J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

K-RMF 적용 연구개발사업 보안계획서 작성 방법 제안 연구

A Research on the Method of Writing a Security Plan for K-RMF Applied Research and Development Projects

이 원 영[1*]
Won-Young Lee

요 약

미국의 RMF(Risk Mangement Framework)는 정보기술(IT)을 수반하는 모든 국방체계의 수명주기 동안 보안위험을 관리하는 국방성 통합보안관리제도이다. 한편 최근에는 국방부의 국방 사이버보안 위험관리 지시를 근거로 2024년 7월부터 적용 예정인 K-RMF의 연구개발사업 적용 효율화를 위한 보안계획서 작성 방법의 연구 필요성이 요구되고 있다. 따라서 본 논문은 기존 RMF 보안계획서와 현행 방첩사 보안대책서를 기반으로 K-RMF 보안계획서 구성 목차와 포함되는 내용을 제안한다. 아울러 세부적인 연구내용은 다음과 같다. 첫째, 국외 RMF 보안계획서 사례와 국내 방첩사의 보안대책서 구성목차를 검토한다. 둘째, 체계 위험관리를 위한 K-RMF 보안평가에서 점검이 필요한 내용을 식별하여 정의하고 업체주관 체계개발사업을 예시로 적용한다. 셋째, 제안하는 연구내용은 전문가 자문회 및 사이버보안 워킹그룹을 통해 그 적절성을 입증할 것이다. 마지막으로 본 연구결과는 K-RMF 적용에 대한 주요 산출물 연구의 첫 시도라는 점에서 중요하며, 앞으로 개발될 보안계획서 유사 산출물의 기초자료로 활용이 기대되고 K-RMF 보안 평가 기준의 토대가 될 것이라 기대된다.

☞ 주제어 : 한국형 사이버보안제도, 보안계획서, 무기체계 보안계획서, 사이버보안

ABSTRACT

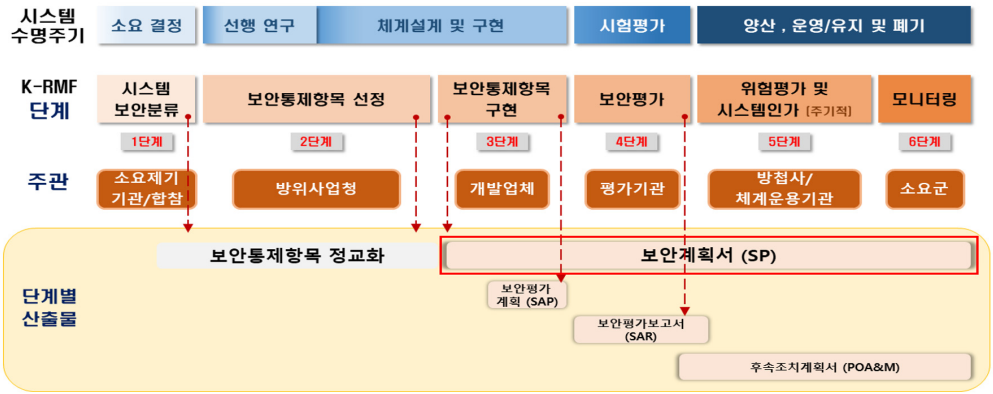
In the United States, RMF is U.S. Department of Defense's integrated security management system that manages security risks throughout the life cycle of all defense systems involving information technology. Recently, it is required researching on how to write a security plan frame for efficient application of the K-RMF, which is scheduled to be applied from July 2024, based on U.S. Department of Defense Cybersecurity Risk Management Directive of the Ministry of Defense in Republic of Korea. Therefore, in this paper, we propose the contents of the K-RMF security plan based on the existing RMF security plan and the current Counter-intelligence security plan. In addition, the detailed research contents are as follows. First of all, we review the cases of foreign RMF security plan and the contents of domestic Counter-intelligence security plan. Second, the contents that need to be checked in the K-RMF security assessment for system risk management were identified and defined, and vendor organized system development project was applied as an example. Third, the proposed contents were validated through the expert advisory commission and cyber security working group. Finally, this study is important in that it is the first attempt to study major document for the application of K-RMF, and it is expected to be utilized as a basis for similar deliverables of the security plan to be developed in the future and to serve as a foundation for K-RMF security evaluation criteria.

☞ Keyword: K-RMF, RMF, Security plan, Weapon system security plan, Cyber security

1. 서 론

디지털 의존도가 높아짐에 따라 정보의 생성과 유통량이 폭증하여 소프트웨어 공급망에 대한 위협 즉, 사이버 영역의 위험관리 중요성이 강조되고 있다. 실제로 2023년 상반기 사이버 침해사고는 작년 대비 약 40% 증가했으며, 단순한 금융 범죄를 넘어 국가적 안보에 직접적인 영향을 미치는 사이버 위협이 증가하고 있다[1]. 미국은 2014년부터 국가적 사이버보안 통합대책으로 RMF(Risk Management Framework)[2, 3, 4, 5, 6]를 개발하여 군에서 의무적으로 사용하고 있으며, 이 외에도 기업, 산업, 학계 등 다양한 분야에서 적용중이다[7]. 특히 미국 국방부는 2019년에 한미 연합체계에 RMF에 준하는 보안제도를 적용할 것을 요구하여 우리 국방부는 군 보안업무 환경을 고려한 한국형 사이버보안제도(K-RMF)를 개발하였다.

1 AI·Cyber Team, Defense Agency for Technology and Quality, Daejeon, 35409, Korea.
* Corresponding author (wylee@dtaq.re.kr)
[Received 9 July 2024, Reviewed 22 July 2024(R2 20 September 2024), Accepted 14 October 2024]



(그림 1) 시스템 수명주기별 K-RMF 단계별 산출물
(Figure 1) Required K-RMF document per system life cycle stage

K-RMF는 무기체계 소요제기부터 폐기까지 총 수명주기 동안 단계별 보안통제를 수행하여 보안위험을 관리하는 통합보안관리제도이다. 먼저 체계 내 생성·유통·저장되는 데이터를 고려하여 시스템 보안분류를 결정하고 체계 특성을 반영하여 보안통제항목을 가감한다. K-RMF 단계별 산출물 생성과정은 [그림 1]과 같이 총 6단계 프로세스로 수행되며 시스템 보안분류, 보안통제항목 선정, 구현, 평가, 시스템 위험평가, 모니터링 순으로 구성되어 단계별 산출물이 작성된다. [그림 1]과 같이 다양한 산출물이 요구되지만 그 중에서도 보안계획서(Security Plan)는 여러 단계에 걸쳐 지속적인 최신화와 승인이 필요한 산출물이다.

하지만 2021년부터 2022년까지 업체주관 체계개발사업을 대상으로 K-RMF 시범적용을 수행한 결과, 개발업체에서 보안계획서 작성을 가장 어려워한 바 있다. 이에 국방기술품질원(이하 기품원)에서 K-RMF의 성공적인 정착을 위해 2022년부터 업체주관 연구개발사업을 대상으로 보안계획서 작성방안, 보안통제항목 분석 등 기술지원 방안을 연구하고 있다. 아울러 기존의 현행 규정과 가이드가 갖고 있는 문제점을 요약하면 다음과 같다. 첫째, 우리 군의 국방정보시스템 도입 및 개발절차에 대규모 소프트웨어를 개발할 경우 시큐어 코딩 적용, 취약점 평가를 비롯한 보안대책 준수 여부 점검 등 보편적인 수준으로 기술 특성을 고려한 체계적인 제도화가 필요하다[8]. 둘째, 사이버 보안은 체계 운용에서 매우 중요한 고려사항이지만 기존의 사이버 보안 시스템은 단차원적인 정보통신망에 의존하고 있어 보안시스템 패치 또는 업그레이드를 지속하기 어렵고 공급망 보안 관리체계 부재 등 으로 보안 취약점이 존재한다[9]. 셋째, 드론 및 센서 장비와 같이 극한의 전장 환경에 투입, 배치되는 군 전술무인체계는 상위 지휘관 입회 하의 원격제어 형태로 운용되어 외부 대항군 사이버 공격 시 즉각적인 위협 대응에 어려움이 있다[10].

따라서 본 논문의 목표는 기존 RMF 보안계획서와 현행 국군방첩사령부(이하 방첩사) 보안대책서를 기반으로 K-RMF 보안계획서 구성 목차와 작성 내용을 제안하는 데에 있다. 본 논문의 세부적인 연구내용은 다음과 같이 요약된다.

1. 본 논문은 미국의 RMF를 벤치마킹한 K-RMF 적용 시 요구되는 보안계획서 작성방안을 제안하는 연구로 미국 RMF 보안계획서 사례와 현행 방첩사 보안대책서를 검토한다.
2. 현행 사례를 검토한 결과를 반영하여 공통으로 요구하는 항목과 핵심적으로 작성이 필요한 항목을 식별하여 보안계획서 목차를 목록화하고 목차별 작성내용을 구성한다.
3. 구성된 보안계획서 작성양식에 맞추어 MOOO 체계를 예시로 보안계획서 사례를 작성하여 연구의 적절성을 확인한다.
4. 보안계획서 작성 양식과 업체주관 체계개발사업 적용 사례를 안건으로 사이버보안 워킹그룹을 개최하여 전문가 자문을 통한 적절성 및 타당성을 검증한다.
5. 끝으로 본 연구결과는 K-RMF 적용에 대한 주요 산출물 연구의 첫 시도라는 점에서 중요하며 앞으로 개발될 유사 산출물의 기초자료로 활용이 기대되며 K-RMF 보안평가 기준의 토대가 될 것으로 예상한다.

2. 관련연구

2.1 NIST* SP 800-18

NIST(미국 국립표준기술연구소)가 연방 정보시스템에 대한 RMF 보안계획서 작성을 위해 제시한 지침으로 오래된 지침이지만 현행 규정 및 가이드에 꾸준히 인용되고 있다[6, 7]. 2021년 5월 미국 바이든 행정부가 시행한 행정명령(EO14028)인 국가 사이버보안 증진을 위한 소프트웨어 공급망 보안 강화 관련 내용도 해당 문서에 나와 있다[8]. NIST RMF는 사이버 보안 측면에서 주로 시스템 수준의 표준화된 위험관리에 중점을 둔다면 미국 국방부 RMF(DoD RMF)는 조직과 임무 수준의 위험분석까지 확장한 고수준의 위험관리 개념이다[9]. NIST SP 800-18의 부록A에서 요구하는 목차는 [표 1]과 같으며, 이를 기준으로 다른 사례를 비교한다.

(표 1) NIST SP 800-18 보안계획서 작성목차
(Table 1) NIST SP 800-18 Security Plan Contents

순	구분	주요내용
1	정보시스템 명칭	체계명
2	정보시스템 보안분류	기밀성(C), 무결성(I), 가용성(A)에 대한 상, 중, 하 단계 예) 중-상-상
3	정보시스템 소유자	이름, 소속, 주소, 이메일, 연락처 등
4	인가권자	이름, 소속, 주소, 이메일, 연락처 등
5	기타 업무별 담당자	담당자별 이름, 소속, 주소, 이메일, 연락처 등
6	보안책임자	이름, 소속, 주소, 이메일, 연락처 등
7	정보시스템 작동상태	운영중, 개발중, 변경중 中 작성
8	정보시스템 분류	핵심응용체계 또는 일반지원체계
9	시스템 개요 및 목적	시스템 목적, 정보처리 절차, 주요기능 등
10	운용환경	주요 하드웨어, 소프트웨어, 통신장비를 포함한 기술적 구현사항 설명
11	시스템 연동 및 정보 공유	연동체계 목록, 종류, 관련 조직, 체계별 인가기관, 연동 합의근거 등
12	관련 법규 및 정책	체계 C, I, A 관련 법, 규정, 정책
13	보안통제항목 기준선	NIST SP 800-53에 따른 보안통제항목 목록으로 보안통제항목 명칭, 구현상태, 구현시 고려사항, 구현책임자 등

* National Institute of Standards and Technology

2.2 NISP**

NISP는 미국의 국가방위산업 보안 프로그램으로 민간 산업계가 기밀정보에 접근하기 위해 준수해야 할 관리준칙이다. NISP에서 요구하는 보안계획서 목차는 [표 2]와 같다. NIST SP 800-18의 목차를 기준으로 보안 평가계획이 추가되고 정보시스템 작동상태, 정보시스템 분류, 관련 법규 및 정책 항목이 누락되었다.

(표 2) NISP 보안계획서 작성목차
(Table 2) NISP Security Plan Contents

순	구분	주요내용
1	시스템 식별	시스템 개요, 보안분류, 적용된 오버레이 종류
2	주요 역할 및 책임	담당자별 인적사항 예) 인가책임자, 정보소유자, 평가자별 이름, 소속, 주소, 전화번호, 이메일 등
3	시스템 환경	물리적 환경, 시설, 데이터 취급 요구사항, 정보접근 정책
4	시스템 개요 및 목적	시스템 개요, 아키텍처, 기능적 구조, 사용자 역할 및 권한
5	시스템 내부 연결구조	직접 연동체계, 관련 근거 (MOU, MOA, CUA, ISA 등)
6	보안 평가계획	공식 평가수단 또는 필요시 추가 평가수단 예) DISA의 취약성 확인도구 STIG Viewer, SCAP 체커 등
7	보안통제항목 기준선	선정된 보안통제항목, 구현현황, 적용 시스템 종류(공통 등)

2.3 DoD DHA***

DoD DHA는 미국의 국방성 보건국에서 NIST SP 800-53을 기반으로 정보흐름에 대한 기밀성, 무결성, 가용성을 확보하고자 RMF를 수행하고 있다. DHA의 보안계획서 목차는 [표 3]과 같다. NIST SP 800-18을 기준으로 정보시스템 작동상태, 정보시스템 분류, 관련 법규 및 정책 항목이 누락되었다.

** National Industrial Security Program
*** Defense Health Agency

(표 3) DHA 보안계획서 작성목차
(Table 3) DHA Security Plan Contents

순	구분	주요내용
1	시스템 개요	Identifies the system.
2	시스템 보안분류 결과	Describes the system categoriazation in accordance with CNSSI1253.
3	시스템 Owner 정보	Identifies the system owner and provides contact information.
4	인가권자	Identifies the authorizing official.
5	그 밖의 권한 담당자	Identifies other desinated contacts.
6	보안책임 담당현황	Identifies the assignment of security responsibility.
7	정보체계 종류	Identifies the type of information system.
8	정보체계 운영현황	Identifies the operational status of the information system.
9	정보체계 운영환경	Describes the information system environment.
10	타 정보체계와 연동관계	Identifies interconnections between other information system.
11	보안통제항목 구현설명	Provides an in-depth description of how each security control is implemented.

2.4 FedRAMP

FedRAMP는 클라우드 제품 및 서비스에 적용되는 보안평가, 인증 및 지속적인 모니터링의 표준화된 방법을 제공하는 프로그램으로 민간 산업계가 기밀정보에 접근하기 위해 준수해야 하는 관리 준칙이다. FedRAMP의 보안계획서 목차는 [표 4]와 같다. NIST SP 800-18을 기준으로 정보시스템 유형, 약어목록과 시스템 사용자 가이드와 침해사고 계획 등 여러 붙임파일들이 추가되었지만, 인가 및 보안책임자 외 업무담당자 정보와 정보시스템 분류 항목은 누락되었다.

2.5 North Carolina Department of Information Technology(IT)

미국 North Carolina 주 정보기술부에서 정보보안교육의 일환으로 활용했던 양식이다. NIST SP 800-53과 800-39 등을 기반으로 RMF 보안통제항목을 사용하며 요구내용 및 기준이 같다. North Carolina Department of Information Technology의 보안계획서 목차는 [표 5]와 같다. NIST SP 800-18을 기준으로 정보시스템 인가권자 및 보안책임자 정보, 정보시스템 작동상태, 관련 법규 및 정책 항목이 누락되었다.

(표 4) FedRAMP 보안계획서 작성목차
(Table 4) FedRAMP Security Plan Contents

순	구분	주요내용
1	정보시스템 명칭	정보시스템 식별ID, 공식명칭, 축약명칭, 소요군, 운영지역, 관리번호 기재
2	정보시스템 분류	NIST 800-60에 의한 정보유형, 식별번호와 기밀성, 무결성, 가용성에 대한 등급 예) Low, Moderate, High
3	정보시스템 보유조직/기관	정보시스템 보유조직 및 기관의 담당자 이름, 직책, 회사명, 주소, 전화번호, 이메일
4	인가책임관	인가책임관 이름, 직책, 회사명, 주소, 전화번호, 이메일
5	예비책임관	예비책임관 이름, 직책, 회사명, 주소, 전화번호, 이메일
6	보안책임관	보안책임관 이름, 직책, 회사명, 주소, 전화번호, 이메일
7	정보시스템 운영상태	정보시스템 운영상태(운영중, 개발중, 성능개량중, 기타) 中 택 1
8	정보시스템 유형	클라우드 서비스 모델, 모델, 레버리지 인증
9	정보시스템 개요	시스템 기능 및 목적, 시스템 구성요소 및 구간, 사용자 정의, 네트워크 구성
10	정보시스템 환경 및 인벤토리	하드웨어, 소프트웨어, 네트워크 목록, 데이터 흐름도, 통신 포트 및 프로토콜
11	시스템 연동 및 연결구조	시스템 IP주소별 해당 서비스, 데이터 전송방향, 통신포트
12	관련 법령, 규정, 지침	체계 보안분류와 관련된 법, 규정 및 정책
13	보안통제항목	선정된 보안통제항목
14	약어	약어목록
15	붙임1.	정보보호 정책 및 절차
16	붙임2.	사용자 가이드
17	붙임3.	디지털 인증시트
18	붙임4.	개인정보 영향평가
19	붙임5.	사용자 동의사항
20	붙임6.	정보시스템 배치계획
21	붙임7.	배치관리 계획
22	붙임8.	침해사고 계획
23	붙임9.	통제항목 구현요약
24	붙임10.	FIPS 199

(표 5) North Carolina Department of IT 보안계획서 작성 목차
(Table 5) North Carolina Department of IT SP Contents

순	구분	주요내용
1	정보시스템 보안계획 목적	정보시스템 구성요소, 운영구조, 보안 요구사항, 보안 관련 역할 및 책임
2	정보시스템 정의	정보시스템 명칭 및 분류, 소유자, 담당자, 예비담당자 정보
3	운영개념	정보시스템 개요 및 목적, 시스템 환경, 시스템 내부 연결구조, 정보흐름구조
4	보안통제항목 기준선	NIST SP 800-53에 따른 보안통제항목 목록 (명칭, 구현상태, 구현시 고려사항)

(표 6) 방첩사 보안대책서 작성목차
(Table 6) DCC**** Security Plan Contents

순	구분	주요내용
1	총괄	체계명, 체계분류, 사업명, 수명주기 단계, 보안대책 총괄, 보안측정(위험평가 결과) 총괄, 보안지원 결과
2	이력	체계사업 이력, 보안대책검토 및 보안측정 의뢰 및 결과
3	정보보호 요구수준	구성요소/구간별 이름, 사용기반망, 처리하는 정보, 정보등급, 정보처리형태, 적용 암호화 방법, 보호요구수준
4	망 연동	연동방식 및 장비명, 승인자, 연동구간, 책임자 정보
5	정보보호체계	정보보호체계별 인증종류 및 암호모듈 검증여부, 책임자 정보
6	체계 자산	하드웨어, 소프트웨어 목록, 책임자 정보
7	제안서 및 계약 필수요구	추가 보호통제항목, 구현방안 등, 책임자 정보
8	네트워크 보호통제항목	선정된 보호통제항목 목록, 구체적인 구현방안, 책임자 정보
9	서버 보호통제항목	선정된 보호통제항목 목록, 구체적인 구현방안, 책임자 정보
10	단말기 보호통제항목	선정된 보호통제항목 목록, 구체적인 구현방안, 책임자 정보
11	응용프로그램 보호통제항목	선정된 보호통제항목 목록, 구체적인 구현방안, 책임자 정보
12	보호관리 보호통제항목	선정된 보호통제항목 목록, 구체적인 구현방안, 책임자 정보
13	오버레이 항목	암호공통, 비밀정보, KCMVP, 무선랜, RFID, 전자우편, VoIP, 외주용역, 부대이전, 영외시설 국방통신망, 네트워크 장비, 저장장치, 군내 외부망(체계) 설치

2.6 국내 방첩사 보안대책서

현재 방첩사는 군사상의 각종 행위에 대한 보안상 유해사항을 사전에 예방 또는 통제하기 위해 국방보안업무훈령, 국방사이버안보훈령, 국방전력발전업무훈령 등 여러 훈령을 근거로 보안대책검토, 보안적합성검증 등 다양한 보안제도를 수행한다. 이에, 각 군 및 기관은 국방사이버안보훈령에 의거하여 정보시스템 도입 시 보호대책수립을 위한 보안대책서를 마련해야 한다. 특히 보안대책서는 국방보안업무훈령 별지 제42호 서식을 기반으로 국방보안업무훈령, 국방사이버안보훈령, 국방정보보안시스템 업무훈령 외 지침 및 가이드 등에서 중복내용을 제거하여 약 220개 보호통제항목으로 구체적인 보안대책을 요구한다. 방첩사 보안대책서 목차는 [표 6]과 같다. NIST SP 800-18과 유사한 수준의 시스템 정보를 요구하지만 다양한 보안제도들이 개별적으로 시행되고 국방획득주기와 연계성이 없는 등 체계적인 보안관리가 어려운 실정이다[10]. 그러므로 K-RMF 적용 무기체계 보안계획서를 통해 여러 국방부 훈령에 산재한 보안 요구사항과 불필요하게 많은 내용을 요구하는 보안제도의 문제점을 개선하고자 한다.

**** Defense Counter-intelligence Command

3. K-RMF 보안계획서 구성요소

3.1 K-RMF 보안계획서 목차

미국의 보안계획서 목차와 현행 방첩사 보안대책서 등을 참고하여 공통적인 항목들을 선별하여 [표 7]과 같이 K-RMF 보안계획서 목차를 구성한다.

(표 7) K-RMF 보안계획서 목차
(Table 7) K-RMF Security Plan Contents

순	구분	주요내용
1	문서이력	버전별 수정일자 및 승인일자 작성
2	관련근거	보안계획서 작성 근거
3	시스템 개요	보안대책서 “1. 총괄” 내용
4	시스템 분류	소요결정문서, 선행연구 조사·분석 보고서 “시스템 보안분류 결과”
5	시스템 인가	인가현황 외 관련 정보
6	주요 업무별 보안책임자	보안대책서 “1. 총괄” 및 “4. ~7. 분야별 책임자”
7	시스템 환경	보안대책서 “1. 총괄” 및 ORD 등 사업 산출물 “시스템 운용환경” 활용
8	시스템 연동 및 연결구조	보안대책서 “4. 망연동” 내용
9	보안통제항목	시스템 보안분류 결과에 따라 선정 및 Tailoring된 보안통제항목
붙임	1.보안환경	(신규작성) 시스템 적용 보안환경
붙임	2.암호기술	시스템 적용 암호기술 현황
붙임	3.자산현황	(신규작성)자산별 정보 및 담당자

(표 7) K-RMF 보안계획서 목차(계속)
(Table 7) K-RMF Security Plan Contents

순	구분	주요내용
붙임	4.인증현황	보안적합성검증 및 CC인증 현황
붙임	5.시스템 간 정보흐름 및 연동동의서	(신규작성)시스템 간 주요 정보흐름 및 연동체계 간 연동합의서
붙임	6.보안통제항목 목록	(신규작성)보안통제항목 오버레이 및 테일러링 사유
붙임	7. SW범주	(신규작성)품목별 상용SW 정보
붙임	8.자산관리	(신규작성)시스템 구성 WBS별 정보
붙임	9. 프로토콜, 포트, 서비스	(신규작성)시스템 구성현황
붙임	10.사용자분류	(신규작성)운용조직 사용자 정보

각 목차별 세부내용 및 참고산출물은 다음과 같다.

1. 시스템 개요 : 시스템에 대한 이해도 제고를 위한 기본적인 내용으로 운용개념, 주요기능 등을 작성하며 이는 운영요구서(ORD), 선행연구 결과보고서 등을 참고하여 작성한다.
2. 시스템 분류 : 시스템 내 생성, 가공, 유통, 저장하는 데이터별 보안영향수준인 기밀성, 무결성, 가용성에 대해 상, 중, 하로 분류하여 최상위 레벨을 시스템 보안부류 레벨을 확정한다. 이는 소요결정문서 및 선행연구 조사·분석 보고서 등을 참고하여 작성한다.
3. 시스템 인가 : 시스템 인가시 작성하며, 인가권자, 인가범위 등 인가정보를 작성한다.
4. 주요 업무별 보안책임자 : 시스템 보안 관련하여 주요 업무별 담당자 정보를 작성하고 담당자가 변경될 때마다 최신화가 필요하다.
5. 시스템 환경 : 시스템에 대한 물리적, 관리적, 기술적 환경을 기술하며 개발단계별 보안대책 등 개발환경을 작성한다. 이는 제안요청서 및 체계개발실행계획서(SDEP)를 참고하여 작성한다.
6. 시스템 연동 및 연결구조 : 네트워크, 시스템, 정보보호체계 등 구성도 및 구성내용을 작성하며 이는 인터페이스 설계기술서(IDD) 등 시스템 개발 산출물을 참고하여 작성한다.
7. 보안통제항목 : 방첩사에서 배포 예정인 보안통제항목 가이드를 활용하여 작성하며 2. 시스템 분류에서 결정된 시스템 보안분류 기준선에서 시스템 특성에 따라 테일러링 또는 오버레이 작업을 거친 최종적으로 선정된 보안통제항목별 구현계획을 작성한다.

3.2 보안계획서 목차별 작성 시기 및 기관

앞의 서론에서 언급한 바와 같이 K-RMF는 보안 내재화를 이루기 위해 연구개발사업 전 주기에 거쳐 적용이 필요하다. 하지만 사업 추진간 효율적인 작성을 위해 사업착수를 기준으로 전/후로 구분하고, 사업착수 후는 사업 착수회의 이후 상세설계검토회의(이하 CDR*****)까지를 의미한다. 이는 기존 보안대책서를 포함한 대부분의 연구개발사업 산출물이 CDR시점에 확정되는 것을 반영한 것이다. 그 외 사업 진행현황 또는 담당자 변경 등 수정사항이 있을 때마다 최신화가 필요한 항목은 변동시로 구분한다. 또한 작성 기관은 착수회의 및 인가시점을 기준으로 크게 소요기관, 사업기관, 개발기관, 운용기관으로 구분하며 그 정의는 다음과 같다.

1. 소요기관 : 대상 체계의 소요를 제기한 기관
2. 사업기관 : 사업을 진행하는 기관(예 : 방사청)
3. 개발기관 : 대상 체계개발을 주관하는 기관(예 : 방산업체)
4. 운용기관 : 대상체계를 운영하는 기관(예 : 군부대)

결과적으로 K-RMF 적용 사업의 보안계획서 작성 구성과 목차별 작성 시기 및 기관은 [표 8]과 같다.

(표 8) 보안계획서 목차별 작성 시기 및 기관
(Table 8) Writing contents point and organization

순	구분	작성시기	작성기관
1	시스템 개요	사업착수 전	소요기관, 사업기관, 개발기관
2	시스템 분류	사업착수 전	소요기관
3	시스템 인가	변동시	소요기관
4	주요 업무별 보안책임자	변동시	소요기관, 사업기관, 개발기관, 운용기관
5	시스템 환경	사업착수 후	개발기관
6	시스템 연동 및 연결구조	사업착수 후	개발기관
7	보안통제항목	사업착수 후	소요기관, 사업기관, 개발기관
붙임	1.보안환경	사업착수 후	사업기관, 개발기관
붙임	2.암호기술	사업착수 후	사업기관, 개발기관
붙임	3.자산현황	사업착수 후	개발기관, 운용기관
붙임	4.인증현황	사업착수 후	개발기관
붙임	5.시스템 간 정보흐름 및 연동동의서	사업착수 후	사업기관, 개발기관

***** CDR : Critical Design Review

(표 8) 보안계획서 목차별 작성 시기 및 기관(계속)
(Table 8) Writing contents point and organization

순	구분	작성시기	작성기관
붙임	6.보안통제항목 목록	사업착수 후	소요기관, 사업기관, 개발기관
붙임	7. SW범주	사업착수 후	개발기관
붙임	8.자산관리	사업착수 후	개발기관,
붙임	9. 프로토콜, 포트, 서비스	사업착수 후	개발기관
붙임	10.사용자분류	사업착수 후	개발기관, 운용기관

4. 보안계획서 작성예시를 통한 적절성 검증

본 논문에서 제안하는 보안계획서 구성 목차에 지휘통제통신체계(C4I) 연구개발사업인 MOOO 체계를 대상으로 보안계획서 예시를 작성하였다. 이를 안건으로 사이버 워킹그룹을 개최하여 K-RMF 관련 정책기관, 민간 공인 인증시험 종사자 등 산·학·연 보안평가 전문가 자문을 통해 연구결과의 적절성과 타당성을 확보하였다.

기품원의 K-RMF 업무절차 및 방법의 공신력 확보를 위한 사이버보안 전문가 워킹그룹을 1, 2차 진행하였다. 전문가 그룹은 20명 내외로 국방부, 방사청, 한국국방연구원 등 국방분야 전문가와 CC인증 등 민간 보안인증을 수행하는 전문가, 체계 개발을 주관하는 방산업체 등으로 구성하였다. 초기 연구산출물을 안건으로 워킹그룹을 수행하였고, 전문가 자문의견을 반영하여 본 논문으로 구체화하였으며, 주요 자문의견은 다음과 같다.

- 자문의견 1 : 체계 수명주기의 주요 의사결정 단계에서 보안계획서 내용 구체화 및 SE단계별 작성시기 구체화 필요

⇨ 작성시기를 고려하지 않은 보안계획서 초안을 개선하여 CDR 시점까지 작성될 수 있도록 보안계획서 목차별로 작성시기와 작성기관을 분류하였다.

- 자문의견 2 : 타 체계 상속 또는 활용항목 명시 필요

⇨ K-RMF 관점에서 유사체계 상속 또는 누적된 K-RMF 산출물을 활용할 수 있도록 향후 연구방향에 반영할 예정이다.

- 자문의견 3 : 시험평가 기본계획서 등 체계 산출물과 유기적 관계 고려가 필요하며, 보안계획서 최종승인권 명확화가 필요함

⇨ K-RMF의 효율적인 적용방안을 위한 기존 산출물 간 연계성 검토 필요성을 인지하였으며, 추후 K-RMF 관리도구 개발 시 보안계획서 최종승인권자를 명확히 하기 위한 정책적 제언이 필요하다.

- 자문의견 4 : 보안통제항목 요구사항 내 매개변수 구체화가 필요하고, 요구사항 추적이 가능하도록 관련 산출물과 링크 형성이 필요함

⇨ K-RMF 시범적용 사업을 통해 단계별 보안계획서 발전 방향 및 매개변수 구체화 예정이다.

- 자문의견 5 : 보안계획서 상세이력 작성 및 관리 필요

⇨ 보안계획서 목차에 문서이력을 추가하여 최초 문서 작성 시 0.1버전을 시작으로 계획 수정시 0.1단위로 버전을 갱신하고 인가권자의 검토 및 승인을 받은 경우 1.0 단위로 버전을 갱신할 것을 가이드에 명시하였다.

- 자문의견 6 : 보안통제항목 구현상태(구현, 부분구현, 미구현 등)에 따른 후속관리로 후속조치계획서에 반영 필요함

⇨ 보안계획서 7장에서 보안통제항목 구현상태가 구현예정, 대체구현, 미구현 등 관리가 필요한 항목에 대해 후속조치계획서 등 위험관리 및 지속적인 모니터링 방안 구체화 연구의 필요성을 인지하였다.

5. 결론 및 향후 연구과제

본 논문에서는 무기체계의 보안위험 완화를 위해 도입되는 K-RMF 제도의 안정적인 도입을 위한 보안계획서 작성방안을 제안하였다. 체계 수명주기 간 지속적인 최신화가 필요한 보안계획서를 연구개발 시점별 작성기관 및 세부내용을 기술하였다. K-RMF 시범적용을 통해 개발업체가 보안계획서 작성에 어려움을 호소함에 따라 배포 가능한 수준의 작성 가이드와 사례를 작성하여 전문가 자문을 통한 적절성을 검증받았다.

본 연구를 통해 효율적인 K-RMF 적용을 위한 기존 STIG 표준 기반의 연구개발주관기관(방산업체) 소프트웨어 데이터 관리시스템과 유사한 K-RMF 관리도구의 필요성을 인지하였고 보안계획서 작성 시 유사체계의 산출물을 활용할 수 있는 방안을 연구할 예정이다.

국방부에서 제정한 국방 사이버보안 위험관리 지시[16]의 시행에 따라 기품원의 임무로 부여받은 위험관리 효율화를 위한 정책 및 제도 발전 지원과 업체 주관 연구개발사업의 보안계획서 작성, 보안통제항목 구현 점검 지원 방안 등 효율적인 위험관리 적용을 위한 기법 발전에 노력할 것이다. 또, 지시에 의해 위험관리 제도가 C4I체계를 대상으로 우선 적용하고 점차 확대 적용됨에 따라 그에 맞는 산출물 활용방안 연구를 수행할 예정이다.

참고문헌(Reference)

[1] One-Sun Cho, “Expanding the surface of cyber attacks and changing the security paradigm : AI-driven preemptive security threat identification and resilience,” Future Horizon, Vol. 56, No. 2-3, pp. 44-51, 2023. https://www.stepi.re.kr/site/stepiko/PeriodicReportView.do?reIdx=62&pageIndex=1&cateCont=A0505&searchYear=&searchCondition=2&searchKeyword=%EC%A1%B0%EC%9B%90%EC%84%A0&searchSort=PUBLIC_DT

[2] In Lee, “Cybersecurity: Risk management framework and investment cost analysis,” Business Horizons, Vol. 64, Issue 5, pp.659-671, 2021. https://doi.org/10.1016/j.bushor.2021.02.022

[3] Micheline J. Naude and Nigel Chiweshe, “A proposed operational risk management framework for small and medium enterprises,” SAJEMS, Vol. 20, No. 1, Mar. 2017. https://doi.org/10.4102/sajems.v20i1.1621

[4] X. Zhang, N. Wuwong, and H. Li, “Information Security Risk Management Framework for the Cloud Computing Environments,” 2010 10th IEEE International Conference on Computer and Information Technology, pp.1328-1334, 2010. https://doi.org/10.1109/CIT.2010.501

[5] Amaghionyeodiwe and Lloyd Ahamefule, “Risk Management Framework (RMF) and the Implementation Challenges,” Proceedings of the Northeast Business & Economics Association, pp.11-14, 2017. https://openurl.ebsco.com/EPDB%3Agcd%3A13%3A22382861/detailv2?sid=ebsco%3Aplink%3Acrawler&id=ebsco%3Agcd%3A134235235

[6] Hyun-suk Cho, Sung-yong Cha, Seung-joo Kim, “A Case Study on the Application of RMF to Domestic Weapon System,” Jounal of the Korea Institute of Information Security & Cryptology, Vol. 29, Issue 6, pp.1463-1475, 2019. https://doi.org/10.13089/JKIISC.2019.29.6.1463

[7] Sang-Hun Na, Tae-Shik Shon, “A Study on the Development of Information Security Management System Using RMF,” JDCS, Vol.23, No. 5, pp.977-983, May, 2022. https://doi.org/10.9728/dcs.2022.23.5.977

[8] Gyu-do Park, Young-ran Lee, “A Methodology for SDLC of AI-based Defense Information System,” Journal of the Korea Institute of Information Security & Cryptology, Vol.33, No.3, pp.577-589, 2023. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10304133

[9] Sun-Wong Kim, Jae-Su Park, Sang-Hun Nam, Seong-Kwon Kwak, “Research on the Future of Satellite Cybersecurity in the Defense Sector,” Defense & Technology, No. 542, pp.122-129, 2024. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11746297

[10] Sang Seo, Sunho Lee, Heaeun Moon, Byeongjin Kim, Jaeyeon Lee, Dohoon Kim, “Utilization of Cyber Deception for Next-Generation Defense Digital Security,” Korea Institute of Information Technology Magazine, Vol. 20, No.1, pp.1-11, 2022. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11179612

[11] DoD Instruction 8510.01, “RMF for DoD Information Technology,” Dec, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[12] NIST SP 800-37 Revision 2, “Risk Management Framework for Information Systems and Organizations,” Dec. 2018. https://csrc.nist.gov/pubs/sp/800/37/r2/final

[13] Sang-Jun Lee, “National Defense Software Security,” Communications of the Korean Institute of Information Scientists and Engineers, Vol.41, No.3, pp.17-26, 2023. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11225048

[14] Seung-Bae Lee, “Changes in U.S. Defense Technology and Project Protection Policy to Enhance Cybersecurity,” Defense & Technology, No.502, pp. 104-111, 2020. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10496905

[15] W. Yang, S. Cha, et. al., “Korean Security Risk Management Framework for the Application of Defense Acquisition System,” Journal of the Korea Institute of Information Security & Cryptology, Vol. 32, No. 6,

pp.1183-1192, Dec. 2022.
http://dx.doi.org/10.13089/JKIISC.2022.32.6.1183
[16] Directive of the Ministry of Defense in Republic of Korea 정보통신기반정책담당관, “국방 사이버보안 위험관리 지시,” April. 2024.
https://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000239594

◐ 저 자 소 개 ◑

이 원 영(Won-Young Lee)
2019년 홍익대학교 컴퓨터정보통신공학과(공학사)
2021년 홍익대학교 일반대학원 전자전산공학과(공학석사)
2020년~2021년 국방기술진흥연구소 미래전력선행연구팀 연구원 근무
2021년~현재 국방기술품질원 AI·사이버팀 연구원 재직
관심분야 : 국방품질경영, 사이버보안, K-RMF, 소프트웨어공학, 데이터베이스, etc.
E-mail : wylee@dtaq.re.kr