

원저

미국 국방 CSRMC 전환 신호의 제도화 성숙도 유형과 K-RMF 운영 모델 고도화 방안

김원태

군인공제회 C&C 사장

교신저자: 김원태 (iamhappyman@naver.com)

요약

본 연구는 미 국방부의 Cyber Security Risk Management Construct(CSRMC)와 Strategic Tenets를 차기 RMF 개편의 전환 신호로 해석하고, 이를 기반으로 K-RMF 운영 모델의 고도화 방안을 제시한다. 이를 위해 위험관리체계를 구조-운영 모델-규범의 3개 레이어와 거버넌스-기술-운영-적용 범위-성과의 4개 렌즈로 교차 분석하였다. 분석 결과, 차기 RMF의 제도화 방향은 운영 중심 COMMON 강화형(S1), 하이브리드 전환형(S2), 제한적 개선형(S3)으로 구조화되었다. 이를 준거로 K-RMF를 진단한 결과, COMMON 상시화와 운영 지표 연계, 자동화된 증빙 수집·검증, 평가 재사용·상호인정 및 통제 상속의 제도화가 핵심 과제로 도출되었다. 또한 정성적 다기준 정책평가와 기술·제도적 의존성 분석을 통해 단기 기반 구축, 중기 확산·정착, 장기 운영 중심 전환의 단계적 로드맵을 제시하였다. 본 연구는 공개된 전환 신호를 활용하여 제도 변화의 가능한 경로를 구조화하고, K-RMF를 운영 데이터 기반의 지속적 위험관리 체계로 전환하기 위한 정책적 설계 준거를 제시한다.

핵심어

CSRMC, K-RMF, 위험관리프레임워크, 지속적 모니터링, 지속적 보증, 자동화 증빙, 통제 상속, 제도화 성숙도

차례

1. 서론
2. 배경 및 비교 준거
3. 연구설계
4. 분석 틀의 설정
5. CSRMC 신호 기반 차기 RMF 제도화 성숙도 유형과 K-RMF 갭 분석
6. 구조화된 정성적 우선순위 평가와 K-RMF 발전 로드맵
7. 결론

Open Access

접수일: 2026년 7월 16일
수정일: 2026년 9월 02일
게재승인일: 2026년 9월 08일
출판일: 2026년 9월 30일

Copyright © 2026 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

Institutionalization Maturity Types of U.S. DoD CSRMC Transition Signals and Recommendations for Advancing the K-RMF Operating Model

Weontae Kim

President, Military Mutual Aid Association C&C, Republic of Korea

Corresponding Author: Weontae Kim (iamhappyman@naver.com)

ABSTRACT

This study interprets the U.S. Department of Defense's Cyber Security Risk Management Construct (CSRMC) and Strategic Tenets as transition signals for the evolution of the Risk Management Framework (RMF) and proposes an advanced operating model for K-RMF. A "3-Layer × 4-Lens" framework is applied across Architecture, Operating Model, and Norms through Governance, Technology/Operations, Scope, and Performance. The analysis identifies three institutionalization maturity types: an operations-centered CONMON enhancement type (S1), a hybrid transition type (S2), and a limited improvement type (S3). Based on these types, key priorities for K-RMF include continuous CONMON linked to operational metrics, automated evidence collection and validation, and institutionalization of assessment reuse, reciprocity, and control inheritance. Qualitative multi-criteria policy assessment and dependency analysis further provide a phased roadmap for foundation building, expansion and institutionalization, and transition to an operations-centered model. This study provides policy design criteria for transforming K-RMF toward operational-data-driven continuous risk management.

KEYWORDS

CSRMC, K-RMF, Risk Management Framework, Continuous Monitoring, Automated Evidence, Control Inheritance, Institutionalization Maturity

1. 서론

1.1. 연구 배경

국방 분야의 디지털 전환은 무기체계의 소프트웨어화, 지휘통제 체계의 네트워크 의존 심화, 인공지능·클라우드 기반 기능의 확산을 동반하며, 사이버 위험을 단순 정보 유출의 문제가 아니라 작전 지속성과 전력화 속도를 동시에 좌우하는 거버넌스 과제로 전환시키고 있다. 미 연방정부와 국방부는 연방 정보보안 현대화법인 FISMA(Federal Information Security Modernization Act, 이하 FISMA) 및 미 국립표준기술연구소 NIST(National Institute of Standards and Technology, 이하 NIST) 위험관리프레임워크(Risk Management Framework, 이하 RMF), 미 국방부 지시 DoDI 8510.01 등을 기반으로 위험관리 절차를 제도화해 왔으나, 기존 RMF가 절차와 문서화 중심으로 운영되면서 신속한 개발 및 전력화 과정에서 운용 승인(Authorization to Operate, 이하 ATO)의 지연과 운영 현실 반영에 한계가 누적되었다는 비판이 제기되어 왔다.[1,2]

이러한 문제의식 하에서 미 국방부는 RMF를 단순하게 개정하기보다, 위험관리의 작동 방식 자체를 ‘승인 이벤트 중심’에서 ‘운영 중심의 지속적인 위험관리’로 재설계하는 방향을 공개 자료 형태로 제시하였다. 대표적으로 사이버보안 위험관리 구성개념(Cyber Security Risk Management Construct, 이하 CSRMC)과 Strategic Tenets는 ‘설계(Design)–구축(Build)–시험(Test)–도입(On board)–운영(Operations)’의 수명주기 구조 및 전략 원칙을 통해 위험관리를 전 주기에 내재화하고, 자동화 및 지속 모니터링(Continuous Monitoring, 이하 COMMON), 통제 상속과 평가 재사용 및 상호인정 등을 강조함으로써 향후 RMF 개편이 지향할 제도화 방향을 ‘전환 신호’의 형태로 보여준다.[3]

본 연구는 기존의 위험관리 연구가 확정된 미국 제도의 사후 도입이나 단순 절차 비교에 치우쳤던 것과 달리, 미확정 ‘전환 신호’를 선제적으로 포착하여 향후 제도화 성숙도 유형을 제시하고, 이에 따른 껍을 분석한 결과를 기초로 K-RMF의 고도화 방안을 제시했다는 학술적 독창성을 지닌다.

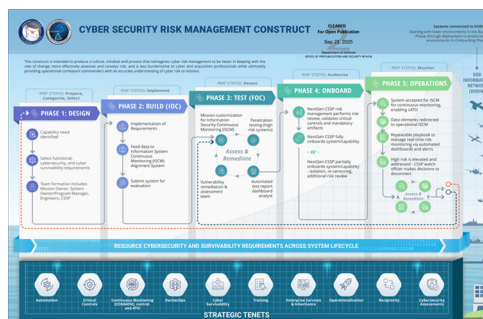


그림 1. CSRMC

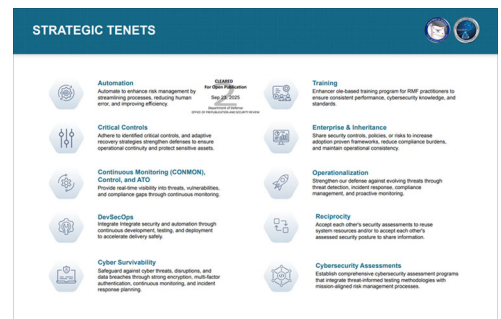


그림 2. CSRMC Strategic Tenets

한편, 한국은 국방 분야에서 K-RMF를 도입·확대하고 있으나, 소프트웨어 중심 무기체계의 급격한 확산 속에서도 여전히 문서와 절차 중심의 단발성 인가 체계에 의존함으로써 전력화 지연과 운영 현실과의 괴리라는 병목 현상을 겪고 있다.[4]

특히 상위 법·제도 기반의 취약성, 문서 기반 절차 중심 운영에 따른 신속성·자동화 한계, 산업계 연계 및 COMMON 체계의 제도화 미흡 등 보완 과제가 지적된다. 특히 CSRMC가 시사하는 운영

중심 거버넌스 전환은 K-RMF가 다음 성숙 단계로 나아가기 위해 무엇을 선제적으로 제도화해야 하는지를 점검하게 하는 비교 준거로 기능한다. 이는 단순히 기술적 도구의 도입을 넘어 정책 행위자들의 신념 변화와 국방 제도 내의 규칙과 행위 상황이 복합적으로 작용하는 거버넌스 재설계의 문제이다.

따라서 본 연구는 단순히 미 국방부의 제도를 소개하는 데 그치지 않고, 이를 외부로부터의 충격으로 간주하여 이러한 전환의 역동성을 포착하기 위해 다차원적인 레이어-렌즈 분석 틀을 설정하고 선제적인 K-RMF 운영 모델 고도화 방안을 도출하고자 한다.

1.2. 연구 문제

본 연구는 확정된 차기 RMF 개편 문서의 사후 추적 및 비교라는 접근에서 벗어나, CSRMC 및 Strategic Tenets가 포함하고 있는 공개된 전환 신호를 해석하여 향후 제도화 방향을 제도화 성숙도 유형으로 구조화하고, 이를 준거로 K-RMF의 선제적 갭 진단과 한국형 고도화 로드맵을 도출하는 정책 설계 연구를 지향한다. 이를 위해 다음 연구 질문에 답한다.

첫째, CSRMC의 전환 신호는 기존의 승인 이벤트 중심 ATO를 ‘데이터 중심의 지속적 보증’으로 재구성하기 위해 기계 판독형 증빙, 자동화 파이프라인, 통제 상속 등 핵심 기술 및 관리적 요소간의 유기적 연계와 운영 모델 전환 메커니즘을 어떻게 정의하고 있는가?

둘째, CSRMC의 상위 원칙과 신호들이 실제 제도적 요구사항(what), 책임·권한(who), 증빙 및 평가(how)의 구체적 운영 규칙으로 바뀌게 되는 경로는 무엇이며, 담론의 형성이나 실행 환경의 제약에 따라 이는 어떤 제도화 성숙도 유형으로 구조화되는가?

셋째, 도출된 제도화 성숙도 유형별 요구조건을 준거로 K-RMF의 수준별 갭을 판정하고, 기술과 제도적 의존성 분석 기반의 구조화된 정성적 우선순위 평가를 거쳐 K-RMF의 단계별 고도화 이행 로드맵은 어떻게 설계되어야 하는가?

1.3. 연구의 기여

본 연구는 다음과 같이 3가지 측면에서 기여할 것으로 기대된다.

첫째, 학문적으로 이번 연구는 기존 RMF와 관련된 연구들이 확정된 규정의 사후 절차 비교에 머물던 한계를 극복하고, 위험관리를 ‘운영 모델 전환’과 ‘거버넌스 변화’의 관점에서 입체적으로 재구조화했다는 점이다. 특히 미확정된 정책의 전환 신호를 3대 레이어와 4대 렌즈 등으로 규명하여 미래 제도화 방향을 예측하는 동태적 성숙도 분석 방법론의 외연을 확장하였다.

둘째, 정책적으로는 기술 및 절차적 요소의 단편적 나열에 그치던 기존 개선안들과 달리, 제도화 성숙도 유형별 설계 요건에 따라 K-RMF의 수준별 갭(Gap)을 판정했다는 점이다. 더 나아가, 도출된 이행 과제들을 구조화된 정성적 우선순위 평가 프로세스를 통해 체계적으로 검증함으로써 국방 안보 환경의 급변 속에서도 복원력을 가질 수 있는 최적의 단기, 중기, 장기 고도화 로드맵을 과학적인 방법으로 제시하였다.

셋째, 산업·현장 측면에서는 기존의 파편화된 보안 증빙을 ‘데이터 중심의 수명주기 보증’ 체계로 재구성함으로써, 방산 및 소프트웨어 개발 주체가 중복적 평가 부담을 최소화하고 예측이 가능한 보안 파이프라인을 설계할 수 있는 실무적 가이드라인을 제공한다.

또한 소프트웨어 중심 무기체계의 급격한 확산과 디지털 전장 전환이라는 도전 과제에 직면한 한국군에 실질적인 방향성을 제공한다. 제안된 K-RMF 운영 모델 고도화 방안은 군사보안 수준의 엄정함에 타협하지 않으면서도, 단발성 인가 지연으로 인한 전력화 공백을 최소화하고 상시 작전

지속성을 보장하는 ‘국방 디지털 거버넌스 재설계’의 실천적 가이드라인으로 활용될 수 있다.

1.4. 연구 방법 및 자료

본 연구는 미 국방부의 CSRMC 관련 공식 및 공개 문서와 한국의 K-RMF 관련 규정에 대한 다차원 분석 틀 기반의 문헌 비교분석을 수행한다. 핵심 자료는 미국의 CSRMC 및 Strategic Tenets, NIST에서 발표한 RMF 및 미 국방부 관련 공개 문서와 한국의 K-RMF 관련 규정·지침이며, ISO/IEC 27001, ISMS-P, FedRAMP 등은 보조 준거틀로 활용한다. 분석은 미 국방부 Strategic Tenets의 10대 핵심 원칙을 핵심 분석 준거이자 원천 속성으로 설정하고, 이를 ‘요구사항(What)-거버넌스·책임·권한(Who)-증빙·평가·데이터 모델(How)’의 3개 레이어로 매핑하여 해석한다. 이 과정에서 도출된 기술적·제도적 요구 속성을 ‘3레이어 × 4렌즈’ 분석 매트릭스 상에 표준화된 비교 준거로 범주화하고, 이를 기반으로 제도화 성숙도 유형을 설정함으로써 정책 진단 및 개선안 도출의 체계성과 논리적 정합성을 확보한다.

1.5. 논문의 구성

본 논문은 ① 이론적·제도적 배경과 비교 준거, ② 분석 틀 및 연구설계, ③ CSRMC 신호에 기초한 제도화 성숙도 유형 도출, ④ 제도화 성숙도 유형별 요구조건에 따른 K-RMF에 대한 구조화된 정성적 우선순위 평가 및 갭 분석, ⑤ 분석 결과를 반영한 단계적 고도화 로드맵 및 구체적 정책 제언 순으로 구성한다.

2. 배경 및 비교 준거

2.1. RMF의 제도적 맥락과 전환 필요

RMF는 본래 위험 기반의 접근을 통해 보안 수준을 검증하고 운영의 정당성을 확보하기 위한 표준 절차로 기능해 왔다. 미국의 RMF는 NIST SP 800-37을 기반으로 ‘분류-통제 항목 선정-구현-평가-인가-모니터링’으로 이어지는 일련의 과정을 제도화함으로써, 보안을 단순한 기술 통제の問題가 아니라 정책·조직·운영 의사결정 체계로 확장해 왔다.[5]

그러나 소프트웨어 정의(Software Defined) 무기체계 확산 및 지속적 통합·배치(Continuous Integration/Continuous Delivery, CI/CD) 중심의 개발·시험·배치 주기가 단축되는 환경에서는, 기존의 문서·절차 중심으로 운영되던 RMF가 정태적·선형적 검증 구조에 고착되어 현재의 동태적 전력화 주기와 충돌하고 있다. 이는 단순한 행정적 ATO 지연을 넘어, 실제 전장의 위협 변화를 제도가 따라가지 못하는 ‘보안 가시성의 공백’을 만들 수 있다는 점에서 근본적인 운영 모델의 전환이 요구된다.[6]

이러한 맥락은 미 국방부가 RMF 개편을 단순 절차 보완이 아니라 ‘운영 기반의 지속적인 위험관리’로의 전환 문제로 다루게 된 배경으로 이해할 수 있다.

2.2. 보조 준거틀의 위치: 조직 거버넌스와 운영 기반 지속 보증

본 연구는 미 국방부의 RMF와 CSRMC, Strategic Tenets와 K-RMF 비교 및 설계를 위해 ISO/IEC 27001, ISMS-P, FedRAMP를 보조 준거로 활용한다. ISO/IEC 27001과 ISMS-P는 NIST-RMF의 3계층 구조 중 Tier 1인 조직 및 Tier 2의 임무·공통 서비스 차원의 거버넌스 기반

을 제공한다. 이러한 전사적 거버넌스 체계하에서 전사적인 통제가 선행될 때, 비로소 하위 체계 및 시스템 단위인 Tier 3 수준의 단발성·중복적 증빙 부담을 경감하고 실질적인 ‘통제 상속’을 실현할 수 있는 구조적 토대가 마련된다.

특히 조직 단위 전반의 관리 체계인 ISMS-P와 한국군의 임무·무기체계 단위 RMF인 K-RMF가 거시 및 미시 차원의 명확한 역할 분담을 이룰 경우, 제도적 중복과 규제 피로감을 최소화하면서 통제의 일관성과 책임성을 제고할 수 있다.[7,8]

한편, FedRAMP는 표준화된 평가 체계와 COMMON을 통해 클라우드 서비스의 위험을 관리하며, 평가 결과와 증빙을 재사용하도록 하는 제도적 장치를 갖춘 대표 사례다.[9]

이는 RMF가 ‘인가 이벤트’ 중심에서 ‘운영 기반의 지속 보증’으로 전환될 수 있음을 보여주는 선행 모델로서, CSRMC가 강조하는 방향성과도 맞닿아 있다.

2.3. 비교 준거의 정식화: K-RMF 고도화의 핵심 설계 요건

ISO/IEC 27001과 ISMS-P가 조직 거버넌스 기반을 제공하고, FedRAMP가 운영 단계의 COMMON 및 증빙 재사용을 제도화한 사례라는 점을 종합하면, 공개 신호 기반의 제도 전환에서 핵심적으로 점검해야 할 설계 요건을 다음과 같이 정리할 수 있다.

첫째, 운영 단계에서 위험을 지속적으로 관리하기 위한 COMMON의 상시성이다. 위험관리의 중심이 단발적 승인인 ATO 위주에서 운영 기반의 지속 보증으로 옮겨갈수록, 운영 데이터 기반의 COMMON이 제도적으로 내재화되어야 한다.

둘째, 자동화된 증빙 파이프라인의 정착이다. 위험관리를 정태적 문서 제출 중심으로 운영할 경우 수작업에 따른 지연과 증빙 데이터의 무결성을 확보함에 있어서 한계가 있다. 따라서 ‘컴플라이언스의 코드화’ 개념을 바탕으로, DevSecOps 과정에서 생성되는 보안 데이터가 실시간으로 수집·정규화·추적되는 자동화 파이프라인 구축이 요구된다.

셋째, 평가 재사용·상호인정 및 통제 상속 메커니즘의 제도화이다. 피평가 시스템마다 동일하거나 유사한 통제를 중복해서 평가하는 비효율을 제거하고, FedRAMP의 선진화된 준거와 같이 표준화된 증빙 및 평가 결과를 타 체계에서 상호 인정하는 제도적 장치가 필수적이다. 이는 군사적 안보 신뢰성을 저해하지 않으면서도 상속이 가능한 통제를 극대화하여 소프트웨어 중심 무기체계의 전력화 주기를 획기적으로 단축하는 핵심 요소가 된다.

2.4. 소결론

본 장은 ① 기존 RMF가 절차와 문서 중심 운영의 한계에 직면해 ‘운영 기반의 지속적인 위험관리’로의 전환 논리가 강화되고 있음을 정리하고, ② ISO/IEC 27001, ISMS-P, FedRAMP를 보조 준거로 설정하여 조직 거버넌스와 운영 기반 지속 보증의 제도화 방식이 어떠한지를 확인하였다.

특히 이번 비교분석을 거쳐 도출된 3대 핵심 설계 요건인 COMMON의 상시성, 자동화된 증빙 흐름, 평가 재사용 및 상호인정 등은 향후 K-RMF의 제도적 성숙도를 측정하는 원천 속성으로 기능한다. 이는 후속 장에서 제시할 ‘3-Layer × 4-Lens’ 분석 틀 내에서 미 국방부 CSRMC 전환 신호의 제도화 성숙도 유형을 해석하고 K-RMF의 수준별 갭을 판정하는 엄정한 객관적 준거 스케일로 활용된다.

3. 연구설계

3.1. 연구설계 개요

본 연구는 공개된 제도 전환 신호를 해석해 제도화 성숙도 유형을 도출하고, 그 결과를 준거로 K-RMF의 개선 과제를 설계하는 ‘신호 기반 예측-비교 진단-정책 설계형’ 연구설계를 채택한다. 핵심 자료는 미 국방부가 공개한 CSRMC 및 Strategic Tenets와 한미 양국의 RMF 관련 공식·공개 문서이며, ISO/IEC 27001, ISMS-P, FedRAMP는 보조 준거로 활용한다. 분석은 ① 기존 RMF와 K-RMF의 기준선 비교, ② CSRMC 신호의 해석과 제도화 성숙도 유형 도출, ③ 제도화 성숙도 유형에 기반한 갭 분석과 구조화된 정성적 우선순위 평가를 통한 로드맵 설계로 구성된다.

3.2. 분석 단위와 비교 기준

본 연구는 RMF를 구조(Architecture)-운영(Operating Model)-규범(Norms)의 3개 레이어로 나누고, 이를 거버넌스(Governance)-기술-운영(Tech/Ops)-적용 범위(Scope)-성과(Performance: 효과성·효율성) 등 4개의 평가 렌즈로 교차 검토하는 레이어-렌즈 분석 틀을 사용한다.

이 분석 틀은 절차 항목의 단순 나열을 넘어, ① 제도 설계(역할·책임·승인 구조), ② 운영 메커니즘(CONMON·자동화·증빙 흐름), ③ 적용의 경계선(대상 체계·공급망 포함), ④ 성과(위험 저감과 전력화-운영 효율) 간 상호작용을 다차원적 공통 분석 프레임워크 상에서 입체적으로 비교·분석할 수 있게 한다.

특히 ‘전환 신호’는 문구 수준의 추정이 아니라, 제도 문서에서 관찰이 가능한 요구사항(what)-책임·권한(who)-증빙·평가(how)로 전환 및 구체화 되는 경로로 다루며, 제도화 성숙도 유형 도출과 갭 판정은 이런 전환 및 구체화 단위에 기반한 관찰 지표(운영 규칙의 명시, 산출물·데이터 흐름, 재사용 메커니즘의 제도화 정도 등)를 통해 수행한다.

3.3. 연구 절차

연구는 다음 5단계로 수행한다.

① 자료 수집 및 DB 구축 단계에서는 정부·기관·표준 기구가 발행한 정책 문서, 지침, 발표 자료 등 공식·공개 문서를 중심으로 데이터베이스를 구축한다(언론·해설 자료는 맥락 참고로 한정하여 활용한다) ② 비교 준거 및 평가 지표 정립 단계에서는 ‘3레이어 × 4렌즈’ 교차 매트릭스를 기본 분석 좌표계로 삼아, 핵심 개념인 CONMON, 자동화, 증빙, 평가 재사용 및 상호인정, 통제 상속 등의 정의에 대한 판정 지표 및 요구 요건을 명확히 구조화한다. ③ 전환 신호 분석 및 제도화 성숙도 유형은 CSRMC의 생애주기 구조와 Strategic Tenets를 전환 신호로 해석하여 구성한다. ④ K-RMF 갭 분석 단계에서는 동일한 레이어-렌즈 비교 준거를 적용하여 K-RMF의 현황을 진단하고 ‘없음-부분 제도화-제도화’ 수준에서 갭을 판정하고, 제도화 성숙도 유형별 요구 요건과의 차이를 도출한다. ⑤ 우선순위 평가 및 로드맵 설계 단계에서는 개선 과제를 단기-중기-장기로 구분하고, 실행 가능성(법·제도·조직·예산)-효과(위험 저감)-효율(속도·비용)-상호운용성 관점의 구조화된 정성적 우선순위 평가로 우선순위를 정한 뒤 이행 로드맵을 제시한다. 평가 근거는 기준표와 함께 기록하며, 가중치 변화에 따른 우선순위 안정성을 점검한다.

3.4. 이론적 참조 틀의 위치

본 연구는 미 국방부 CSRMC 전환 신호 형성 과정과 K-RMF 운영 실태를 체계적으로 해석하기 위해 옹호연합모형(Advocacy Coalition Framework, 이하 ACF), 제도 분석 및 발전 틀(Institutional Analysis and Development, 이하 IAD), 질적 비교분석(Qualitative Comparative Analysis, 이하 QCA)의 핵심 기제를 분석적 탐색 틀로 참조 및 활용한다. 이는 각 이론의 엄밀한 실증적 모형 검증보다는 정책 신념의 전환(ACF), 행위 상황 내 사용 규칙(IAD), 조건 간 결합 논리(QCA)라는 이론적 시각을 정책 분석 및 껍 진단의 해석적 도구로 준용하기 위함이다.[10-12]

① ACF는 미 국방부 정책 하위 체계 내 행위자들의 ‘정책에 관한 신념의 전환’을 고려하여 K-RMF의 제도화 성숙도 유형(S1~S3)을 도출하는 분석 틀로 작동한다. ② IAD는 K-RMF의 껍 진단 시 ‘행위 상황’ 내에서 ‘사용 규칙’을 분해하여 현장의 운영상 병목을 식별하는 진단 도구로 활용된다. ③ QCA는 진리표나 불연산 기반의 수리적 집합 모형을 직접 적용하기보다는, [자동화 x CONMON x 통제 상속/상호인정] 등 핵심 조건 간의 ‘결합 논리(Combinatory Logic)’를 정책의 껍 진단 및 구조화된 정성적 우선순위 평가 결과와 논리적으로 일치하는지 검증하는 해석적 프레임워크로 준용한다.

3.5. 연구의 한계

본 연구는 공개 문서 기반의 분석이므로 비공식 관행이나 내부 의사결정의 미시적 맥락을 완전하게 포착하기 어렵고, 차기 RMF 확정 문서가 없는 상황에서 제도화 성숙도 유형이 후속 문서 공개에 따라 조정될 수 있다. 또한 K-RMF는 적용 및 확대 과정에 있어 성과 데이터가 제한적일 수 있어 정량적 효과 검증은 연구 범위를 벗어난다.

다만 본 연구는 제도화 성숙도 유형별 실증적 확인 지표를 구체적으로 선언하고, 구조화된 비교 분석 준거 및 평가 지표를 명확히 제시하여 타당성 검증이 가능하도록 설계하였다. 따라서 본 연구의 분석 틀은 차기 미 국방 RMF의 최종 확정 문서가 발간되거나 국내 성과 데이터가 축적되는 시점에 유연하게 재적용할 수 있는 개방형 연구 플랫폼의 역할을 수행하며, 향후 국방 안보 정책의 변동을 지속 추적하는 동태적 가이드라인을 제공한다는 점에서 한계를 상쇄하는 의의를 지닌다.

4. 분석 틀의 설정

4.1. 분석 틀의 필요성

비교연구의 핵심은 사례를 나열하는 것이 아니라, 동일한 기준과 분석 단위에 기반해 체계적 비교를 가능하게 하는 분석 틀을 구축하는 데 있다. 특히 본 연구는 확정된 차기 RMF 개편 문서의 사후 비교가 아니라, CSRMC 및 Strategic Tenets라는 공개적으로 전환하겠다는 신호를 기반으로 제도화 성숙도 유형을 도출하고, 이를 준거로 K-RMF의 선제적 개선 로드맵을 설계한다. 따라서 분석 틀은 단순한 현황 비교를 넘어, 현재 상태(what is)-전환 방향(what is likely)-정책 설계(what should be)를 하나의 분석 틀로 연결할 수 있어야 한다.

이 과정에서 ACF는 미국 측 전환 신호가 형성되는 정책 신념·행위자·담론 맥락을 해석하는 데, IAD는 K-RMF 운영에서 규칙과 구체적 행위나 상황, 예를 들자면 ATO 심사, 운영 중 변경 관리, CONMON 보고 등이 어떻게 상호작용과 성과로 연결되는지를 진단하는 데 보조적으로 참조된다. 다만 본 연구의 중심이 되는 분석 단위는 제도 변화의 ‘절차의 존재 여부’가 아니라, 전체 수명주기 동안

위험관리의 운영 모델과 그 운영을 뒷받침하는 증빙 체계가 어떻게 설계되고 제도화되는지에 있다.

4.2. 분석 기준의 도출: 레이어 - 렌즈 교차 분석 틀

본 연구는 위험관리 체계를 ‘구조(Architecture)-운영 모델(Operating Model)-규범(Norms)’의 3개 레이어로 나누어 분석한다. 여기서 구조(Architecture)는 법·규정·산출물 요구·책임 및 승인 구조 등 제도의 설계와 관련된 요소를, 운영 모델(Operating Model)은 COMMON·자동화·증빙 수집·평가·재사용 등 실제로 작동되는 메커니즘을, 규범(Norms)은 ‘처리 속도 vs 규범 준수’와 같은 정책의 우선순위, 기술 채택의 원칙, 협력적 생태계 지향 등 제도의 규범적 기반을 의미한다.

각 레이어는 거버넌스(Governance) - 기술 및 운영(Tech/Ops) - 적용 범위(Scope) - 성과(Performance) 등의 4개 평가 렌즈로 교차하여 검토한다. 거버넌스(Governance)는 법·제도 정합성과 책임·권한·의사결정 구조를, 기술 및 운영(Tech/Ops)은 자동화·COMMON·위협 기반 평가·DevSecOps의 실행 메커니즘을, 적용 범위(Scope)는 대상 체계와 공급망 포함 여부에 대한 경계를, 성과(Performance)는 위협의 저감(효과성)과 전력화·운영 효율(효율성)을 평가한다. 이 레이어-렌즈 결합은 비교를 항목 나열이 아니라 다차원 상호작용에 대한 분석으로 전환하는 공통 좌표계로 기능한다.

4.3. 교차 매트릭스와 구체화 원칙

본 연구는 3개 레이어와 4개 렌즈를 교차한 매트릭스를 기본 구조로 사용한다. 표 1의 각 셀은 단순한 분류 항목이 아니라, 해당 영역에서 관찰이 가능한 정책적 요구사항, 책임·권한 규정, 산출물·증빙 요건, 운영 데이터 및 지표, 재사용 메커니즘을 체계적으로 분류하고 평가하기 위한 공통 좌표계이며, 5장에서는 각 교차 영역별 대표적으로 근거가 되는 문구와 판정 지표를 제시한다. 꺾판정은 ‘없음, 부분 제도화, 제도화’의 수준으로 구분하는 것을 포함하며, ‘제도에 있거나 표준화·자동화·운영 규칙이 미흡한 상태’를 별도의 개선 과제로 식별한다.

예컨대 COMMON은 [운영 모델(Operating Model)×기술/운영(Tech/Ops)]에서 직접 관찰되지만, 거버넌스(책임·권한 및 보고 규칙)와 성과(위험 저감·운영 부담) 렌즈에서도 함께 평가된다. 또한 평가 재사용 및 상호인정과 통제 상속은 기술/운영 메커니즘이면서 동시에 거버넌스(승인 규칙·책임소재)와 성과(중복평가 감소·비용/시간 절감) 차원에서 교차 평가된다.

표 1. 레이어-렌즈 교차 검토를 위한 분석 틀(교차 매트릭스)

구분	G. 거버넌스	T. 기술/운영	S. 적용범위	P. 성과
A. 구조	- 인가 주체 및 승인의 책임 구조 - 법·제도·규정 간 상호정합성	- 증빙·산출물 표준 Data 규격 - 기계 판정형 모델	- 평가대상 체계 분류 기준 - 인가 경계선	- 규제 이행 간 행정 소요 시간 - 서류제출 및 중복평가 비용
O. 운영	- ATO 승인 권한 - 운영 중 변경 관리 관련 규칙	- COMMON 수집 주기 및 자동화 여부 - Telemetry 수집, 분석 파이프라인	- DevSecOps CI/CD 파이프 라인 연동 - 공급망 연계 및 추적 범위	- 위험 감지·완화 리드타임 - 전력화 배치 및 인가 주기 속도
N. 규범	- 정책 우선순위 (전력화 속도 vs 규정 준수) - 통제 상속/책임 공유 정당성	- 데이터 중심 증빙 문화 - 표준 자동화 도구 채택 원칙	- 민관군 및 방산 생태계 협력 범위 - 동맹, 연합 간 상호인정 지향	- 현장 수용성 및 규제 피로도 - 환경 변화에 대한 동태적 복원력

4.4. 소결론

본 장은 공개 신호 기반의 제도화 성숙도 유형 도출과 K-RMF 갭 분석을 수행하기 위해, RMF를 ‘구조(Architecture)-운영 모델(Operating Model)-규범(Norms) 레이어’로 나누고, 이를 4개 평가 렌즈로 교차 검토하는 분석 틀을 제시하였다. 이 분석 틀은 후속 장에서 CSRMC 신호가 제도적 요구 요건으로 전환 및 구체화 되는 경로를 구조화하고, 제도화 성숙도 유형별 운영 모델 설계 요건을 기준으로 K-RMF의 갭과 로드맵을 도출하는 공통 좌표계로 활용된다.

5. CSRMC 신호 기반 차기 RMF 제도화 성숙도 유형과 K-RMF 갭 분석

5.1. 분석 접근과 비교 단위의 재정의

본 장은 제4장에서 제시한 ‘레이어-렌즈’ 교차 분석 틀을 적용하여, 미 국방부가 공개한 CSRMC 및 Strategic Tenets를 차기 RMF 개편 방향을 가늠하는 공개 전환 신호로 해석한다. 이때 도출되는 제도화 성숙도 유형(S1~S3)은 미 국방부 전환 신호의 현실화 범위에 따른 K-RMF가 단계적으로 수용 및 지향해야 할 ‘목표 성숙도 모델’로서 기능한다.

분석의 초점은 아직 공개되지 않은 ‘개편 문서의 조항’을 추정하는 데 있지 않다. 대신 CSRMC 신호가 갖고 있는 운영 모델 전환의 설계 요건인 운영 기반 COMMON, 자동화된 증빙 수집·검증, 평가 재사용·상호인정 및 통제 상속, 공급망 증빙 내재화 등을 비교 단위로 삼아, 이를 기준으로 K-RMF의 제도·운영 갭을 도출한다.

갭은 단순 ‘부재/미흡’의 이분법이 아니라 ‘非 제도화(없음)-부분 제도화(있으나 표준화·자동화·운영 규칙 미흡)-제도화(있으면서 작동)’의 수준’으로 판정하며, 제도에 규정은 존재하나 운영상 구현 수준이 낮아 정책적 개입이 필요한 영역을 별도 개선 과제로 식별한다. 또한 K-RMF는 운영 단계의 COMMON과 운영 중 평가·재인가 등 운영 관리의 기본 골격을 일부 갖추고 있으므로, 본 장의 갭 분석은 이상적 목표 모델 대비 부족을 지적하는 데 그치지 않고, 제도화와 확산의 현실적인 방안(범위·속도·거버넌스 조정)까지 함께 고려하여 제시한다.

5.2. CSRMC 전환 신호의 추출과 전환 / 구체화 규칙

CSRMC와 Strategic Tenets는 위험관리를 ‘설계(Design)-구축(Build)-시험(Test)-도입(On board)-운영(Operations)’으로 이어지는 수명주기 전반에 내재화하고, 운영 단계에서 ‘위험을 지속적으로 관측·평가·완화하는 방향’을 강조한다. 본 연구는 이 공개 신호를 단순 슬로건이 아니라 제도화가 가능한 요구 요건으로 전환하기 위해, 신호를 ‘요구사항(what)-책임과 권한(who)-증빙 및 평가(how)’의 구체화가 가능한 단위로 구조화하였다. 즉, 원칙 수준의 메시지가 실제 제도 문서에서 어떤 산출물·지표·보고 의무·평가 방식·승인 구조로 구체화할 수 있는지를 규칙으로 정리하고, 그 조합을 통해 제도화 성숙도 유형을 구성한다.

특히 신호가 반복적으로 지시하는 공통 방향은 ① 승인 이벤트를 축소하거나 지속 인가로의 이동, ② 운영 데이터 중심 증빙 및 자동화, ③ 평가 결과의 재사용 및 상호인정과 통제 상속을 통한 중복평가 최소화, ④ DevSecOps 기반 전체 수명주기 통합과 공급망 증빙의 제도화 등으로 요약된다. 이러한 요소는 이후 제도화 성숙도 유형 간 차이를 가르는 핵심 분기점으로 작동한다.

5.3. 차기 RMF 제도화 성숙도 유형

ACF의 신념 체계 관점에서 차기 RMF 제도화 성숙도 유형은 미 국방 정책 하위 체계 내 주도 연합의 신념 변화를 반영한다. 기존 RMF가 ‘단발성 ATO 중심의 정태적 컴플라이언스’라는 정책의 핵심 신념에 의존했다면, CSRMC 전환 신호는 ‘운영 데이터 기반의 지속 보증’을 핵심 신념으로 하는 새로운 신념 체계 연합의 주도권 확보를 의미한다. 이러한 신호의 강도와 제도화 범위를 기준으로, 차기 RMF 제도화 성숙도 유형을 다음 3개로 정리하였다.

① 제도화 성숙도 유형 S1은 운영 중심의 COMMON 강화형이다. ATO를 단발성 이벤트가 아니라 지속적 운영 지표 기반의 ‘COMMON’으로 전환한다. 증빙은 운영 데이터 기반으로 자동 수집 및 검증되며, 평가 결과의 재사용 및 상호인정과 통제 상속이 제도적으로 확립된다. DevSecOps 연계와 공급망 증빙도 표준화된 요구 요건으로 내재화된다. ② 제도화 성숙도 유형 S2는 하이브리드 전환형이다. 전통적 ATO 구조는 유지하되, 고위험 영역부터 운영 중심 통제를 단계적으로 확대한다. 자동화와 증빙 표준은 우선순위 기반으로 점진적 도입, 평가 재사용 및 상호인정은 일부 영역에서 제한적으로 제도화된다. ③ 제도화 성숙도 유형 S3는 제한적 개선형이다. ATO 문서 중심의 구조를 대체로 유지하면서, 일부 절차 효율화와 일부 도구만 도입하는 수준에 머문다. COMMON과 자동화는 ‘권고 및 선택’ 수준에 가까우며, 평가 재사용 및 상호인정과 통제 상속은 제한적으로 적용된다.

표 2. CSRMC 신호 기반 차기 RMF 제도화 성숙도 유형별 비교(안)

구 분	운영 중심 COMMON 강화형(S1)	하이브리드 전환형(S2)	제한적 개선형(S3)
승인/인가	지속 보증형(운영지표, 임계값 기반), 조건부 운영, 동적 통제	조건부/단계적 승인 + 핵심 통제는 COMMON	전통 ATO 유지, 템플릿, 절차 간소화
증빙 체계	운영 데이터가 핵심 증빙, 자동 수집, 자동 제출	문서+운영 증빙 병행, 핵심 증빙 세트부터 확장	문서 산출물 중심, 일부 자동보고 수준
COMMON	상시 의무화, 위험 임계값 기반 자동조치	핵심 통제부터 단계적 확대	제한적/권고 수준, 주기적 점검 중심
자동화	평가, 증빙 수집, 리포팅 자동화가 운영 모델의 중심	자동화는 단계적 도입 (우선순위 기반)	자동화는 부분 도입 (도구 사용 수준)
재사용/상호인정	통제 상속, 상호인정 제도화 (중복평가 최소화)	제한적 재사용 (플랫폼/핵심 통제 중심)	재사용 구조 미약, 사업별 반복 평가 위험
공급망	표준화된 공급망 증빙 요구 + 운영 연계	고위험 체계부터 단계적 제도화	필요시 개별 요구 (편차 위험)

5.4. K-RMF 갭 분석: 제도화 성숙도 유형의 준거별 차등 과제

IAD의 행위 상황 및 사용 규칙 관점에서 K-RMF를 진단해 보면, 현행 제도는 ‘규정상 텍스트’와 현장의 ‘실제 사용 규칙’ 간 불일치를 보인다. 획득 및 인가라는 행위 상황에서 평가기관과 사업자 간 상호작용을 지배하는 규칙이 ‘문서화된 산출물 제출 및 일회성 심사’에 고착되어 있어, 개발 및 운영 주체 간 실시간 데이터 공유를 막는 행위 규칙상의 병목으로 작동하고 있다. 이러한 병목을 전제로 K-RMF의 운영 중심의 COMMON 관점에서 분석하면 다음의 핵심 갭이 두드러진다.

① COMMON의 ‘상시성’과 운영 데이터 기반의 증빙 체계가 제도적으로 표준화되어야 한다. 운영 중 위험을 지속적으로 관측하고 그 결과가 평가·완화·재인가로 연결되는 메커니즘이 약할 경우, 운영 중심의 전환은 형식화될 가능성이 높다. ② 자동화된 증빙 수집 및 검증과 평가 파이프라인을 제도적으로 수용해야 한다. 문서 제출 중심의 증빙은 속도와 품질면에서 한계가 있기 때문에, 개

발·시험·운영 과정에서 생성되는 데이터를 증빙으로 인정하고 자동으로 추적하는 체계가 필요하다. ③ 평가 재사용/상호인정 및 통제 상속 메커니즘을 도입해야 한다. 동일하거나 유사한 평가의 반복은 전력화 지연과 비용 증가를 유발하므로, 표준화된 증빙과 결과를 재사용할 수 있는 제도적 장치가 있어야 한다. ④ 산업체·운영부대와의 연계 거버넌스가 강화되어야 한다. 운영 데이터와 증빙을 생산하는 주체가 개발자·운영자·평가기관·승인권자 등 다양하게 걸쳐 분산되어 있기 때문에, 증빙의 흐름과 책임 및 권한의 재설계가 필요하다. ⑤ 공급망 증빙을 위험관리 요구 요건에 통합해야 한다. 공급망 위험은 체계의 외부에서 유입되므로, 개발·도입 단계의 증빙 요구를 운영 단계의 위험관리와 연결하는 구조가 필요하다.[13]

표 3. 제도화 성숙도 유형의 준거 별 K-RMF 핵심 갭(요약)

설계 요건	S1 준거시 우선순위	S2 준거시 우선순위	S3 준거시 우선순위
COMMON 상시화, 운영 지표 연계	최우선	상	중
자동화된 증빙/평가 파이프라인	최우선	상	중
평가 재사용/ 상호 인정 및 통제 상속	상	중	하
공급망 증빙 통합	상	중	중
산업-운영-평가 거버넌스 재설계	상	상	중

5.5. 소결론

본 장은 CSRMC와 Strategic Tenets를 공개 전환 신호로 해석하고, 신호가 제도화 성숙도 유형의 요구 요건으로 전환 및 구체화 되는 경로를 바탕으로 3개의 제도화 성숙도 유형을 도출하였다. 또한 유형별 운영 모델 설계 요건을 준거로 K-RMF의 갭을 ‘없음-부분-제도화’ 등의 수준으로 구분하여 요약함으로써, 다음 장에서 구조화된 정성적 우선순위 평가와 단계적 로드맵 설계를 수행하기 위해 준비하는 과정이다.

6. 구조화된 정성적 우선순위 평가와 K-RMF 발전 로드맵

6.1. 구조화된 정성적 우선순위 평가: 평가 기준과 적용

본 장에서는 5장의 제도화 성숙도 유형별 분석 결과를 바탕으로 K-RMF 고도화를 위한 세부 이행 과제와 단계별 로드맵을 도출한다. 과제별 우선순위는 전문가 평가의 주관적 편향을 배제하고 국방 사이버 체계의 구조적 필연성을 확보하기 위해 ‘기술-제도적 의존성 분석(Dependency Analysis)’과 ‘구조화된 정성적 우선순위 평가’를 통합 적용하여 결정하였다.

평가 기준은 ① 미 국방부 CSRMC 지침과의 정책적 시급성, ② 타 과제 수행을 위한 기술적·제도적 선후관계, ③ 한국군 인프라 내 실현 가능성의 3가지 축으로 구성하였다. 각 이행 과제의 우선순위 및 평가 등급은 미 국방부 CSRMC, Strategic Tenets를 포함한 각종 문헌에 명시된 아키텍처상의 선후관계와 기술적 연계성을 논리적이고 체계적인 분석 틀에 따라 계층적으로 판정하여 도출했으며 이를 평가한 종합 결과는 표 4와 같다.

표 4. 정성적 대기준 및 기술적 의존성 분석 구조

이행 과제	정책적 시급성	기술적 선후관계	실현 가능성	우선순위 (추진 단계)
① COMMON 상시화 및 지표 연계	높음	선행 필수 과제 (데이터 기반 제공)	높음	1순위 (단기)
② 자동화 파이프라인 구축	높음	COMMON 후행 (수집 체계 연동)	중간	2순위 (단기~중기)
③ 행정 서식 간소화 및 수용성 제고	중간	독자 수행 가능 (제도 개선 병행)	높음	3순위 (단기)
④ SBOM 제출 의무화 및 정적 분석	높음	파이프라인 연계 (자동화 정착 후)	중간	4순위 (중기)
⑤ K-RMF 거버넌스 전담 조직 신설	중간	최종 정착 기반 (법·조직 개정 수반)	낮음	5순위 (중장기)

우선순위 결정 논리는 다음과 같다.

첫째, ‘COMMON 상시화’는 실시간 위협 수집의 기본 바탕이 되므로, 모든 자동화 및 정적 분석 과제에 선행되어야 하는 ‘기술적 필수 기반(Prerequisite)’으로 1순위로 지정되었다.

둘째, ‘자동화 파이프라인 구축’은 COMMON 데이터 체계 위에 작동하는 후행 과제로서 2순위에 배치되었으며, ‘행정 서식 간소화’는 기술적 의존성과 무관하게 독자 추진이 가능하고 현장 수용성을 즉시 제고할 수 있어 단기 병행 과제로 구분함과 동시에 3순위로 설정하였다.

셋째, ‘SBOM 및 정적 분석’과 ‘거버넌스 조직 신설’은 기술적 숙성도와 법·제도적 개정이 수반되는 고도화 단계이므로 중·장기 이행 과제(4·5순위)로 단계적 배치하였다. 이와 같은 의존성 기반 배치를 통해 단기적 성과와 중장기 구조 개혁을 동시에 달성할 수 있다.

6.2. 우선순위 도출: 기술·제도적 의존성과 성숙도 유형별 단계적 진화

6.1절의 기술·제도적 의존성 분석(Dependency Analysis) 결과, 제도화 성숙도 유형(S1~S3)과의 연계 속에서 우선순위가 높으면서 선행되어야 할 공통 핵심 과제는 다음 세 가지로 수렴한다.

첫 번째, COMMON의 상시화와 운영 지표 기반 위험평가 연계이다. 이는 운영 중심 전환을 위한 최우선 ‘기술적 필수 기반(Prerequisite)’으로, 모든 데이터 연동 및 자동화 과제 작동의 전제 조건을 제공한다. 두 번째, 평가 재사용과 상호인정 및 통제 상속 메커니즘이다. 이는 중복평가 구조를 줄이고 현장의 행정 부담을 즉시 완화하는 핵심 장치로, 제도 전환 초기 수용성을 높이는 ‘단기 병행 과제(S1 준거)’로 적용한다. 세 번째, 자동화된 증빙 수집·정규화·검증 파이프라인이다. 이는 첫 번째와 두 번째에서 구축된 데이터 표준화 기반 위에서 연동되는 ‘기술적 확장 과제(S2 준거)’로서 문서 중심 운영의 병목을 직접 해결한다.

반면 공급망 증빙 내재화(SBOM)와 산업-운영-평가 거버넌스 재설계는 전 체계의 고도화를 위해 필수적이긴 하지만, 법·제도 개정 및 생태계 성숙이 수반되는 ‘구조적 완결 과제(S3 준거)’이므로 추후 단계적 접근이 필요하다. 따라서 로드맵은 단계적 성숙도 진화 방향에 맞추어, 단기(1단계: 정착기)에는 ‘제한적 절차 개선 및 기본 표준 정비(S3 수준 달성)’, 중기(2단계: 고도화기)에는 ‘자동화 파이프라인 구축 및 하이브리드 적용 확산(S2 수준 달성)’, 장기(3단계: 도약기)에는 ‘거버넌스 완전 재편 및 운영 중심 COMMON의 구조적 완성(S1 수준 완전 전환)’으로 체계화하는 것이 합리적인 것으로 판단된다.

표 5. 로드맵 정리

추진 단계	핵심 이행 과제	기술-제도적 선후관계 (Dependency Logic)	연계 유형
단기 (정착기)	- COMMON 상시화 및 지표 연계 - 평가 재사용/통제 상속 메커니즘	[선행 필수 기반 및 즉시 시행] 실시간 위협 데이터 수집 체계를 최우선 정착시키고, 평가 재사용을 통해 현장 부담 경감	S3
중기 (고도화기)	- 자동화 증빙 수집·검증 파이프라인 - SBOM 제출 및 정적 분석	[기술적 확산 및 연동] 1단계의 수집·재사용 데이터 체계 위에서 작동하는 자동화 및 공급망 보안 검증 파이프라인 구축	S2
장기 (도약기)	거버넌스 및 법제화 완전 재설계	[구조적 완성] 1·2단계의 기술·운영적 성과를 바탕으로 법·제도 정비 및 전담 거버넌스 조직 신설	S1

6.3. 단기, 중기, 장기 로드맵 (제도 - 표준 - 조직 - 기술)

아래 표 6은 구조화된 정성적 우선순위 평가 결과를 바탕으로, K-RMF 고도화를 위한 단계별 이행 패키지를 정리한 것이다.

표 6. K-RMF 고도화 로드맵

구분	단기(기반 구축)	중기(확산·정책)	장기(운영 중심 전환 완성)
목표	운영 데이터 기반 증빙의 최소 표준 확립	자동화·재사용 메커니즘 제도화 및 적용 확대	지속 보증형 운영 모델과 국제 정합성 강화
제도 (규정·절차)	COMMON 최소 요구사항(보고 주가·책임·지표) 명시, 운영 중 변경 관리/재평가 핵심 기준 정비	조건부/지속 인가 운영 규칙 확대, 평가 재사용·통제 상속의 적용 조건·책임 규정화	성과 기반 지속 보증(지표 중심) 정책, 상호인정 범위 확대(연합·협력)
표준 (증빙·지표)	최소 증빙 세트의 정의 (운영 로그·취약점 패치·구성관리 등) 및 형식 표준화	증빙 자동 수집·정규화 표준 확립, 평가결과 및 증빙 메타데이터 표준화(재사용을 전제로)	공급망 증빙(SBOM 등)과 운영 지표 통합 표준 완성
조직/ 거버넌스	운영자·개발자·평가기관·승인권자간 증빙에 필요한 파이프라인 재설계, 데이터 소유 및 접근권한 정리	민·관·군 협력 기반 운영(공동 증빙 저장소 및 공유 규칙), 인센티브 및 제재 시스템 보완	생태계 기반 거버넌스(산업 참여·연합 협력) 내재화
기술/도구	자동화된 증빙 수집(파이프라인) 시범 적용, 대시보드 기반 COMMON 가시화	DevSecOps 연계 확대(빌드/배포/운영 통합), 자동 평가 및 리포팅 도구 확대 적용	정책·운영 데이터 연계 자동화 고도화(지속 보증형)

6.4. 정책 제언: ‘목록’이 아니라, ‘이행 전략’으로

로드맵의 정책적 함의는 다음과 같이 정리된다.

첫째, K-RMF 고도화의 출발점은 새로운 절차를 추가하는 것이 아니라 증빙 방식의 전환이 우선되어야 한다. 문서 중심의 증빙에서 벗어나, 운영 중에 생성되는 데이터인 로그·점검 결과·구성 및 패치 상태 등을 공통된 형식과 최소 기준으로 수집·정리할 수 있어야 한다. 이러한 ‘운영 데이터 기반 증빙의 최소 표준’을 마련해야 이후 자동화된 평가, 평가 결과의 재사용, 기관 간 상호인정이 현실적으로 가능해질 것이다.

둘째, 평가 재사용 및 상호인정과 통제 상속은 효율화를 위한 수단이지만, 결과에 대한 신뢰가 전제되어야 작동하는 제도적 장치이다. 따라서 도구 도입을 먼저 추진하기보다, 어떤 조건에서 재사용이 허용되는지에 대한 승인 규칙, 누가 책임을 지는지에 대한 책임과 권한, 사후 검증이 가능

한지에 관한 감사 가능성 등 거버넌스 규칙을 선행적으로 제도화해야 한다. 이는 중복평가를 줄이면서도 보안 수준을 유지하기 위한 필수적인 조건이다.

셋째, COMMON은 단순한 기술 기능이 아니라 운영 중심의 위험관리를 가능하게 하는 거버넌스 체계로 이해해야 한다. 운영 단계에서 위험을 ‘보고-평가-완화’로 연결하는 규칙, 운영 중 변경 발생 시 재평가 및 재인가로 연결되는 기준, 그리고 단계별 책임의 적절한 배분이 함께 설계되어야 COMMON이 형식적 보고를 넘어 실질적 운영 관리로 기능할 수 있다.

넷째, 공급망 증빙을 위한 SBOM을 포함한 구성요소·출처·취약점 영향·빌드 및 배포 기록 증빙 등은 특정 단계의 1회성 요구사항이 아니라 ‘개발-도입-운영의 전 과정’을 연결하는 관리의 기반이다. 공급망 증빙이 실효성을 가지려면, 장기적으로 운영 지표인 취약점 영향 분석, 패치 및 완화 리드타임, 구성요소 변경 추적 등과 연동되어 지속적으로 갱신·활용되는 구조로 통합되어야 하며, 이를 통해 전체 수명주기 동안 위험관리로의 전환을 뒷받침할 수 있다.

6.5. 소결론

본 장은 제도화 성숙도 유형에 기반한 갭 분석 결과를 구조화된 정성적 우선순위 평가 방법으로 평가하여, K-RMF 고도화 과제의 우선순위를 도출하고 단기, 중기, 장기 로드맵으로 재구성하였다. 제시된 로드맵은 ‘운영 중심의 COMMON’으로의 전환을 목표로, COMMON 상시화와 자동화된 증빙 흐름, 평가 재사용/상호인정 및 통제 상속을 단계적으로 제도화하는 이행 전략을 제공한다.

7. 결론

본 연구는 미국 국방부가 공개한 CSRMC 및 Strategic Tenets를 차기 RMF 개편 방향을 가늠하는 전환 신호로 해석하고, 신호가 제도 요구 요건으로 전환 및 구체화 될 가능 경로를 구조화하여 제도화 성숙도 유형을 도출한 뒤, 이를 준거로 한국 K-RMF의 갭과 고도화 로드맵을 제시하였다. 분석의 핵심은 아직 공개되지 않은 개편 문서의 조항을 예단하는 데 있지 않고, 공개 신호가 함축하고 있는 운영 모델 전환의 설계 요건인 운영 기반의 COMMON, 자동화된 증빙 수집·검증, 평가의 재사용/상호인정 및 통제 상속, 공급망 증빙의 내재화 등을 비교 단위로 삼는 데 있다. 이를 위해 본 연구는 위험관리 체계를 구조-운영-규범의 3개 레이어로 분해하고, 거버넌스-기술 및 운영-적용 범위-성과(효과성·효율성)의 4개 렌즈로 교차 검토하는 분석 틀을 적용하였다.

분석 결과, CSRMC 신호는 RMF 운영을 ‘승인 이벤트 중심’에서 ‘운영 중심의 지속 위험관리’로 전환하는 방향을 일관되게 보여주고 있으며, 그 제도화 성숙도 유형은 신호의 강도와 범위에 따라 ‘운영 중심 강화형, 하이브리드 전환형, 제한적 개선형’ 등 3가지로 제시할 수 있음을 확인하였다.

또한 제도화 성숙도 유형별 요구 요건을 준거로 K-RMF를 진단한 결과, K-RMF는 운영 단계 관리의 기본 골격을 일부 갖추고 있으나, 운영 기반 전환을 실질화하기 위해서는 ① COMMON의 상시화와 운영 지표 연계, ② 자동화된 증빙 수집·정규화·검증 파이프라인, ③ 평가 재사용과 상호인정 및 통제 상속 메커니즘을 우선 제도화할 필요가 있음을 도출하였다. 특히 중복평가 구조를 줄이면서도 보안 수준을 유지하기 위해서는 증빙의 표준과 메타데이터 구조, 책임·권한 및 승인 규칙을 함께 정비하는 제도 설계가 중요함을 제시하였다.

본 연구의 학문적 기여는 ① RMF 계열 연구가 절차 비교에 머무르기 쉬운 한계를 넘어 RMF를 운영 모델 전환의 관점에서 구조화하고, 공개 신호를 기반으로 제도 변화의 가능한 스펙트럼을 제도화 성숙도 유형으로 도출하는 방법으로 분석 접근을 제시했다는 점이다. ② 정책적 기여는 각 제

도화 성숙도 유형별 전환 요구 요건을 기준으로 K-RMF의 갯을 ‘없음, 부분 제도화, 제도화’ 수준에서 판정하고, 구조화된 정성적 우선순위 평가를 통해 우선순위를 정당화하여 단기, 중기, 장기 로드맵으로 제시했다는 점이다. ③ 산업·현장 측면에서는 ‘개발-시험-배치-운영’ 등 전 수명주기에 걸친 증빙 흐름과 요구 요건을 정리함으로써, 방산 및 공공 SW 개발·운영 주체가 예측이 가능한 보안 프로세스와 증빙 체계를 설계하는 데 참고 가능한 실무적 관점을 제공한다.

한편, 본 연구는 공개 문서 기반 분석이라는 한계를 가진다. 따라서 제도 운영에서 발견되는 비 공식 관행이나 조직 내부 의사결정의 미시적 맥락을 완전하게 포착하기 어렵고, 차기 RMF 개편의 확정 문서가 공개되면 제도화 성숙도 유형의 일부가 조정될 수 있다. 또한 K-RMF의 적용 확장 과정에서 정량적 성과 데이터가 제한적이므로, 위험이 줄어드는 효과를 포함하여 비용이나 시간의 절감 등과 같은 정량적 검증은 후속 연구 과제로 남는다. 다만 본 연구는 구조화된 비교 분석 준거와 전환 및 구체화 규칙, 제도화 성숙도 유형별 확인 지표를 명시함으로써, 향후 확정 문서 공개 및 실증 자료 축적 이후에도 동일 기준으로 반복 적용·검증될 수 있는 비교 연구 인프라를 제공한다.

후속 연구는 첫째, 차기 미 국방부 RMF 개편 공식 문서 및 관련 시행 지침이 발간되는 시점에 본 연구가 도출한 제도화 성숙도 유형(S1~S3)의 타당성을 객관적으로 측정하고 매핑하기 위한 ‘사후 검증 체크리스트’를 적용한 평가 연구가 필요하다. 이를 위한 사후 검증을 위한 체크리스트 예시는 표 7에 제시하였다.

표 7. 사후 검증 체크리스트 (예시)

구분	체크 포인트	실제
지속 인가(CATO)의 규정화 수준	단발성 ATO를 대체하는 지속 인가 제도가 공식 지침상 기본 인가 절차로 규정되었는가?	S1: CATO 기본 인가화 ☐ S2: CATO-ATO 선택적 병행 ☐ S3: ATO 유지 및 절차 개선 ☐
기계 판정형 증빙 수용 범위	수작업 문서 산출물이 아닌 DevSecOps 파이프라인 상의 실시간 운영 데이터가 1차 증빙으로 수용되는가?	S1: Telemetry 1차 증빙 전면 인정 ☐ S2: 신규 클라우드 체계 한정 수용 ☐ S3: 서류 중심 유지 및 서식 간소화 ☐
통제 상속 및 상호인정 법제화	상위 플랫폼 클라우드의 통제 상속 및 타 기관 평가 결과가 중복 검증 없이 공식 인정되는가?	S1: 통제 상속 상호 인정 자동화 ☐ S2: 조건부 상호 인정 ☐ S3: 개별 체계별 재평가 유지 ☐
공급망 보안의 인가 루프 연동	소프트웨어 자재명세서 제출 및 실시간 취약점 추적 메커니즘이 RMF 인가 요건에 자동 연동되는가?	S1: 동적 SBOM 수집·검증 필수화 ☐ S2: 정적 SBOM 제출 의무화 ☐ S3: 권장 사항 수준 유지 ☐

둘째, K-RMF의 적용 사례가 축적될수록 COMMON 운영 데이터, 평가 리드타임, 중복평가 감소 정도, 운영비용 변화 등 성과 지표를 수집해 정량적 효과 검증을 수행할 수 있다. 셋째, 공급망 증빙(SBOM 등)과 DevSecOps 도구 체계의 확산을 고려할 때, 자동화된 증빙 파이프라인의 표준화와 상호인정 범위 설정은 국제 협력 및 연합 운용 차원의 핵심 의제로 부상할 가능성이 높으며, 이에 대한 제도 설계 연구가 요구된다.

참고문헌

- [1] GAO. Cybersecurity: NASA Needs to Fully Implement Risk Management. 2025.
- [2] AFCEA Signal. Defense Industry Welcomes Initial CSRMC Policy. <https://www.afcea.org/signal-media/cyber-edge/defense-industry-welcomes-initial-csrmc-policy> (검색일 2026. 6. 24).

- [3] U.S. Department of Defense. Department of Defense Announces New Cyber Security Risk Management Construct. <https://www.defense.gov/News/Releases/Release/Article/4314411/departments-of-defense-announces-new-cybersecurity-risk-management-construct/> (검색일 2026. 6. 24).
- [4] 국방부. 제2025-8호 국방 사이버보안 위협관리 지시(일부 개정). 2025.
- [5] NIST. Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations. 2018.
- [6] GAO. Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. 2016.
- [7] ISO/IEC. ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. 2022.
- [8] 과학기술정보통신부·개인정보보호위원회·한국인터넷진흥원. 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증기준 안내서. 2024.
- [9] U.S. OMB. Modernizing the Federal Risk and Authorization Management Program (FedRAMP) (OMB Memo M-24-15). 2024.
- [10] Jenkins-Smith HC et al. (Eds.). The Advocacy Coalition Framework. Palgrave Macmillan. 2025.
- [11] Ostrom E. 박상우 역. 제도의 다양성 이해하기. 대구대학교 출판부. 2010.
- [12] 최강화. 질적비교분석과 필요조건분석. 한경사. 2023.
- [13] 윤성철, 손태식. K-RMF 제도 시행의 성숙도와 과제: 정책전이 및 제도적 적합성 관점. 국방과 보안, 제7권 제2호, pp. 333-365. 2025.