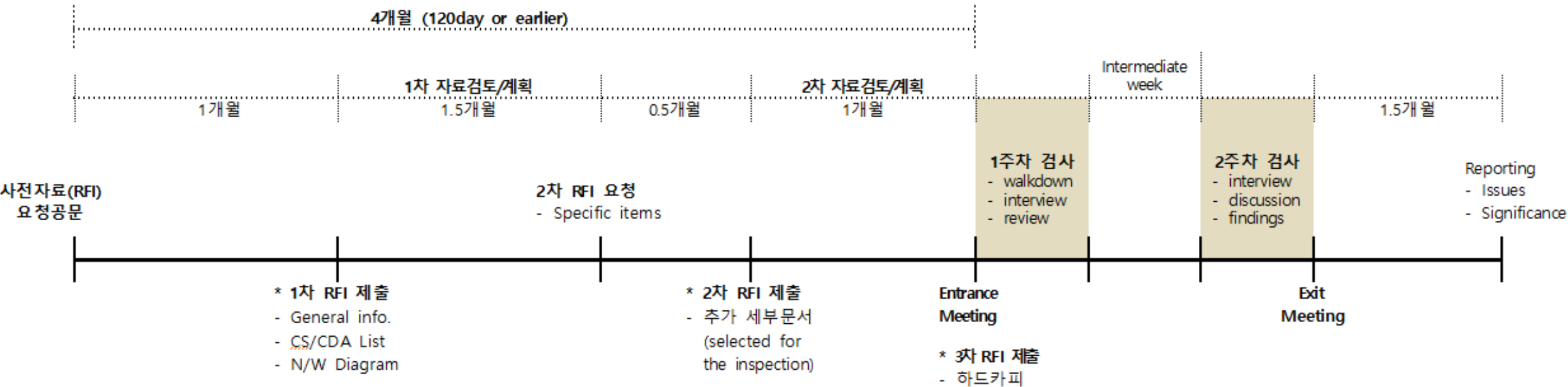
□ NRC Activities

- 9/11 이후, Updated DBT(10 CFR 73.1, 2007)를 통해 사이버보안 규제



□ NRC Activities

- MS8(full implementation) 검사 체계



□ NRC Activities

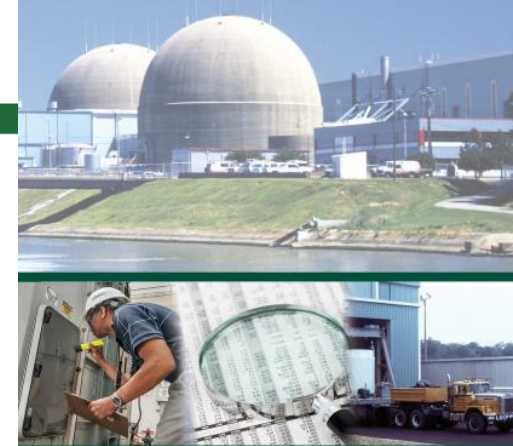
출처 : 2019 NRC OIG 감사결과 공개용



OFFICE OF THE INSPECTOR GENERAL
U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of NRC's Cyber Security Inspections at Nuclear Power Plants

OIG-19-A-13
June 4, 2019



Finding 1)

- The CS inspection program faces future staffing challenges

Finding 2)

- The CS inspection program has not identified performance measures

Office of the Inspector General
U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-19-A-13
June 4, 2019

Results in Brief

Why We Did This Review

Under the Cyber Security Rule at 10 Code of Federal Regulations 73.54, the Nuclear Regulatory Commission (NRC) requires that licensees operating a nuclear power plant provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. The Cyber Security Rule required licensees to submit for NRC review and approval a Cyber Security Plan with a proposed implementation schedule.

NRC is conducting cyber security inspections through 2020 to verify that licensees have fully developed cyber security programs conforming to the Cyber Security Rule and licensing basis commitments such as the approved Cyber Security Plan.

The audit objective was to determine whether the cyber security inspection program provides reasonable assurance that nuclear power plant

Audit of NRC's Cyber Security Inspections at Nuclear Power Plants

What We Found

NRC's cyber security inspections generally provide reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness.

However, although NRC trains current staff as cyber security inspectors, the inspection program faces future staffing challenges because demographic and resource constraints work against optimal staffing. Challenges in maintaining cyber security expertise among the inspectors could hinder NRC's ability to manage cyber security risk.

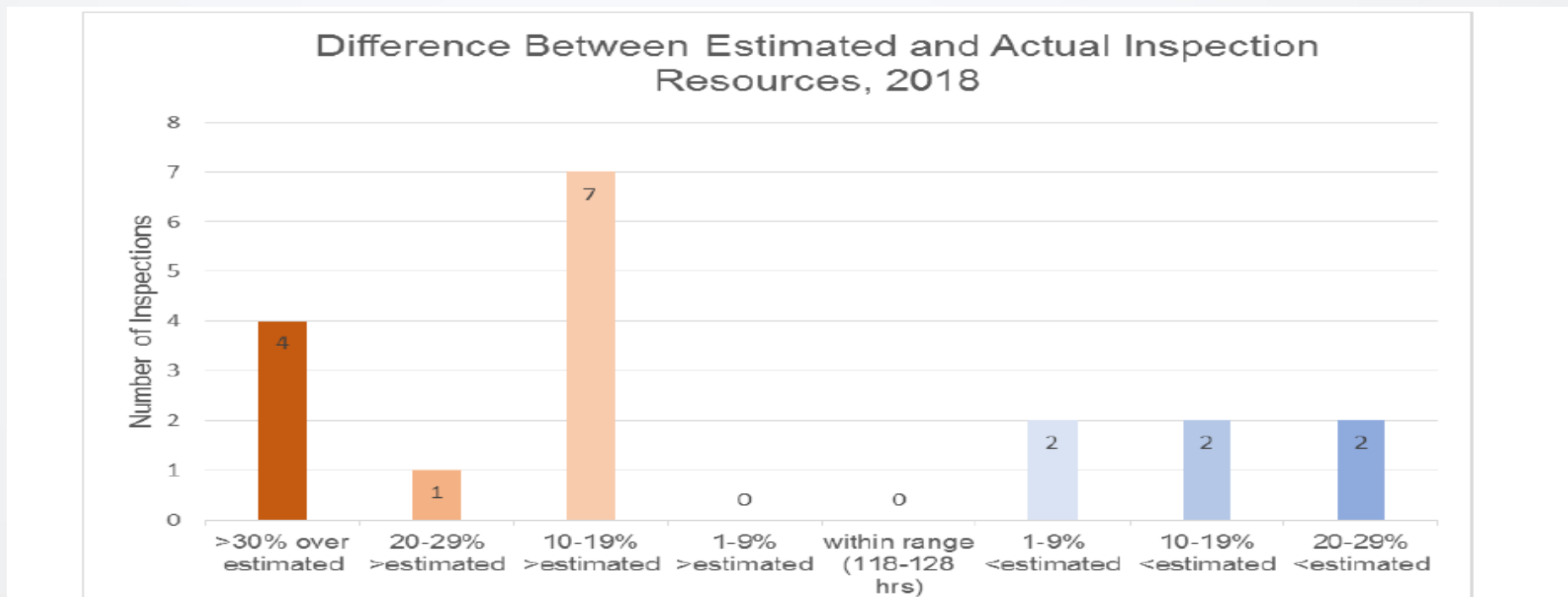
Additionally, the current cyber security inspection program is risk-informed but not yet fully performance based. The cyber security inspection program has not identified performance measures because of technical and regulatory challenges in program implementation, and there are challenges in predicting the level of effort required to conduct inspections. Identifying appropriate performance measures will permit NRC's cyber security inspection program to become more efficient and reliable without diminishing the level of assurance.

What We Recommend

□ NRC Activities

Recommendation 1) Hiring flexibilities, Internal rotations, Competency modeling, Availability of outside training and continuous training, Appropriate numbers and roles of staff

Recommendation 2) Use the results of experience and discussions with industry to develop and implement suitable **cyber security performance measure(s) (e.g., testing, analysis of logs, etc.)** by which licensees can demonstrate sustained program effectiveness.



□ CS Performance Measure Cases

❖ (draft) CS Inspection Procedure 71130.10 ('21.3)

- The inspector(s) will **consider the following inspection requirements** when developing the inspection plan and identifying the inspection sample.
 - 03.01 Review Ongoing Monitoring and Assessment Activities
 - 03.02 Verify Defense-in-Depth Protective Strategies
 - 03.03 Review of Configuration Management and Change Control
 - 03.04 Review of Cyber Security Program
 - 03.05 Evaluation of Corrective Actions

Sections 03.01 to 03.05 constitute the areas that include the inspection requirements.

If a licensee develops performance testing or performance metrics, as described in Section 03.06, and found satisfactory through review by the inspectors, **identified sections may be waived**

□ CS Performance Measure Cases

❖ (draft) CS Inspection Procedure 71130.10 ('21.3)

• 03.01 Review Ongoing Monitoring and Assessment Activities

a) Review Ongoing Monitoring Activities *(Per. Testing)*

- CDA에 적용된 security control들의 지속성을 확인하는 사업자의 프로세스와 평가활동을 검증
- 사업자가 만족할만한 "performance testing" 제출한다면, waive될 수 있음.

b) Review Vulnerability Assessment Activities *(Per. Testing)*

- 신뢰소스로부터 vulnerability & threat 공지 받고, screen/evaluating/disposal 프로세스와 평가활동을 검증

c) Review Effectiveness Analyses

- 24개월 단위의 효과성 검토로 periodic audits of CS program, procedures, SSI activities & testing/maintenance/calibration program 등을 포함

❖ (draft) CS Inspection Procedure 71130.10 ('21.3)

• 03.02 Verify Defense-in-Depth Protective Strategies

a) DID protective strategies (Per. Testing)

- 사이버위협에 대한 DID에 따른 사업자의 detect, response, recover 역량 유지에 대한 검증
- 예) automatic mechanisms to capture logs & to generate alarms

b) Defensive Security Architecture (Per. Testing)

- 보안레벨간 boundary protection을 보증하기위한 프로세스와 평가활동 검증

c) Maintain Security Controls

- CDA가 CS high assurance를 위하여 보안통제 유지 사항을 검증

d) User Identification and Authentication (Per. Testing)

e) PMMD (Per. Testing)

□ CS Performance Measure Cases

❖ (draft) CS Inspection Procedure 71130.10 ('21.3)

- **03.03 Review of Config. Management and change control**
 - a) design changes or replacement equipment *(Per. Testing)*
 - b) security impact analysis of changes and environments *(Per. Testing)*
 - c) supply chain and services acquisition
- **03.04 Review of Cyber Security Program**
 - a) CSP changes & implementing procedures
 - b) Review incident response and contingency plans
 - c) Review training
- **03.05 Evaluation of Corrective Action**

□ CS Performance Measure Cases

❖ Performance Testing

- If the answer to the following are “yes”, then the inspector may determine that the demonstration of **the performance and function test is adequate**
 - 1) In accordance with the CSP, licensees are required to collect data, to document results, and to evaluate the effectiveness of existing cyber security programs and cyber security controls. **Did the licensee submit information that describes and documents results of its performance testing assessment program as part of the Request for Information (RFI) submission?**

❖ Performance Testing

2) Was the **cyber-attack performance and functional test authentic and realistic?**

Specifically, the virtual network test configuration had to reasonably match the site's specific computer network configuration(s) and the cyber-attack testing performed, and realistically challenged the virtual network.

3) **If the licensee identified issues during the performance testing, did they appropriately categorize and correct the deficiencies?** If the testing deficiency revealed a noncompliance with the CSP, did the licensee implement appropriate compensatory measures, prioritize the deficiency, and implement corrective actions? Licensees are required to monitor the cyber security program through random testing of cyber security intrusion monitoring tools, periodic functional testing, and vulnerability scans/assessments.

❖ Performance Metrics

- **If the following data is provided completely** to the inspection team during the RFI submission, **the inspection team shall be reduced by contractor.**
 - 1.1 **(Access control)** No. of violations of access control policy identified during the quarter
 - 1.3 **(Access control)** No. of non-compliance incidents of CS controls by 3rd personnel
 - **0~1** = Good Performance
 - **1~2** = Licensee needs to investigate & make appropriate corrective actions
 - **3 or more** = Licensee needs to investigate, make appropriate corrective actions & adjust program to eliminate future performance deficiencies

□ CS Performance Measure Cases

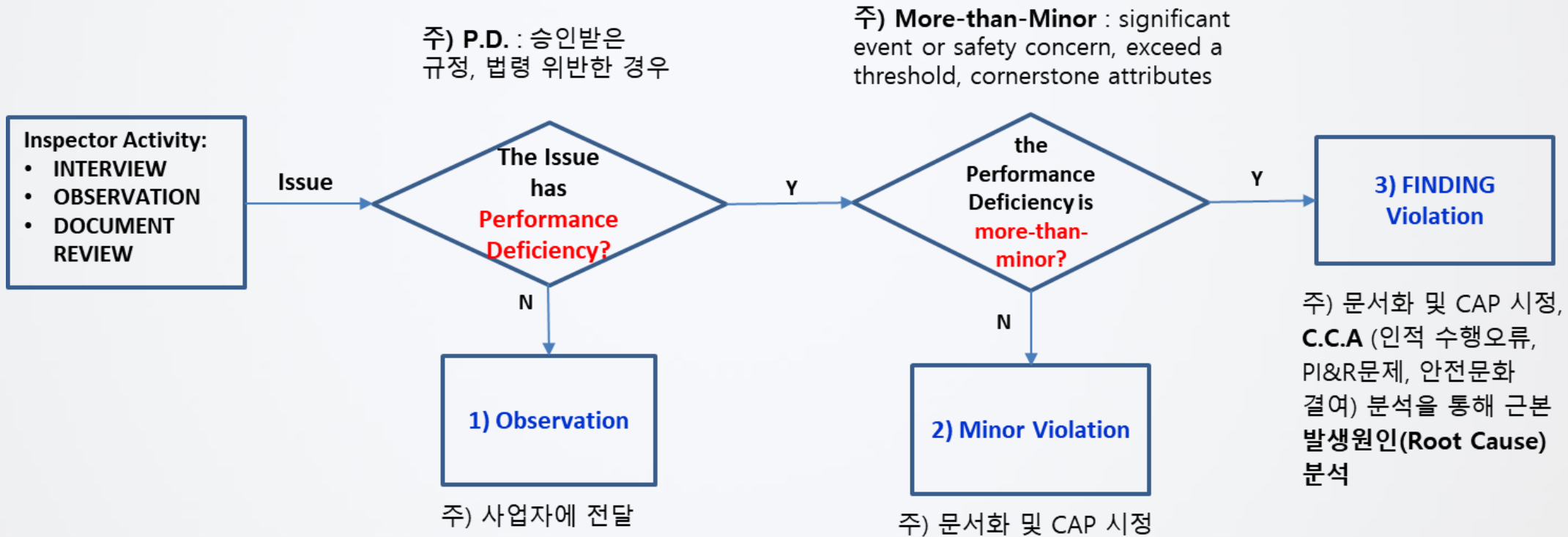
❖ Performance Metrics


Table I: Performance Metrics

Control Classification	Good Performance	Corrective Action	Performance Deficiency
Access control	0	1-2	3 or more
Third-party	0-1	2	3 or more
PMMD connected	0-1	2	3 or more
Security flaws	0-1	2-3	4 or more
Config. change	0-1	2-3	4 or more
Mal. code	0-1	2-3	4 or more
Periodic scan	0	0~1%	> 1%
Security func.	0-1	2-3	4 or more
Training	100-95%	94-90%	< 90%
Open port	0-1	2-3	4 or more

□ CS Performance Measure Cases

❖ Performance Metrics





Q&A

Thank you for your attention
