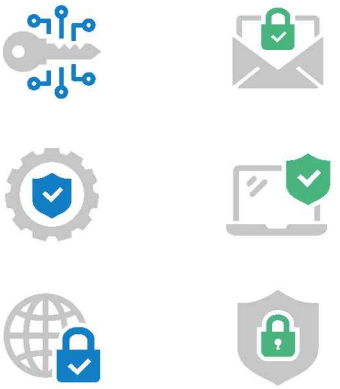
2024 VOL. 06
2024. 08

KISA INSIGHT



미국 NIST 사이버보안 프레임워크 2.0 (Cybersecurity Framework 2.0) 주요 내용과 시사점

한국인터넷진흥원 백기연 수석연구원 | 김성훈 팀장

DIGITAL &
SECURITY
POLICY

KISA 한국인터넷진흥원

CONTENTS

KISA INSIGHT

2024 VOL. 06

미국 NIST 사이버보안 프레임워크 2.0 (Cybersecurity Framework 2.0) 주요 내용과 시사점

백기연 | 김성훈

I 개발 배경

1-1. 사이버보안 프레임워크 개발(CSF 1.0) 1

1-2. 사이버보안 프레임워크 개선(CSF 1.1) 2

II 사이버보안 프레임워크 2.0 주요 내용

2-1. 개요 3

2-2. CSF 구성 요소(코어, 조직 프로필, 구현 계층) 5

2-3. 온라인을 통한 정보 제공 11

III 사이버보안 위험정보 공유체계 및 통합 개선

3-1. 위험 관리 정보공유 개선 13

3-2. 위험 관리 프로그램과 통합 개선 14

3-3. 국내 정보보호 프레임워크와 비교 16

IV 시사점

4-1. 조직의 사이버보안 위험 관리 개선 및 효율화 17

4-2. 조직의 고유한 사이버보안 관리체계와의 조화 18

4-3. 새로운 ICT 기술환경에 적용할 수 있는 보안 프레임워크 제공 18

DIGITAL & SECURITY POLICY

『KISA Insight』는
디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를
분석하여 정책 자료로 활용하기 위해
한국인터넷진흥원에서 기획, 발간하는 심층 보고서입니다.

작성

한국인터넷진흥원 정책연구실 정책연구팀

백기연 수석연구원	061-820-1636	kybaek@kisa.or.kr
김성훈 팀장	061-820-1426	shkim@kisa.or.kr

발간일 2024년 8월 12일

기획·발간처 한국인터넷진흥원 정책연구실 정책연구팀

요약

미국의 주요 사회기반시설에 대한 사이버 공격 시도가 국가 경제와 안보에 미칠 위협에 대비하기 위해 대통령 행정명령을 발표하고 사이버보안 프레임워크를 개발

- 오바마 행정부는 「국가 주요 기반시설의 사이버 위협 대응 강화」를 위한 행정명령(EO 13636, '13.2월)을 발표하고, NIST는 동 행정명령에 따라 정부, 민간 부문과 협력하여 주요 기반시설의 사이버 보안 개선을 위한 프레임워크(Cybersecurity Framework 1.0, CSF 1.0) 개발
  - 프레임워크는 코어, 프로필, 구현 계층의 세 부분으로 구성되어 있으며, 비즈니스 관점에서 사이버보안 활동을 계획하고 조직의 위험 관리 프로세스의 일부로 사이버보안 위험을 고려
- 이후 트럼프 행정부는 「연방 네트워크와 주요 기반시설의 사이버보안 강화」를 위한 행정명령 (EO 13800, '17.5월)을 통해 정부 기관의 사이버보안 위험 관리에 CSF 도입을 의무화
  - NIST는 연방 기관의 프레임워크 도입 및 활용을 위한 8가지 구현 지침을 게시하고 ('17.5월), 기반시설 외의 조직에 프레임워크 적용 확대를 위한 개선안(CSF 1.1, '18.4월) 발표
  - 프레임워크를 활용한 조직의 사이버보안 위험 자체평가, 사이버 공급망 위험관리 범주 추가 등 업데이트

NIST는 사이버보안 환경변화와 국내외 활용 수요를 반영하고자 다양한 부문의 의견 수렴을 통해 사이버보안 프레임워크를 업데이트하여 공개(CSF 2.0, '24. 2월)

- CSF 2.0은 기존 프레임워크의 적용 범위를 확대하고, 핵심 기능 개편, 구현 사례제공 등 개선
  - '사이버보안 주요 인프라 개선을 위한 프레임워크'를 '사이버보안 프레임워크'로 명칭 변경
- ▲적용범위 확대(주요 기반시설 → 모든 조직), ▲거버넌스 강조('관리 govern' 기능 추가) 및 공급망 위험관리 강화, ▲분류항목 업데이트(23개의 카테고리를 22개로, 108개의 세분류를 106개로 조정)
- 더불어 NIST 웹사이트를 통해 ▲참조 정보, ▲구현 사례, ▲퀵 스타트 가이드 등 소규모 조직이나 조직 내 특정 부문에서 CSF 도입 및 구현에 필요한 정보를 게시하고, 정기적으로 업데이트

CSF 2.0을 활용하여 조직의 사이버보안 위험 관리를 개선·효율화하고, 위험 관리체계에 사이버보안 위험 관리를 통합하며, 새로운 ICT 기술 환경에 적용할 수 있는 보안 프레임워크 제공

I

개발 배경

1-1 사이버보안 프레임워크 개발(CSF 1.0)

▌오바마 행정부는 미국의 주요 사회기반시설에 대한 사이버공격에 대비하기 위하여 「국가 주요 기반시설의 사이버 위협 대응 강화를 위한 행정명령(EO 13636)[1]」 발표('13.2월)

- 뱅크오브아메리카, 씨티그룹 등 미국 대형은행 웹사이트에 대한 DDoS 공격[2]('12.9월) 등 주요 기반시설에 대한 사이버공격 시도가 국가 경제와 안보에 심각한 위험으로 이어질 수 있다는 우려 확산

  - 이에 연방 기관과 주요 기반시설 운영 및 보유 업체 간의 사이버 위협정보 공유체계 구축, 사이버보안 프레임워크(Cybersecurity Framework) 개발을 핵심으로 하는 국가안보 강화를 위한 행정명령 발표

▌동 행정명령에 따라 NIST*는 주요 기반시설의 사이버 위험 감소를 위한 "사이버보안 프레임워크(CSF 1.0)[3]" 개발('14.2월)

* National Institute of Standards and Technology : 미국 상무부 산하 국립표준기술연구소

- NIST는 행정 각 부와 협력하여 취약점과 전문 기술정보를 공유하고, 개발 과정에 정부 기관, 기반시설 소유자와 운영자, 민간 등 이해관계자의 의견 수렴 과정을 통해 행정명령 공포 후 1년 만에 최종 보고서를 공개

- 사이버보안 프레임워크는 조직의 사이버보안 위험 관리를 위한 기술 중립적이며 비용 효율적인 위험 기반 접근방식의 가이드라인

  - 정책, 비즈니스, 기술적 접근에 부합하는 표준, 방법론, 절차, 프로세스를 제시하고, 민간 부문의 자발적 합의에 기초하여 기존의 국내 및 국제 표준, 산업계 모범사례를 반영

---

1) Whitehouse, "Improving Critical Infrastructure Cybersecurity", 2013.02.12.

2) The New York Times, "American Banks Undamaged by Cyberattacks", 2012.09.26.

3) NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0", 2014.02.12.

1-2 사이버보안 프레임워크 개선(CSF 1.1)

▌트럼프 행정부는 사이버보안 프레임워크를 연방 정부기관의 위험 관리에 의무 적용하는 내용을 골자로 하는 「연방 네트워크 및 중요 기반시설의 사이버보안 강화를 위한 행정명령(EO 13800)[4]」 발표('17.5월)

- 트럼프 행정부는 '사이버보안조정관(cybersecurity coordinator)'을 폐지하고 국토안보부(DHS, U.S. Department of Homeland Security) 중심의 사이버안보 역량 강화 추진
- 연방 기관은 사이버보안 프레임워크를 사이버 위험 관리에 도입하고 행정명령 발표 후 90일 이내에 국토부 장관 및 예산관리국장(OMB Director)에게 위험관리보고서를 제출해야 함

▌동 행정명령에 따라 NIST는 연방정부 기관들의 사이버보안 프레임워크 도입 및 활용을 위한 8가지 구현 지침('17.5월)을 게시하고,[5] 프레임워크의 적용 분야 확대를 위한 개선안[6] 발표(CSF 1.1, '18.4.16)

- 구현지침은 ① 조직의 위험 관리와 사이버보안 위험 관리 통합, ② 사이버보안 필요 요건 관리, ③ 사이버보안 및 구매 프로세스 통합 및 일치, ④ 조직의 사이버보안 평가, ⑤ 사이버보안 프로그램 관리, ⑥ 사이버보안 위험에 대한 전반적인 이해 유지, ⑦ 사이버보안 위험 보고, ⑧ 맞춤화된 프로세스 고지 등 8가지 내용을 담고 있음
- CSF 1.1은 주요 기반시설의 사이버보안 강화를 위한 프레임워크를 연방정부 기관의 보안 위협 점검을 위한 목적으로 확대
  - 또한 ① 인증 및 신원관리를 위한 포괄적인 통제, ② 사이버보안 위험 자체평가, ③ 공급망 내의 사이버보안 관리, ④ 취약점 공개(vulnerability disclosure) 업데이트 및 컴플라이언스 등 다양한 의미로 해석될 수 있는 용어 정비

〈표 1〉 사이버보안 프레임워크 1.0과 1.1 비교

구분	CSF 1.0	CSF 1.1
개발 근거	행정명령 13636('13.2월)	행정명령 13800('18.4월)
적용 대상	주요 기반시설	주요 기반시설, 연방정부 기관
주요 내용	• 사이버보안 정보공유체계 구축 • 개인정보 및 시민의 자유 보호 • 주요 기반시설 사이버보안 개선을 위한 합의 절차 수립 • **주요 기반시설 위험 감소를 위한 기본 프레임워크 개발** • 자발적인 주요 기반시설 사이버보안 프로그램 수립	• **연방 네트워크 사이버보안을 위한 연방 IT 인프라 현대화** • 중요 인프라 사이버보안 강화 – 고위험 중요 인프라 식별·지원 – 중요 인프라 사이버보안 위험 관리 관행 공개 • 국가 사이버보안 강화를 위한 국제 협력, 인력양성

출처) 백악관 발표 자료 재구성

4) Whitehouse, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", 2017.05.16.

5) 한국인터넷진흥원, "NIST의 사이버 보안 프레임워크 주요 내용". 2018.09. 재인용

6) NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1", 2018.04.16.

II

사이버보안 프레임워크 2.0 주요 내용

2-1 개 요

CSF 2.0은 사이버보안 환경의 변화를 반영하여 다양한 유형과 규모의 조직을 대상으로 사이버보안 위험평가, 개선 및 관리를 위해 활용할 수 있는 체계적인 방법론을 제시

- CSF는 분야, 국가, 기술 중립적이며 사이버보안 위험에 대한 이해, 평가, 우선순위, 의사소통을 위한 리소스를 제공하여 다양한 이해관계자가 이해할 수 있는 바람직한 상태를 설명
  - 조직 전체 또는 일부의 현재 또는 목표한 사이버보안 태세를 **설명**, 격차를 **이해**하고 격차를 좁히기 위한 진전을 평가
  - 조직의 임무, 법과 규칙 요구사항, 위험 관리 및 거버넌스 기대사항과 맞추어 사이버보안 위험을 관리하기 위한 **식별, 조직화, 우선순위 결정**
  - 조직 안팎으로 경영진, 관리자, 실무자 등 사이버보안 전문성과 무관하게 위험, 역량, 필요성, 기대에 대하여 의사소통하기 위한 **공통 언어를 제공**

CSF 2.0은 기존 프레임워크의 적용 범위 확대, 핵심 기능 개편 및 구현 사례 제공 등 개선

- ①적용범위 확대(주요 기반시설→모든 조직), ②거버넌스 강조('관리 govern' 기능 추가) 및 공급망 위험관리 강화 ③분류항목 업데이트(분류 23개→22개, 소분류 108→106개)
  - '사이버보안 중요 인프라 개선을 위한 프레임워크'를 '사이버보안 프레임워크'로 변경하고 주요 기반시설 외에 다양한 조직 및 국외에서도 활용할 수 있도록 수정
- NIST 웹사이트를 통해 ① 참조 정보, ② 구현 사례, ③ Quick Start Guide를 제공하여 소규모 조직이나 조직 내 특정 부문에서도 CSF를 쉽게 도입하고 활용할 수 있도록 가이드 제공 및 업데이트
  - 현행 국제 표준, 지침, 프레임워크, 규제 등과 CSF 간의 매핑을 통해 사이버보안 결과 달성을 위한 공통정보 제공
  - 코어의 세분류에 제시된 사이버보안 활동 결과를 달성하기 위한 행동 절차를 개념적으로 설명하기 위하여 구현 예시 추가

• 사이버보안 측정 및 평가에 대한 이해를 명확히 하고자 NIST의 새로운 정보보호 평가 지침(SP 800-55, Measurement Guide for Information Security)에 따라 현행화하고 거버넌스, 위험 관리, 제3자 고려사항을 중심으로 계층을 명확하게 구분

〈표 2〉 사이버보안 프레임워크 2.0 주요 개선사항

		기존(1.1)	개선(2.0)
①**적용범위 확대**		병원, 발전소 등 주요 기반시설 및 연방 정부 기관	유형·규모에 관계없이 모든 조직에 적용
②**관리 추가**	기능	식별, 보호, 탐지, 대응, 복구(5개)	**거버넌스(신규)**, 식별, 보호, 탐지, 대응, 복구(6개)
③**환경변화에 따른 업데이트**	분류	**23개**	**22개**
		1. 식별(6개) : 자산관리, 사업환경, 거버넌스, 위험평가, 위험관리 전략, 공급망 위험관리(이동)	1. 식별(3개) : 자산관리, 위험평가, 개선
		2. 보호(6개) : ID 관리 및 접근제어, 인식교육 및 훈련, 데이터 보안, 정보보호 추진절차, 유지보수, 보호기술	2. 보호(5개) : ID 관리 및 접근제어, 인식교육 및 훈련, 데이터 보안, 플랫폼 보안, 기술 인프라 탄력성
		3. 탐지(3개) : 이상징후 및 이벤트, 지속적인 보안 모니터링, 탐지 절차	3. 탐지(2개) : 부작용 분석, 지속적인 모니터링
		4. 대응(5개) : 대응 계획, 커뮤니케이션, 분석, 피해완화, 개선	4. 대응(4개) : 사고관리, 사고분석, 사고 대응 보고 및 정보공유, 사고 완화
		5. 복구(3개) : 복구계획, 개선, 커뮤니케이션	5. 복구(2개) : 사고복구 계획 실행, 사고 복구 정보공유
			6. 거버넌스(6개) : 조직관리, 위험관리전략, 역할 · 책임 및 권한, 정책, 감독, 사이버보안 공급망 위험 관리
	세분류	**108개**	**106개**
		개인정보보호, 공급망 위험관리, 인공지능 위험관리 강화 등을 위한 내용을 업데이트하여 분류별로 사이버보안 활동 소분류 제공	

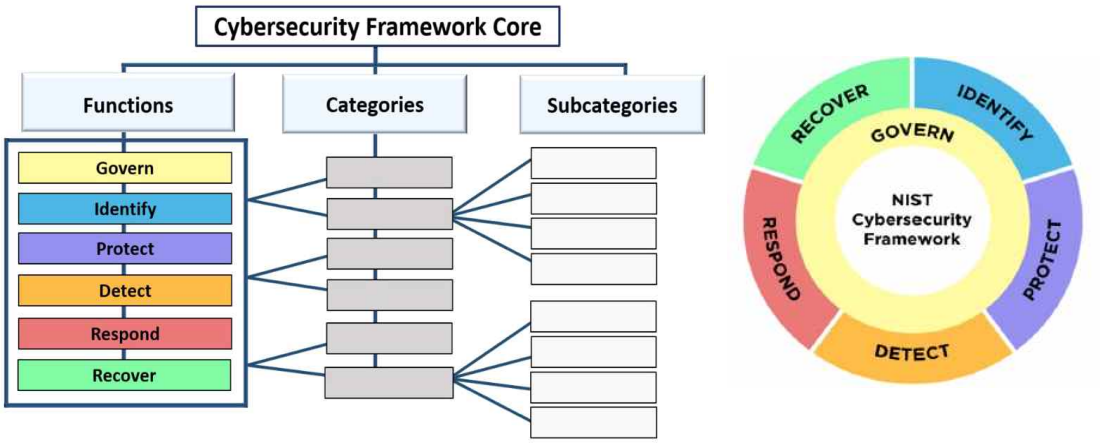
출처) NIST 발표 자료 재구성

2-2 CSF 2.0 구성 요소(코어, 조직 프로필, 구현 계층)

CSF 코어core는 모든 조직이 사이버보안 위험을 관리할 수 있도록 지원하는 상위 수준의 사이버보안 활동 결과를 기능(function), 분류(category), 세분류(subcategory)로 계층화

- CSF 코어는 IT, IoT, OT 모든 ICT와 클라우드, 모바일, 인공지능 시스템 등 다양한 기술 환경에 적용할 수 있음

[그림 1] CSF 코어의 구조와 6가지 기능(functions)



출처) NIST

- 기능 : 최상위 수준의 사이버보안 활동 결과를 6가지로 구분하여 구조화하며, 모든 기능은 유기적으로 작동하며 동시에 처리되기 때문에 휠 형태로 표현할 수 있음

  - 관리 Govern : 조직의 역할, 이해관계자의 기대 등을 고려하여 다른 5대 기능의 결과 달성 및 우선순위 선정을 위한 활동을 제시하며, 기업 위험 관리(Enterprise Risk Management, ERM) 전략에 사이버보안 위험 관리를 통합할 수 있도록 지원

〈표 3〉 CSF 2.0 거버넌스(Govern) 기능 內 주요 내용

분류(식별코드)	정의
조직 관리(GV.OC)	조직의 사이버보안 위험관리 결정을 위한 조직환경(임무, 이해관계자의 기대, 법적 규제, 계약 요구사항 등)에 대한 이해
위험 관리 전략(GV.RM)	조직의 우선순위, 제약조건, 위험 허용 범위 및 선호도 등 운영에 대한 위험 결정을 지원하기 위한 전략적 방향 수립 및 논의
역할·책임 및 권한(GV.RR)	사이버보안 관련 책임성, 성과 평가, 지속적인 개선을 촉진하기 위한 역할, 책임 및 권한 확립
정책(GV.PO)	조직의 사이버보안 정책, 절차를 수립하여 시행
감독(GV.OV)	조직 전반의 사이버보안 위험 관리 성과 검토를 통해 전략적 방향 수립 및 조정
사이버보안 공급망 위험 관리(GV.SC)	사이버보안 공급망 위험 관리 절차는 조직의 이해관계자를 통해 식별, 확립, 관리, 모니터링 및 개선

- 식별 Identify : 하드웨어 · 소프트웨어 · 시설 · 인력 등 조직의 자산 분류 및 공급업체의 사이버보안 위험에 대한 이해 등 ERM 및 '관리'를 통해 식별된 요구사항에 부합하는 활동의 우선순위 지정
- 보호 Protect : 사이버보안 사고의 발생 가능성과 영향을 예방 또는 감소시키기 위한 사이버보안 위험 관리 활동
- 탐지 Detect : 침해 지표, 잠재적인 사이버보안 위협 사건을 적시에 발견·분석하여 성공적인 사고 대응 및 복구 활동 지원
- 대응 Respond : 탐지된 사이버보안 사고에 대한 조치를 통해 사고의 영향을 억제
- 복구 Recover : 정상적인 운영을 위한 사이버보안 사고의 시의적절한 복구를 통해 사이버보안 사고 영향력 감소

• 분류 : 각 기능을 구성하는 사이버보안 활동의 결과를 그룹화

• 세분류 : 각 분류를 구체적인 기술 및 관리 활동을 통한 결과로 세분화

〈표 4〉 대응 기능에 대한 분류 및 세분류 예시

기능	분류	세분류
대응(RS)	사고 관리(RS.MA) 탐지된 사이버보안 사고에 대한 대응을 관리	
		01 : 사고가 확인되면 관련된 제3자와 협력하여 사고 대응 계획을 실행 02 : 사고 보고서를 분류하고 검증 03 : 사고가 분류되어 우선순위 지정 04 : 사고는 필요에 따라 격상되거나(elevated) 상승됨(escalated) 05 : 사고 복구의 시작기준이 정해짐

참고 1 사이버보안 프레임워크 2.0 코어

▌코어는 6가지 기능, 22개 분류, 106개 세분류로 구성되며 각 기능은 연속적으로 동시에 작동

- 프레임워크 2.0에서는 사이버보안 위험 관리를 기업 위험 관리의 일부로 통합하기 위하여 '거버넌스'를 기능으로 분류하고, 공급망 위험 관리를 통합 · 확장하여 거버넌스로 기능에 편성
- 지속적인 개선의 중요성을 고려하여 '식별' 기능 內 개선(ID.IM) 분류를 신설

기능	분류(식별코드)	세분류
6개	22개	106개
관리 (Govern, GV)	▸ 조직의 사이버보안 위험관리 전략, 기대, 정책의 수립·전달·모니터링	
	조직관리 Organizational Context (GV.OC)	5
	위험 관리 전략 Risk Management Strategy (GV.OC)	7
	역할, 책임 및 권한 Roles, Responsibilities, and Authorities (GV.RR)	4
	정책 Policy (GV.PO)	2
	감독 Oversight (GV.OV)	3
	사이버보안 공급망 위험 관리 Cybersecurity Supply Chain Risk Management (GV.SC)	10
식별 (Identify, ID)	▸ 조직의 현재 사이버보안 위험에 대한 이해	
	자산관리 Asset Management (ID.AM)	7
	위험 평가 Risk Assessment (ID.RA)	10
	개선 Improvement (ID.IM)	4
보호 (Protect, PR)	▸ 조직의 사이버보안 위험 관리를 위한 조치 실행	
	ID 관리, 인증, 접근제어 Identity Management, Authentication, and Access Control (PR.AA)	6
	인식교육 및 훈련 Awareness and Training (PR.AT)	2
	데이터 보안 Data Security (PR.DS)	4
	플랫폼 보안 Platform Security (PR.PS)	6
	기술 인프라 복원력 Technology Infrastructure Resilience (PR.IR)	4
탐지 (Detect, DE)	▸ 가능한 사이버보안 공격 및 손상을 발견하고 분석	
	지속적인 모니터링 Continuous Monitoring (DE.CM)	5
	부정적 이벤트 분석 Adverse Event Analysis (DE.AE)	6
대응 (Respond, RS)	▸ 탐지된 사이버보안 사고에 대한 조치 실행	
	사고 관리 Incident Management (RS.MA)	5
	사고 분석 Incident Analysis (RS.AN)	4
	사고 대응 보고 및 공유 Incident Response Reporting and Communication (RS.CO)	2
	사고 완화 Incident Mitigation (RS.MI)	2
복구 (Recover, RC)	▸ 사이버보안 사고에 영향을 받은 자산과 운영 복원	
	사고복구 계획 실행 Incident Recovery Plan Execution (RC.RP)	6
	사고복구 공유 Incident Recovery Communication (RC.CO)	2

▌조직 프로필(Organizational Profile)은 '코어'의 결과 관점에서 조직이 수행하고 있는 사이버보안 활동의 현재와 목표 상태를 설명하는 체계

- 조직의 요구사항, 이해관계자의 위험 허용 한계치, 조직의 리소스 등을 고려하여 기능별 목표 달성 수준과 현황을 작성하고 로드맵 수립

– 현재 프로필 : 조직이 현재 달성한(달성하고자 하는) 코어의 결과를 자세히 설명하고, 각 결과가 어느 정도 또는 어떻게 달성되었는지 특성화

– 목표 프로필 : 조직이 사이버보안 위험 관리 목적을 달성하기 위하여 선택하고 우선순위로 정한 바람직한 결과를 설명. 새로운 요구사항, 새로운 기술 도입, 위협 인텔리전스 추세 등 조직의 사이버보안 태세에 대한 예상되는 변화를 고려

[그림 2] 단계별 CSF 조직 프로필 생성 및 활용

① 조직 프로필의 범위 지정
② 조직 프로필 작성에 필요한 정보* 수집
* 정책, 위험 관리 우선순위, 자원, 기업 위험 프로필, 비즈니스 영향 분석(BIA) 등
③ 조직 프로필 생성
④ 현재-목표 프로필 격차 분석 및 실행 계획 수립
⑤ 실행 계획 구현 및 조직 프로필 업데이트

① 프로필 범위 정의의 기반이 될 상위 수준의 사실과 가정을 문서화. 조직은 각각 다른 범위를 갖는 조직 프로필을 원하는 대로 만들 수 있음(전체 조직 또는 일부 금융 시스템, 랜섬웨어 위협 대응, 금융 시스템 관련 랜섬웨어 사고 처리 등)

② 조직의 정책, 위험 관리 우선순위 및 재원, 기업 위험 프로필 비즈니스 영향 분석(BIA), 사이버보안 요구사항 및 표준, 관행 및 도구(절차 및 보호장치), 담당 업무

③ 선택한 CSF 결과를 포함하기 위한 정보의 유형이 무엇인지 결정하고 필요한 정보를 문서화. 목표 프로필 계획 및 우선순위 지정 정보를 제공하기 위해 현재 프로필의 위험 영향을 고려하고, 목표 프로필의 기저선으로 커뮤니티 프로필을 고려

④ 현재-목표 프로필의 간의 차이를 식별, 분석하기 위해 격차 분석을 실시하고, 이를 해결하기 위해 우선순위가 지정된 실행 계획(리스크 레지스트리, 리스크 디테일 리포트, 실행 계획 및 마일스톤(POA&M) 개발

⑤ 실행 계획은 전체 기한이 있거나 진행중일 수 있음

- 지속적인 개선을 위해 필요할 때 이 단계를 반복할 수 있으며, 프로필을 활용하여 사이버보안 기능 및 개선 기회를 비즈니스파트너, 잠재 고객 등 외부 이해관계자에게 문서로 공유하거나 조직의 사이버보안 위험 관리 요구사항 및 기대치를 공급업체, 협력사 등에 설명할 수 있음

▌구현 계층(Tier)은 조직 프로필을 통해 도출된 사이버보안 위험 거버넌스와 관리 현황을 네 개의 계층으로 구분하여 조직의 사이버보안 위험 거버넌스 및 관리 관행의 특징을 명확하게 제시

- 각 계층은 조직의 사이버위험 관리 관행을 ①부분적, ②위험정보 공유, ③반복적, ④적응 단계로 설명하며, 비공식적, 임기응변식 대응에서 민첩하고 위험정보에 기반한 지속적인 개선으로 발전
- 구현 계층을 활용하여 조직의 현재 및 목표 프로필에 대한 정보를 공유할 수 있으며, 조직의 기존 위험 관리 방법론을 보완

– 구현 계층을 활용하여 조직의 현재 및 목표 프로필을 알리고, 조직의 기존 위험 관리 방법론을 보완할 수 있음

– 사이버보안 위험을 줄일 수 있는 경우 더 높은 계층으로의 이동이 권장됨

[그림 3] **사이버보안 위험 거버넌스 및 관리를 위한 CSF 구현 계층**

참고 2 CSF 구현 계층의 개념 예시

▌구현 계층은 사이버보안 위험 거버넌스와 관리의 특성을 개념화하여, 사이버보안 위험을 관리하는 조직의 관행과 프로세스를 이해하고 벤치마크 할 수 있는 도구를 제공

- 계층을 활용하여 조직의 현재 및 목표 프로필에 대한 정보 및 사이버 성숙도 수준을 공유할 수 있으며, 조직의 사이버보안 위험을 관리하는 방법에 대한 조직 전체의 방향성을 설정할 수 있음

계층	사이버보안 위험 거버넌스	사이버보안 위험 관리
계층 1 : 부분 적용	‣ 조직의 사이버보안 위험 전략 및 우선순위는 임시적이며, 공식적으로 목표나 위협 환경에 근거하지 않음	‣ 조직의 보안 위험 인식 수준이 낮음 ‣ 비정기적, 사례별 사이버보안 위험 관리 구현 ‣ 내 · 외부 협력 및 정보공유체계 미흡 ‣ 공급업체, 제품 및 서비스에 대한 위험을 인식하지 못함
계층 2 : 위험정보 활용	‣ 관리자가 위험 관리 절차 승인, 전사적으로 적용되지 않음 ‣ 사이버보안 활동과 보호 요구사항 우선순위는 조직의 목표, 위협 환경, 비즈니스 요구사항 등에 반영됨	‣ 조직 차원의 위험 인식은 있으나, 전사적 접근방식은 확립되지 않음 ‣ 조직, 외부 자산에 대한 사이버위험 평가를 실시하지만 반복하지 않음 ‣ 내부 관계자간 비정기적 정보공유 ‣ 공급업체, 제품 및 서비스에 대한 위험을 인지하나, 일관된 공식 조치는 취하지 않음
계층 3 : 위험정보 활용/ 반복	‣ 조직 차원의 위험 관리 절차가 공식적으로 승인, 정책으로 수립됨 ‣ 위험 정보 정책, 프로세스, 절차가 의도에 맞게 정의, 구현, 검토됨 ‣ 위협, 기술환경 변화 등에 따라 위험관리 절차를 정기적으로 업데이트	‣ 조직 차원의 일관된 위험 관리 방식 적용, 직원들은 역할 · 책임에 대한 지식 보유 ‣ 자산에 대한 지속적인 위험 모니터링, 내 · 외부 정보공유가 원활함 ‣ 조직의 위험 전략은 공급업체, 제품 및 서비스와 관련된 사이버보안 위험에 따라 결정 ‣ 서면 계약/위험 위원회, 정책 구현, 모니터링 등을 통해 공식적인 조치를 취하며 지속적으로 모니터링 및 검토
계층 4 : 적응	‣ 전사적 위험 관리 전략이 확립되어 조직 문화의 일부로 수용됨 ‣ 경영진은 재무나 기타 조직의 위험과 동등한 맥락으로 사이버보안을 관리 ‣ 현재와 미래의 위험환경과 위험 허용범위에 대한 이해에 기반한 조직 예산	‣ 위협, 기술 발전에 대한 지속적인 분석실시 및 위험 관리에 활용 ‣ 광범위한 조직 내·외부 정보공유체계 확립

2-6 온라인을 통한 정보 제공

▌NIST는 CSF에 대한 조직의 이해, 도입, 활용을 지원하기 위하여 온라인으로 ①참조 정보, ②구현 사례, ③퀵 스타트 가이드를 제공하고 정기적으로 업데이트

- 참조 정보(Informative references): 코어의 결과 달성을 위해 현행 국제 표준, 지침, 프레임워크, 규제, 정책 등과 CSF의 지침을 상호 참조할 수 있도록 매핑 정보를 제공

* 예) 관리, 위험 관리 전략(GV.OC)-01 → CRI Profile Version 2.0

- 구현 사례 : 세분류에 제시한 결과를 달성하기 위한 개념적, 행위 중심(공유, 문서화, 개발, 모니터링, 분석, 평가, 실행 등)의 사례를 단계적으로 설명

[그림 4] CSF 세분류의 구현 사례(implementation examples) 예시

Function	Category	Subcategory	Implementation Examples	Informative References
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored				**CRI Profile Version 2.0: GV** **Information and Communications Technology (ICT) Risk Outcomes: GV.PO**
	Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood			**CRI Profile Version 2.0: GV.OC** **Information and Communications Technology (ICT) Risk Outcomes: GV.CT** **Information and Communications Technology (ICT) Risk Outcomes: GV.CT-5**
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**1st**: 1st Party Risk **Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	**CRI Profile Version 2.0: GV.OC-01** **CRI Profile Version 2.0: GV.OC-01.01** **Information and Communications Technology (ICT) Risk Outcomes: GV.CT-5** **Information and Communications Technology (ICT) Risk Outcomes: GV.CT-3**

출처) NIST

- 퀵 스타트 가이드 : 특정한 CSF 관련 주제를 조직의 사이버보안 개선 또는 사이버보안 위험 관리 과정에서 고려할 수 있는 실행 가능한 “첫 번째 단계” 로 추려낸 간략한 문서

– 조직 프로필 및 구현 계층 작성, 커뮤티니 프로필 구성, 중소기업을 위한 맞춤형 정보, 조직이 기술 제품 및 서비스를 스마트하게 인수하고 공급하기 위한 C-SCRM 시작 방법, ERM 실무자가 CSF 2.0을 활용하여 조직의 사이버보안 위험 관리를 개선하기 위한 기업위험관리 방법 등을 제공

※ 커뮤니티 프로필 : 여러 조직 간의 관심사와 목표를 공유하기 위해 작성, 게시된 CSF 결과의 기준. 특정 부문, 하위 부문, 기술, 위협 유형, 활용 사례에 따라 개발되어 조직은 자신의 목표 프로필 기저선으로서 커뮤니티 프로필을 활용할 수 있음

III

사이버보안 위험정보 공유체계 및 통합 개선

▌사이버보안 프레임워크를 활용하여 조직의 임무, 이해관계자의 기대, 위험 수용도 및 위험 허용범위를 이해하면, 사이버보안 지출과 활동을 결정하기 위한 우선순위를 정할 수 있음

- 조직은 잠재적 영향과 가능성에 따라 부정적 위험의 완화, 이전, 회피, 수용 및 긍정적 위험의 인식, 공유, 강화, 수용 등 한 가지 이상의 방법으로 위험을 처리할 수 있음
- 조직은 CSF를 활용하여 조직 내부의 사이버보안 기능을 관리할 수 있으며, 외부적으로 외주업체 등 제 3자를 감독하거나 의사소통할 수 있음
- CSF를 도입하지 않더라도 사이버보안 위험 및 위험 관리 조치에 대한 이해, 평가, 우선순위 지정 및 정보를 공유하기 위한 지침으로 활용할 수 있음
- 또한 우선순위와 가용 자원을 고려하여 사이버보안 상태 개선 및 고유한 임무의 필수 기능에 대한 연속성 유지를 위한 전략적 결정에 집중, 구현하는데 활용할 수 있음

3-1 위험 관리 정보공유체계 개선

CSF는 사이버보안에 대한 기대, 계획, 자원에 관한 정보공유 향상을 위한 기반 제공

- 조직의 우선순위 및 전략 방향에 중점을 두는 경영진, 조직의 목표 달성에 영향을 미칠 수 있는 사이버보안 위험을 관리하는 관리자, 사이버보안 기술을 구현 · 운영하는 실무자 간의 정보공유를 촉진
- '관리' 기능을 통해 **경영진**과 조직의 위험정보 공유를 촉진, **관리자**는 경영진이 설정한 전체 사이버보안 목표를 통보하고 단계적으로 전달하며, **실무자**는 특정 사이버보안 활동을 계획, 이행, 모니터링하기 위해 목표 상태 구현 및 운영상의 위험 변화 측정에 집중

[그림 5] CSF를 통한 위험 관리 의사소통 개선

출처) NIST

- 조직 프로필 생성 및 사용을 위해 관리자는 경영진으로부터 조직의 우선순위, 자원, 위험 방향에 대한 정보를 수집한 후 실무자와 협력하여 비즈니스 요구사항을 공유하고 위험정보를 활용한 조직 프로필 생성
- 관리자와 실무자는 현재와 목표 프로필 간의 격차를 줄이기 위한 조치를 구현하고 시스템 수준의 계획에 필요한 핵심 정보를 제공
- 시스템 수준의 제어, 모니터링을 포함하여 조직 전체의 목표 상태에 도달하면 위험 등록부와 진행 리포트를 업데이트하여 공유할 수 있으며, 관리자는 잠재적인 피해 감소 및 이익 확대를 위한 조정에 필요한 인사이트를 확보

3-2 위험 관리 프로그램과의 통합 지원

▌사이버보안 프레임워크는 사이버보안 및 사이버보안 위험 관리에 대한 용어를 경영진이 이해할 수 있는 일반적인 위험 관리 용어로 제시

- NIST는 사이버보안 위험 관리와 ERM 간의 상호 관계를 설명하는 다양한 리소스를 제공하며, 조직은 개별 ICT 위험 관리 프로그램과 CSF를 통합하여 유익한 정보를 얻을 수 있음

- 사이버보안 위험 관리와 ERM 간의 상호 관계를 설명하는 NIST의 리소스

▸ NIST 사이버보안 프레임워크 2.0 –기업 위험 관리 Quick-Start 가이드
▸ 사이버보안과 기업 위험 관리(ERM) 통합(NIST IR 8286)
▸ 기업 위험 관리를 위한 사이버보안 위험 식별 및 평가(NIST IR 8286A)
▸ 기업 위험 관리를 위한 사이버보안 위험 우선순위 선정(NIST IR 8286B)
▸ 기업 위험관리 및 거버넌스 감독을 위한 사이버보안 위험 단계화(NIST IR 8286C)
▸ 비즈니스 영향 분석을 통한 위험 우선순위 지정 및 대응 정보 제공(NIST IR 8286D)
▸ ICT 위험이 기업에 미치는 영향 : 기업 위험 포트폴리오 내 ICT 위험 프로그램 거버닝 및 관리(SP 800-221)
▸ ICT 위험의 결과 : ICT 위험 관리 프로그램의 기업 위험 포트폴리오 통합(SP 800-221A)

▌사이버보안 프레임워크를 활용하여 사이버보안 위험 관리와 개별 ICT 위험 관리 프로그램을 통합할 수 있음

- 사이버보안 위험 관리 및 평가

– 정보 시스템과 조직을 위한 위험 관리 프레임워크(SP 800-37) 및 NIST 위험 관리 프레임워크(RMF)의 위험 평가 수행 지침(SP 800-30) 등 사이버보안 위험 관리와 평가 프로그램 통합

– CSF는 “정보 시스템과 조직의 보안 및 프라이버시 통제(SP 800-53)”에서 선택 및 우선순위 지정을 컨트롤하는 RMF의 접근법을 보완하는데 사용할 수 있음

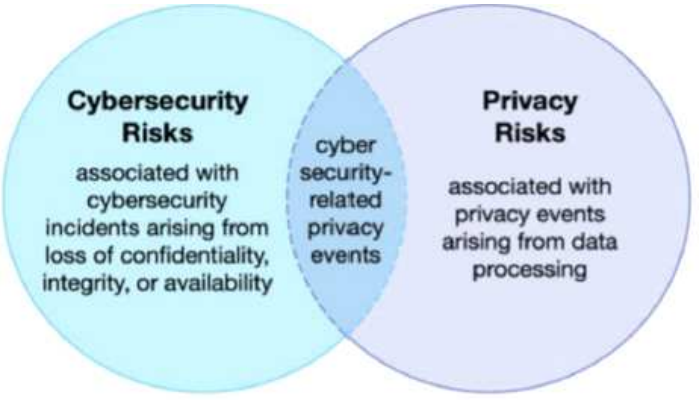
- 프라이버시 위험

– 사이버보안 위험과 개인정보 보호는 독립적인 분야지만 사이버보안 위험 관리는 데이터의 기밀성, 무결성 및 가용성 손실에 관계된 개인정보보호 위험을 해결하는 데 필수적으로 상황에 따라 목표가 중첩될 수 있음

– 조직의 임무 또는 비즈니스 목표 달성을 위한 데이터 처리 과정에서 개인정보보호 이벤트가 발생할 수 있으며, 해당 이벤트의 스펙트럼은 존엄성(낙인 등)에서부터 실질적 피해(차별, 경제적 손실, 신체적 피해 등)까지 광범위함

- NIST의 개인정보 프레임워크와 사이버보안 프레임워크를 함께 활용하여 위험의 다양한 측면을 해결할 수 있으며, 개인정보 위험평가 방법론(PRAM)을 활용하여 개인정보 위험평가 시 발생하는 문제를 목록화할 수 있음

[그림 6] 사이버보안과 개인정보 위험의 관계



출처) NIST

- 공급망 위험: 조직은 CSF를 활용하여 공급망 전반에 걸쳐 사이버보안 위험 감독 및 이해관계자와의 정보공유를 강화할 수 있음
  - CSF C-SCRM(GV.SC) 소분류는 온전히 사이버보안과 C-SCRM에 중점을 중점을 둔 결과를 제시하며, 시스템 및 조직을 위한 사이버보안 공급망 위험 관리 실무(SP 800-161r1)는 C-SCRM에 대한 심층 정보 제공
- 새로운 기술로 인한 위험: 인공지능 위험관리 프레임워크(AI RMF)의 코어는 기능, 분류, 세분류를 통하여 AI 결과를 설명하고 AI와 관련된 위험을 관리할 수 있음

3-3 국내 정보보호 프레임워크와 비교

NIST의 사이버보안 프레임워크와 국내 정보보호 관리체계 인증(ISMS), 개인정보보호 관리체계 인증(ISMS-P), 클라우드서비스 보안인증(CSAP) 제도를 비교 분석

- **('관리' 기능)** 국내 정보보호 인증체계는 경영진의 참여, 조직 구성, 정책 수립 등 정보보호 거버넌스 구현을 인증기준으로 관리하고 있음
- **(공급망 위험관리)** CSAP는 공급망 관리정책, 공급망 변경 관리 등 '서비스 공급망 관리'가 인증항목에 포함되어 있으며, ISMS에는 명시되어있지 않음
- **(의무화)** NIST의 CSF는 주요 기반시설 및 연방 정부 기관 도입을 의무화하고 있으며, ISMS는 기업의 규모, 업종에 따라 법적 인증을 의무화하고 있음

〈표 5〉 CSF와 국내 사이버보안 인증제도 비교

구분	CSF	정보보호/개인정보보호 관리체계인증 (ISMS/ISMS-P)*	클라우드서비스 보안인증(CSAP)
대상	▸ 모든 조직	▸ 모든 조직	▸ 클라우드 서비스 사업자
목적	▸ 기업의 사이버보안 위험 거버넌스 및 위험 관리 지침 제공	▸ 기업의 정보보호 · 개인정보보호조치에 대한 인증기준 적합성 평가	▸ 민간 클라우드 서비스의 안전성 · 신뢰성 검증을 위한 보호조치에 대한 인증기준에 적합성 평가
의무 대상	▸ 병원, 발전소 등 주요 기반시설 및 연방 정부 기관	▸ ISP, IDC, 병원 · 학교, 정보통신 서비스 제공자	▸ 공공 및 행정기관 서비스 제공 시 필요
분류 (인증) 체계	▸ 관리, 식별, 보호, 탐지, 대응, 복구 6개 기능, 23개 분류, 106개 소분류	▸ ISMS : 관리체계 수립 및 운영, 보호대책 요구사항 2개 영역, 80개 인증기준 ▸ ISMS-P : 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항 3개 영역, 101개 인증기준	▸ IaaS : 관리적 · 물리적 · 기술적 및 공공기관용 추가 보호조치 14개 분야 116개 통제항목 ▸ SaaS : 관리적 · 기술적 및 공공기관용 추가 보호조치 – (표준)13개 분야, 79개 항목 – (간편)11개 분야, 31개 항목 ▸ DaaS : 관리적 · 물리적 · 기술적 및 공공기관용 추가 보호조치 14개 분야 110개 통제항목
기타	▸ 조직의 사이버보안 위험관리 구현 계층 (Tiers) 제시 ▸ 공급망 위험관리 지침 제공(10개 항목)	▸ 개인정보 처리단계별 세부적 관리지침 평가	▸ 공급망 보안관리 조치 평가(2~4개 항목)

* 행정기관 대상 전자정부 정보보호 관리체계(G-ISMS)는 '09년부터 운영되었으며, '14년 ISMS로 통합

IV

시사점

4-1 조직의 사이버보안 위험 관리 개선 및 효율화

CSF는 위험 기반 접근방식으로 조직의 현재 사이버보안 위험 관리 수준을 객관적으로 평가하고 목표 수준과의 격차 분석을 통해 목표 상태를 구현할 수 있는 절차와 사례를 제시

- 조직은 구현 단계(Tiers)를 활용하여 조직의 현재 사이버보안 성숙도를 평가하고, 식별된 개선 기회를 기반으로 목표 수준을 달성하기 위한 프로세스 및 구현 지침을 활용할 수 있음
- 체계적이고 포괄적인 프레임워크 활용을 통해 사이버보안 제어의 견고성을 강화하여 잠재적인 사이버보안 위험으로부터 조직의 비즈니스 연속성을 확보하는 등 사이버 복원력 강화
- 프레임워크를 사이버 보안 위험관리 도구로 활용하여 조직이 제공하는 서비스의 중요 활동을 결정하고 지출의 우선순위를 선정하여 투자 효과를 극대화할 수 있음
- 조직 프로필을 활용하여 현재 조직의 사이버보안 기능과 개선 기회를 비즈니스 파트너, 잠재적 고객 등 외부 이해관계자와 문서로 공유할 수 있으며, 목표 프로필은 조직의 사이버보안 위험 관리 요구사항과 기대치를 공급업체, 파트너 및 제3자에게 전달하는데 활용할 수 있음

  – 더불어 사이버보안에 대한 전문지식 없이도 경영진, 관리자, 실무자를 포함한 내·외부 이해관계자가 이해할 수 있는 사이버보안 관리 결과를 설명하는 공통 언어를 제공

- 다만 CSF는 조직의 사이버보안 위험 관리 수준 및 사이버보안 성숙도 평가를 위한 개념적인 구조를 설명하고 목표 수준 달성을 위해 참고할 수 있는 지침, 표준, 모범사례 등을 제공하지만, 명확한 절차, 의무 등은 제시하지 않아 가이드라인으로서의 한계가 있음

4-2 조직의 고유한 사이버보안 관리체계와의 조화

CSF는 조직이 사이버보안 관리 수준 향상을 위해 도입, 구축, 대체해야 할 의무를 제시하기보다 비용 효율적인 측면에서 기존의 절차를 보완하도록 설계됨

- CSF는 다른 프레임워크, 표준, 지침 및 모범 사례들을 조직의 기존 위험 관리 프로세스 및 사이버보안 프로그램에 중첩시켜 위험 접근방식의 격차를 확인하고 개선 로드맵 개발할 수 있도록 지원

CSF는 다양한 국가의 모든 조직이 사이버보안 위험을 관리하고 줄이는데 필요한 도구를 제공

- CSF는 사이버보안에 대한 공통 위험뿐만 아니라 조직의 위험 수용도 및 허용범위, 조직의 임무와 이를 달성하기 위한 목표 등에 따른 문제를 해결하는 데 필요한 유연한 접근방식을 허용하며, 사이버보안 위험 완화를 위해 즉시 고려할 수 있는 잠재적인 보안 제어 목록을 매핑
  - 재무, 개인정보, 공급망, 평판, 기술 또는 물리적 위험 등 기업의 다른 위험들과 함께 사이버보안 위험을 관리하는데 유용
- CSF 2.0을 도입하기 위해서는 국내 ICT 환경에 대한 이해와 정보보호 관련 법, 제도 등 규제환경에 대한 분석이 선행되어야 하며, 기존의 정보보호 인증체계에 대한 조정 및 확장 가능성을 고려해야 함

4-3 새로운 ICT 기술환경에 적용할 수 있는 보안 프레임워크 제공

CSF의 기능, 분류, 세분류는 IT, IoT, OT 등 조직의 모든 ICT에 적용할 수 있으며, 클라우드, 모바일, 인공지능 시스템 등 모든 유형의 기술 환경에 적용할 수 있음

- CSF는 기업 위험 관리와 사이버보안 위험 관리의 접점을 제공하며 사이버보안, 개인정보보호, 공급망 보안, 인공지능 등 개별 ICT 위험 관리와 사이버보안 위험평가 지침의 보완 및 통합을 지원
- 국내에서 인공지능 등 신기술 대응 보안 프레임워크 개발을 위해 CSF 체계 활용을 고려해볼 수 있음

www.kisa.or.kr

KISA INSIGHT

KISA 한국인터넷진흥원