

NIST 사이버보안 프레임워크 (CSF) 2.0

국립 표준 기술 연구소

본 출판물은 <https://doi.org/10.6028/NIST.CSWP.29.kor> 에서 무료로 이용할 수 있습니다

2024년 2월 26일

사이버보안 프레임워크(CSF) 2.0

국립 표준 기술 연구소

(National Institute of Standards and Technology)

2024년 2월 26일

번역: 곽병현 (The University of Tennessee in Knoxville)

감독: 이원재 (DNV Business Assurance Korea)

Translated by Byoungyeun Kwak (The University of Tennessee in Knoxville). Reviewed by Woenjae Lee (DNV, Cyber Security Assurance Assessor / ISO Senior Assessor). Translated with permission courtesy of the National Institute of Standards and Technology (NIST). Translation reviewed on behalf of NIST by TaikaTranslations LLC under contract {133ND23PNB770271}. Official U.S. Government Translation.

곽병현 번역(녹스빌 테네시 대학). 이원재 검토(DNV, 사이버보안보증평가사/ISO 선임평가사). 미국 국립 표준 기술원(NIST)의 허가를 받아 번역되었습니다. {133ND23PNB770271} 계약에 따라 공식 미국 정부 번역인 Taika Translations LLC에서 NIST를 대신하여 번역 검토했습니다.

판권 소유, 미 상무 장관.

본 간행물의 공식 영어 버전은 NIST: <https://doi.org/10.6028/NIST.CSWP.29> 에서 무료로 제공합니다

요약

NIST 사이버보안 프레임워크(The NIST Cybersecurity Framework, CSF) 2.0은 산업, 정부 기관 및 기타 조직이 사이버보안 위험을 관리할 수 있도록 지침을 제공합니다. 이 프레임워크는 조직의 규모, 산업 분야 또는 사이버보안 성숙도와 관계없이 모든 조직이 사이버보안 활동을 효과적으로 이해하고 평가하며, 우선순위를 지정하고 의사소통할 수 있도록 높은 수준의 사이버보안 결과 분류 체계를 제공합니다. 사이버보안 프레임워크(이하 CSF)는 특정 사이버보안 목표를 달성하는 방법을 규정하지 않습니다. 대신, 특정 목표를 달성하는데 사용할 수 있는 실천 방법과 통제 방안에 대한 추가 지침을 제공하는 온라인 자료들을 소개합니다. 본 문서는 CSF 2.0과 그 구성 요소들, 그리고 이를 활용할 수 있는 다양한 방법들을 설명합니다.

키워드

사이버보안; 사이버보안 프레임워크(CSF); 사이버보안 위험 거버넌스; 사이버보안 위험 관리; 기업 위험 관리; 프로파일; 구현 단계.

대상

CSF의 주요 대상은 사이버보안 프로그램을 개발하고 이끄는 책임자들입니다. 또한, 리스크 관리에 참여하는 경영진, 이사회, 기업 인수 전문가, 기술 전문가, 리스크 관리자, 법률 전문가, 인사 담당자, 사이버 보안 및 리스크 관리 감사인 등 다른 이해 관계자들도 유용하게 사용할 수 있습니다. 더불어, 정책을 수립하거나 이에 영향을 주는 사람들(예: 협회, 전문 기관, 규제 기관)이 사이버보안 리스크 관리의 우선순위를 정하고 이에 관하여 소통하는 데 도움을 줄 수 있습니다.

보충 내용

NIST는 조직이 CSF를 구현하는 데 도움이 될 추가 자원인 퀵 스타트 가이드(Quick Start Guides)와 커뮤니티 프로파일(Community Profiles)를 계속해서 구축하고 호스팅할 것입니다. 모든 자원은 NIST CSF 웹사이트([NIST CSF website](#))에서 공개적으로 제공됩니다. NIST CSF 웹사이트에서 참조할 추가 자원 관련 제안은 언제든지 cyberframework@nist.gov로 NIST로 보내주시십시오.

독자에게 알림

특히 언급되지 않는 한, 본 출판물에는 여기서 인용, 참조, 발췌한 문서를 전혀 포함시키지 않았습니다.

또한, CSF 2.0 이전 버전에서는 사이버보안 프레임워크가 '핵심 인프라 사이버보안 개선을 위한 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity)'라고 불렸으나, CSF 2.0에서는 이 명칭을 사용하지 않습니다.

감사의 글

CSF는 미국과 전 세계의 산업, 학계, 정부와의 다년간의 협력을 통해 얻은 결과입니다. NIST는 이 개정된 CSF에 기여한 모든 분들에게 감사드립니다. CSF 개발 과정에 대한 정보는 NIST CSF 웹사이트([NIST CSF website](#))에서 확인하실 수 있습니다. 또한, CSF 사용에 대한 경험 및 피드백을 언제든지 cyberframework@nist.gov로 NIST와 공유할 수 있습니다.

목 차

1. 사이버보안 프레임워크(CSF) 개요	1
2. CSF 코어 소개	3
3. CSF 프로파일 및 단계 소개	6
3.1. CSF 프로파일	6
3.2. CSF 단계	7
4. CSF를 보완하는 온라인 자원 소개	9
5. 사이버보안 위험 소통 및 통합 개선	10
5.1. 위험 관리 소통 개선	10
5.2. 다른 위험 관리 프로그램과의 통합 개선	12
부록 A. CSF 코어	15
부록 B. CSF 단계	24
부록 C. 용어집	26

그림 목차

그림 1. CSF 코어 구조	3
그림 2. CSF 기능	5
그림 3. CSF 조직 프로파일 생성 및 사용 단계	6
그림 4. 사이버보안 위험 거버넌스 및 관리를 위한 CSF 단계	8
그림 5. CSF를 사용하여 위험 관리 소통 개선	10
그림 6. 사이버보안과 개인정보 보호 위험 관계	13

머릿말

사이버보안 프레임워크(CSF) 2.0은 산업, 정부, 학계, 비영리 기관을 포함한 모든 규모와 부문의 조직이 사이버보안 위험을 관리하고 줄이는 것을 돕기 위해 설계되었습니다.. 이 프레임워크는 조직의 사이버보안 프로그램의 성숙도와 기술적 복잡성에 관계없이 유용합니다. 하지만, 이는 CSF를 모든 조직의 같은 방식으로 접근하여 사용하라는 뜻이 아닙니다. 각 조직은 공통적인 위험도 있고 고유의 위험도 있으며, 위험을 감수하는 정도와 허용 범위도 다르고, 특정한 임무와 그 임무를 달성하기 위한 목표도 다릅니다. 따라서 필연적으로 각 조직은 CSF를 구현하는 방식이 다를 수 있습니다.

이상적으로 CSF는 사이버보안 위험을 포함하여 재정, 개인정보, 공급망, 평판, 환경의 기술적 물리적 위험을 포함한 기업의 다른 위험을 다루는 데 사용됩니다.

CSF는 청중들의 사이버보안 전문 지식 정도와 상관없이 경영진, 관리자, 실무자를 포함한 광범위한 대상이 이해할 수 있도록 바람직한 결과를 *설명합니다*. 이러한 결과는 부문, 국가, 기술 중립적이기 때문에 조직에서 자신의 고유한 위험, 기술, 임무를 위한 고려 사항을 다루는 데 필요한 유연성을 제공합니다. 결과는 사이버보안 위험을 완화하기 위해 즉시 고려할 수 있는 잠재적 보안 통제 목록으로 직접 연결됩니다.

CSF는 구체적 지침을 처방하지 않지만, 사용자가 특정 결과에 대해 알아보고 선택하는 데 도움을 줍니다. 특정 결과를 달성할 수 있는 방법에 대한 제안은 CSF를 보완하는 온라인 자원 모음에 포함된 퀵 스타트 가이드(Quick Start Guides, QSG)등 다양한 자료에서 제공합니다. 또한, 일부 프로세스 자동화를 원하는 조직을 도울 수 있도록 다양한 도구를 다운로드 받을 수 있는 형식으로 제공됩니다. 퀵 스타트 가이드는 CSF 사용의 초기 방법을 제안하고 독자가 CSF 및 관련 자원을 더 깊이 알아볼 수 있도록 지원합니다. [NIST CSF 웹사이트](#)에서 제공하는 CSF와 이러한 보충 자원은 위험을 관리하고 줄이는 것을 돕는 "CSF 포트폴리오"로 간주되어야 합니다. CSF가 어떻게 적용되든 간에 사용자는 자신의 사이버보안 상태의 맥락을 고려하고 특정 필요에 맞게 CSF를 적용해야 합니다.

이전 버전을 기반으로, CSF 2.0에는 *거버넌스와 공급망의 중요성*을 강조하는 새로운 기능들이 포함되었습니다. 퀵 스타트 가이드에 특별한 주의를 기울여, 크거나 작은 조직 모두에게 CSF가 유용하고 쉽게 접근할 수 있도록 하였습니다. NIST는 현재 *구현 예시와 참조 정보*를 제공하며, 이는 온라인 상에 정기적으로 업데이트됩니다. 현재 및 목표 상태 *조직 프로파일*을 생성하는 것은 조직이 자신들의 상태와 되고자 하는 상태를 비교할 수 있게 하며, 보안 통제를 더 빠르게 구현하고 평가할 수 있게 합니다.

사이버보안 위험은 지속적으로 증가하고 있으며, 이를 관리하는 과정은 끊임없이 이어져야 합니다. 조직이 사이버보안 문제에 처음으로 대응하기 시작했든, 충분한 자원을 갖춘

사이버보안 팀을 오랜 기간 동안 운영해 왔든 마찬가지입니다. CSF는 모든 유형의 조직에서 활용할 수 있도록 설계되었으며, 앞으로 장기적으로 적절한 지침을 제공할 수 있을 것으로 기대됩니다.

1. 사이버보안 프레임워크(CSF) 개요

이 문서는 NIST 사이버보안 프레임워크(CSF) 2.0 버전입니다. 이 프레임워크는 다음과 같은 구성 요소가 포함되어 있습니다.

- **CSF 코어(Core):** CSF의 핵심으로, 모든 조직이 사이버보안 위험을 관리할 수 있도록 돕는 고수준의 사이버보안 결과 분류체계입니다. CSF 코어 구성 요소는 각 결과를 자세히 설명하는 기능, 카테고리, 그리고 하위 카테고리의 계층 구조로 되어 있습니다. 이 결과는 사이버보안 전문 지식과 관계없이 경영진, 관리자, 실무자를 포함한 광범위한 대상이 이해할 수 있습니다. 해당 결과는 부문, 국가, 기술 중립적이기 때문에 조직은 자신의 고유한 위험, 기술, 업무 관련한 내용을 고려할 수 있는 유연성을 확보할 수 있습니다.
- **CSF 조직 프로파일(Organizational Profiles):** CSF 코어의 결과를 기반으로 조직의 현재 상태나 목표 사이버보안 상태를 설명하는 메커니즘입니다.
- **CSF 단계(Tiers):** 조직의 사이버보안 위험 거버넌스 및 운영 관행의 엄격성을 평가하는데 적용할 수 있습니다. 단계는 조직이 사이버보안 위험을 어떻게 인식하고, 이를 관리하기 위해 어떤 절차를 마련하고 있는 관련 맥락을 제공합니다.

이 문서는 조직에서 목표 삼을 수 있는 바람직한 결과를 *설명합니다*. 결과를 명시하거나 그 결과를 어떻게 달성해야 하는지에 대해서는 규정하지 않습니다. 조직이 원하는 결과를 달성할 수 있는 방법에 대한 설명은 CSF를 보완하는 온라인 자료 모음에서 제공되며, NIST CSF 웹사이트([NIST CSF website](#))를 통해 이용할 수 있습니다. 이러한 자료는 결과를 달성하기 위해 사용할 수 있는 실무과 제어 관련 추가 지침을 제공하며, 조직에서 CSF를 이해, 채택, 사용하는 데 도움을 줄 수 있습니다. 여기에 포함된 자료는 다음과 같습니다.

- 각 결과 관련 지침을 제공하는 기존 글로벌 표준, 지침, 프레임워크, 규정, 정책 등을 가리키는 유익한 참고 문헌([Informative References](#)).
- 각 결과를 달성할 수 있는 잠재적 방법을 보여주는 구현 예시([Implementation Examples](#)).
- CSF와 그 온라인 자원을 사용하는 방법에 대한 실질적 지침을 제공하는 퀵 스타트 가이드([Quick-Start Guides](#)), 이전 CSF 버전에서 버전 2.0으로 전환 포함.
- 조직이 CSF를 실행하고 사이버보안 위험 관리에 대한 우선 순위를 설정하는 데 도움이 되는 커뮤니티 프로파일과 조직 프로파일 템플릿([Community Profiles and Organizational Profile Templates](#)).

조직은 CSF 코어, 프로파일, 단계, 보완 자료를 사용하여 사이버보안 위험을 이해 및 평가하며 우선 순위를 정하고 소통할 수 있습니다.

- **이해하고 평가하기:** 조직의 일부 또는 전체의 현재 또는 목표로 하는 사이버 보안 상태를 설명하고, 부족한 부분을 파악하며, 이러한 격차를 해소하기 위한 진행 상황을 평가합니다.
- **우선순위 정하기:** 조직의 임무, 법적 및 규제 요구 사항, 위험 관리 및 거버넌스 기대치에 부합하는 사이버보안 위험 관리를 위한 조치를 식별하고, 조직하며, 우선 순위를 정합니다.
- **소통하기:** 사이버보안 위험, 능력, 필요 및 기대 관련하여 조직 내외부와 소통할 수 있는 공통 언어를 제공합니다.

CSF는 산업, 정부, 학계, 비영리 조직을 포함한 모든 규모와 부문의 조직이 사용할 수 있도록 설계되었습니다. 조직의 사이버보안 프로그램의 성숙도와 관계없이 적용할 수 있는 기본 자원으로, 자발적으로 채택할 수도 있고 정부 정책이나 시행을 통해 채택할 수도 있습니다. CSF의 분류체계와 참조된 표준, 지침, 관행(실천 방법)은 특정 국가에 한정된 것이 아니며, 이전 버전의 CSF는 미국 내외 수많은 정부 및 기타 조직에서 성공적으로 활용하고 있습니다.

CSF는 다른 자원(예: 프레임워크, 표준, 지침, 선도적 관행 등)과 함께 사용하여 사이버보안 위험을 더 잘 관리하고 기업 단위에서 정보 및 통신 기술(ICT) 위험의 전반적인 관리를 알려야 합니다. CSF는 모든 조직이 규모에 관계없이 사용할 수 있도록 맞춤화할 수 있는 유연한 프레임워크입니다. 각각의 조직은 각자가 다른 위협과 취약점을 포함하여 고유한 위험을 지니고 있으며, 위험 허용도 및 고유한 임무 목표와 요구 사항도 다릅니다. 따라서 조직의 위험 관리 접근 방식과 CSF의 구현도 다양해집니다.

이 문서의 나머지 부분은 다음과 같이 구성되어 있습니다.

- 제2장은 CSF 코어의 기능, 카테고리, 하위 카테고리 같은 기본 사항을 설명합니다.
- 제3장은 CSF 프로파일과 단계의 개념을 정의합니다.
- 제4장은 CSF의 온라인 자원 모음 중 선택된 구성 요소에 대한 개요를 제공합니다. 여기에는 유익한 참고 문헌, 구현 예시, 퀵 스타트 가이드가 있습니다.
- 제5장은 조직에서 CSF를 다른 위험 관리 프로그램과 통합하는 방법에 대해 논의합니다.
- 부록 A는 CSF 코어입니다.
- 부록 B는 CSF 단계의 개념적 일러스트레이션을 포함하고 있습니다.
- 부록 C는 CSF 용어의 용어집입니다.

2. CSF 코어 소개

부록 A는 CSF 코어를 설명합니다. CSF 코어는 사이버보안 결과를 기능, 카테고리, 최종 하위 카테고리 순으로 배열한 것입니다(그림 1 참조). 이 결과는 수행해야 할 작업 목록이 아니며, 특정 결과를 달성하기 위해 필요한 구체적인 행동은 조직과 사용 사례에 따라 다르고, 이를 담당하는 사람에 따라 다를 수 있습니다. 또한, 코어 내의 기능, 카테고리, 하위 카테고리의 순서와 크기가 이들의 달성 순서나 중요성을 의미하지는 않습니다. 코어의 구조는 조직 내에서 위험 관리를 실질적으로 운영하는 사람들에게 가장 잘 맞도록 설계되었습니다.

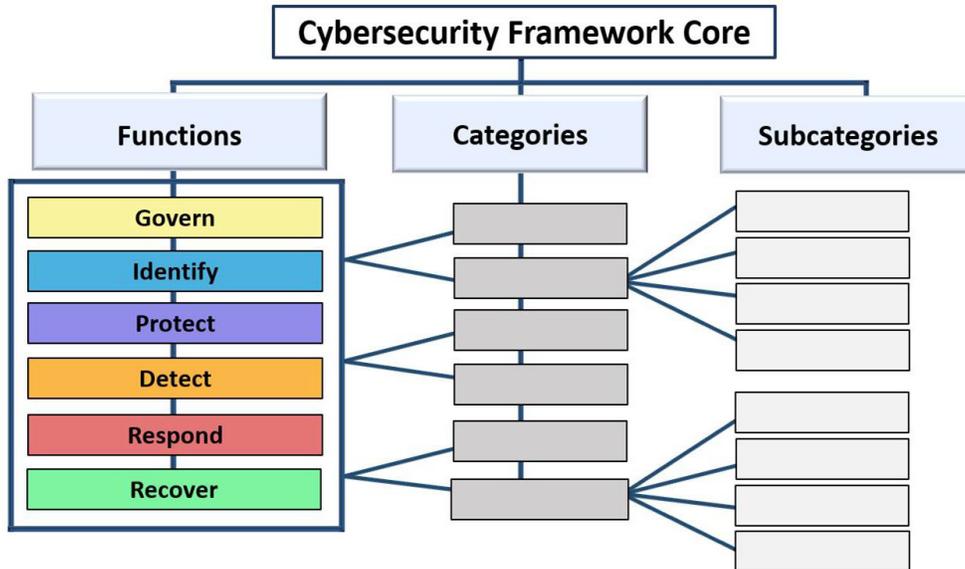


그림 1. CSF 코어 구조

CSF 코어 기능 — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER —은 사이버보안 결과를 최상위 수준에서 체계화합니다.

- GOVERN [거버넌스] (GV)** — 조직의 사이버보안 위험 관리 전략, 기대치, 정책을 수립, 전달, 모니터링 합니다. GOVERN 기능은 조직의 임무와 이해관계자의 기대에 맞게 다른 다섯 가지 기능의 결과를 달성하고 우선순위를 정하는 방법에 대한 정보를 제공합니다. 거버넌스 활동은 조직의 보다 넓은 기업 위험 관리(Enterprise Risk Management, ERM) 전략에 사이버보안을 통합하는 데 중요합니다. GOVERN은 조직 맥락의 이해, 사이버보안 전략과 사이버보안 공급망 위험 관리의 수립, 역할, 책임, 권한, 정책, 사이버보안 전략의 감독을 다룹니다.
- IDENTIFY [식별] (ID)** — 조직의 현재 사이버보안 위험이 파악됩니다. 조직의 자산(예: 데이터, 하드웨어, 소프트웨어, 시스템, 시설, 서비스, 인력), 공급자 및 관련 사이버보안 위험을 이해함으로써, 조직은 GOVERN 하에서 식별된 임무 요구 사항 및 위험 관리 전략에 맞춰 우선순위를 설정할 수 있습니다. 이 기능에는 사이버보안

위험 관리를 지원하는 조직의 정책, 계획, 프로세스, 절차, 관행을 개선할 기회를 식별하는 작업도 포함됩니다. 이는 모든 여섯 가지 기능에 대한 활동을 알리는 데 도움이 됩니다.

- **PROTECT [보호] (PR)** — *조직의 사이버보안 위험을 관리하기 위한 보호 조치를 사용합니다.* 자산과 위험을 식별하고 우선 순위가 정해지면, PROTECT는 이러한 자산을 보호하여 사이버보안 사고의 발생 가능성과 부정적인 영향을 예방하거나 감소시키고, 기회를 활용할 가능성과 영향을 증가시키는 능력을 지원합니다. 이 기능에 포함된 결과는 신원 관리, 인증, 접근 제어, 인식 및 교육, 데이터 보안, 플랫폼 보안(즉, 물리적 및 가상 플랫폼의 하드웨어, 소프트웨어 및 서비스 보안), 그리고 기술 인프라의 복원력입니다.
- **DETECT [탐지] (DE)** — *발생 가능성이 있는 사이버보안 공격과 위협을 발견하고 분석합니다.* DETECT는 이상 현상, 침해의 징후 및 기타 잠재적으로 부정적인 사고를 시기적절하게 발견하고 분석할 수 있도록 하며, 이를 통해 사이버보안 공격과 사고가 일어나고 있다는 것을 알 수 있습니다. 이 기능은 성공적인 사고 대응 및 복구 활동을 지원합니다.
- **RESPOND [대응] (RS)** — *감지된 사이버보안 사고 관련 조치를 취합니다.* RESPOND는 사이버보안 사고의 영향을 제한하는 능력을 지원합니다. 이 기능 내의 결과에는 사고 관리, 분석, 완화, 보고, 커뮤니케이션을 포함됩니다.
- **RECOVER [복구] (RC)** — *사이버보안 사고에 영향을 받은 자산 및 운영을 복원합니다.* RECOVER는 사이버보안 사고의 영향을 줄이고 정상적인 운영을 시기적절하게 복원하여 복구 과정 동안 적절한 커뮤니케이션을 가능하게 하는 능력을 지원합니다.

많은 사이버보안 위험 관리 활동이 부정적인 사고가 발생하지 않도록 예방하는 데 초점을 맞추지만, 부정적인 사고는 긍정적인 기회로 활용하는 데 도움이 될 수도 있습니다. 사이버보안 위험을 줄이기 위한 조치는 조직에 다른 방식으로 이익을 줄 수 있습니다. 예를 들어, 조직의 여유 공간을 상업 호스팅 제공업체에 우선 제공하여 그들과 다른 조직의 데이터 센터를 호스팅하게 하고, 나중에 주요 재무 시스템을 조직 내 데이터 센터에서 호스팅 제공자로 이전하여 사이버보안 위험을 줄이는 것이 그러한 예입니다. 이러한 행동은 비용 절감은 물론, 조직의 수익 증가에도 기여할 수 있습니다.

그림 2는 모든 기능이 서로 관련되어 있기 때문에 CSF 기능을 원형으로 표시합니다. 예를 들어, 한 조직에서 IDENTIFY에서 자산을 분류하고 PROTECT에서 그 자산을 보호하기 위한 조치를 취합니다. GOVERN 및 IDENTIFY 기능에서 계획 및 테스트에 한 투자는 DETECT

기능에서 예상치 못한 사건을 시기적절하게 탐지하는 데 도움이 되며, RESPOND 및 RECOVER 기능에서는 사이버보안 사고에 대한 대응 및 복구 조치가 가능합니다. GOVERN은 원의 중심에 있으며, 조직이 다른 다섯 가지 기능을 어떻게 구현할지에 대한 정보를 제공합니다.

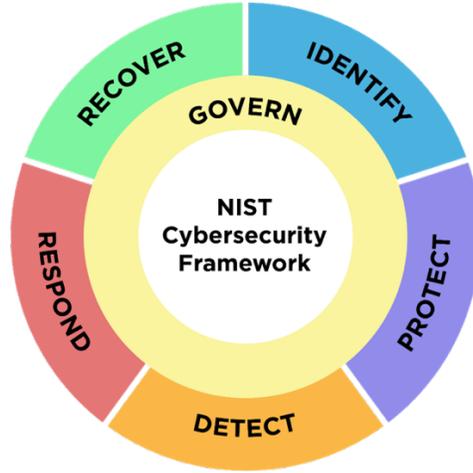


그림 2. CSF 기능

이런 기능은 동시에 수행되어야 합니다. GOVERN, IDENTIFY, PROTECT, DETECT를 지원하는 조치가 지속적으로 이루어져야 하며, RESPOND와 RECOVER를 지원하는 조치는 항상 준비되어 있다가 사이버보안 사고가 발생했을 때 실행되어야 합니다. 모든 기능은 사이버보안 사고와 관련된 중요한 역할을 가지고 있습니다. GOVERN, IDENTIFY, PROTECT 결과는 사고를 예방하고 준비하는 데 도움을 주며, GOVERN, DETECT, RESPOND, RECOVER 결과는 사고를 발견하고 관리하는 데 도움을 줍니다.

각 기능은 그 내용을 요약하는 동사로 명명됩니다. 각 기능은 관련 사이버보안 결과로 이루어진 *카테고리*로 나뉩니다. 이러한 결과는 함께 해당 기능을 구성합니다. 하위 카테고리는 각 카테고리를 기술적 및 관리 활동의 더 구체적인 결과로 세분화합니다. 하위 카테고리가 모든 결과를 포괄하는 것은 아니지만, 각 카테고리를 지원하는 자세한 결과를 설명합니다.

기능, 카테고리, 하위 카테고리는 조직이 사용하는 모든 ICT에 적용됩니다. 여기에는 정보 기술(IT), 사물 인터넷(IoT), 운영 기술(OT)이 포함됩니다. 또한, 클라우드, 모바일, 인공지능 시스템을 포함한 모든 유형의 기술 환경에도 적용됩니다. CSF 코어는 미래 지향적이며 기술 및 환경의 미래 변화에 적응할 수 있도록 설계되었습니다.

3. CSF 프로파일 및 단계 소개

이 섹션에서는 CSF 프로파일과 단계의 개념을 정의합니다.

3.1 CSF 프로파일

조직 프로파일(CSF Organizational Profile)은 코어의 결과 측면에서 조직의 현재 및/또는 목표 사이버보안 상태를 설명합니다. **조직 프로파일**은 조직의 업무 목표, 이해관계자의 기대, 위협 환경, 요구 사항을 고려하여 코어의 결과 이해, 사용자정의, 평가, 우선순위 설정, 소통하는 데 사용합니다. 그다음 조직은 특정 결과를 달성하기 위해 각 조치를 우선순위에 따라 정리하고 그 정보로 이해관계자와 소통할 수 있습니다.

모든 조직 프로파일은 다음 중 하나 이상을 포함합니다:

1. **현재 프로파일**(Current Profile)은 조직이 현재 달성하고 있거나 달성하려고 시도하고 있는 코어 결과를 명시하고, 각 결과가 어떻게, 어느 정도로 달성되고 있는지를 구체화합니다.
2. **목표 프로파일**(Target Profile)은 조직이 사이버보안 위험 관리 목표를 달성하기 위해 우선 순위를 정하여 선택한 목표 결과를 명시합니다. 목표 프로파일은 새로운 요구 사항, 새로운 기술 도입, 위협 인텔리전스 추세와 같은 조직의 사이버보안 상태에 예상되는 변화를 고려합니다.

커뮤니티 프로파일은 여러 조직 간에 공유 관심사와 목표를 다루기 위해 생성하고 게시하는 CSF 결과의 기준선입니다. 커뮤니티 프로파일은 일반적으로 특정 부문, 하위 부문, 기술, 위협 유형, 기타 사용 사례를 위해 개발합니다. 조직은 커뮤니티 프로파일을 자체 목표 프로파일의 기초로 사용할 수 있습니다. 커뮤니티 프로파일의 예시는 NIST CSF 웹사이트([NIST CSF website](#))에서 찾아볼 수 있습니다.

그림 3과 아래에 요약된 단계를 통해 조직에서 조직 프로파일을 사용하여 사이버보안을 지속적으로 개선하는 것을 돕는 방법 중 한 가지를 확인할 수 있습니다.



그림 3. CSF 조직 프로파일 생성 및 사용 단계

1. **조직 프로파일의 범위를 설정.** 프로파일이 기반을 둔 고수준의 사실과 가정을 문서화하여 그 범위를 정의합니다. 조직은 원하는 만큼 많은 조직 프로파일을 가질 수 있으며, 각 프로파일은 다른 범위를 가질 수 있습니다. 예를 들어, 한 프로파일이 전체 조직을 다룰 수도 있고, 조직의 재무 시스템에 초점을 맞출 수도 있으며, 해당 재무 시스템과 관련된 랜섬웨어 위협과 사고 처리에 초점을 맞출 수도 있습니다.
2. **조직 프로파일을 준비하기 위해 필요한 정보를 수집.** 정보의 예로는 조직 정책, 위험 관리 우선 순위 및 자원, 기업 위험 프로파일, 사업 영향 분석(BIA) 등록부, 조직이 따르는 사이버보안 요구 사항 및 표준, 관행 및 도구(예: 절차 및 보호 조치), 작업 역할 등이 있습니다.
3. **조직 프로파일을 생성.** 선택된 CSF 결과에 포함해야 할 정보 유형을 결정하고 필요한 정보를 문서화합니다. 현재 프로파일의 위험 요소를 고려하여 목표 프로파일 계획 및 우선 순위 설정에 참고합니다. 또한, 커뮤니티 프로파일을 목표 프로파일의 기초로 사용하는 것을 고려할 수 있습니다.
4. **현재 프로파일과 목표 프로파일 사이의 격차를 분석하고 행동 계획을 생성.** 현재 프로파일과 목표 프로파일 사이의 차이를 식별하고 분석하기 위해 격차 분석을 수행하고, 그 격차를 해결하기 위해 우선 순위화 된 행동 계획(예: 위험 등록부, 위험 세부 보고서, 행동 계획 및 이정표[POA&M])을 개발합니다.
5. **행동 계획을 실행하고 조직 프로파일을 업데이트.** 행동 계획에 따라 격차를 해결하고 조직을 목표 프로파일로 이동시킵니다. 행동 계획은 전체 마감일을 가질 수도 있고 계속 이어질 수도 있습니다.

지속적인 개선의 중요성을 감안할 때, 조직은 필요한 만큼 이러한 단계를 반복할 수 있습니다.

조직 프로파일은 추가적인 용도로도 사용할 수 있습니다. 예를 들어, 현재 프로파일은 조직의 사이버보안 능력과 개선의 기회를 외부 이해관계자에게 문서화하고 소통하는 데 사용할 수 있습니다. 이러한 이해관계자에는 비즈니스 파트너 또는 잠재 고객이 포함될 수 있습니다. 또한, 목표 프로파일은 공급업체, 파트너 및 기타 제3자에게 조직의 사이버보안 위험 관리 요구 사항과 기대를 표현하는 데 도움을 줄 수 있으며, 이는 해당 당사자들이 달성해야 할 목표가 될 수 있습니다.

3.2 CSF 단계

조직은 단계를 사용하여 현재 프로파일과 목표 프로파일을 설정하는 데 도움을 받을 수 있습니다. 단계는 조직의 사이버보안 위험 거버넌스 및 관리 관행의 엄격성을 특징짓고, 조직이 사이버보안 위험을 어떻게 보고, 그 위험을 관리하기 위해 어떤 프로세스를 갖추고 있는지에 대한 맥락을 제공합니다. 그림 4와 부록 B에서 개념적으로 보여주는 바와 같이, 단계는 조직이

사이버보안 위험을 관리하는 관행을 불완전(Tier 1), 위험 인식(Tier 2), 재현 가능(Tier 3), 적합(Tier 4)으로 나타냅니다. 단계는 비공식적이고 임시방편적인 대응에서부터 민첩하고 위험을 고려한 지속적인 개선에 이르는 접근 방식으로의 진전을 설명합니다. 단계를 선택하는 것은 조직이 사이버보안 위험을 어떻게 관리할지에 대한 전반적인 기초를 설정하는 데 도움을 줍니다.

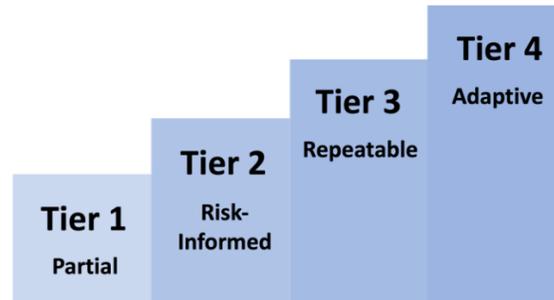


그림 4. 사이버보안 위험 거버넌스 및 관리를 위한 CSF 단계

단계는 조직의 사이버보안 위험 관리 방법론을 대체하기보다는 보완해야 합니다. 예를 들어, 조직은 단계를 사용하여 조직 전체적인¹⁾ 사이버보안 위험 관리 접근 방식을 벤치마크하여 내부적으로 소통할 수 있습니다. 위험이나 의무가 더 클 때 또는 비용-편익 분석을 통해 부정적인 사이버보안 위험을 줄이는 것이 실행 가능하면서 해당 비용이 효율적일 때 더 높은 단계로 진전을 권장합니다.

NIST CSF 웹사이트([NIST CSF website](#))는 프로파일과 단계 사용에 대한 추가 정보를 제공합니다. 이는 NIST가 호스트하는 조직 프로파일 템플릿([NIST-hosted Organizational Profile templates](#))과 다양한 기계 판독 가능 형식 및 인간 친화적 형식의 커뮤니티 프로파일([Community Profiles](#)) 저장소를 포함한 정보를 제공합니다.

1 이 문서에서 "조직 전체"와 "기업"이라는 용어는 동일한 의미로 사용됩니다.

4. CSF를 보완하는 온라인 자원 소개

NIST와 다른 조직에서 CSF의 이해, 채택, 사용에 도움이 되도록 온라인 자료 모음을 제작했습니다. 해당 자료는 온라인에 호스팅되어 있기 때문에, 이 문서보다 더 자주 업데이트될 수 있으며, 기계도 읽을 수 있는 형식으로 제공됩니다. 반면, 이 문서는 사용자에게 안정성을 제공하기 위해 자주 업데이트되지 않습니다. 이 섹션에서는 유익한 참고 문헌(Informative References), 구현 예(Implementation Examples), 퀵 스타트 가이드(Quick Start Guides), 이렇게 세 가지 유형의 온라인 자료에 대한 개요를 제공합니다.

유익한 참고 문헌([Informative References](#))은 코어와 다양한 표준, 지침, 규정 및 기타 콘텐츠 간의 관계를 매핑합니다. 유익한 참고 문헌은 조직이 코어의 결과를 달성할 수 있는 방법에 대해 정보를 제공하는 데 도움이 됩니다. 유익한 참고 문헌은 부문 또는 기술에 특정할 수 있습니다. 이들은 NIST 또는 다른 조직에 의해 생산될 수 있습니다. 일부 유익한 참고 문헌은 하위 카테고리보다 범위가 좁을 수 있습니다. 예를 들어, 정보 시스템 및 조직을 위한 [SP 800-53의](#) 보안 및 개인정보 보호 통제 조치는 하위 카테고리에서 설명된 결과를 달성하기 위해 필요한 여러 참조 중 하나일 수 있습니다. 다른 유익한 참고 문헌은 더 높은 수준일 수 있습니다. 예를 들어, 여러 하위 카테고리를 부분적으로 다루는 정책의 요구 사항과 같습니다. CSF를 사용할 때, 조직은 가장 관련성 높은 유익한 참고 문헌을 식별할 수 있습니다.

구현 예시([Implementation Examples](#))는 하위 카테고리의 결과를 달성하기 위한 간결하고 실천적인 단계의 개념적 예시를 제공합니다. 예시를 표현하는 데 사용되는 동사에는 공유, 문서화, 개발, 수행, 모니터링, 분석, 평가 및 훈련이 포함됩니다. 이것은 조직이 결과를 달성하기 위해 취할 수 있는 모든 행동의 포괄적인 목록이 아니며, 사이버보안 위험을 다루기 위해 필요한 기본적인 행동의 기준을 나타내지 않습니다.

퀵 스타트 가이드([Quick-Start Guides \(QSGs\)](#))는 특정 CSF 관련 주제에 대한 간단한 문서로, 종종 특정 대상에 맞춰 조정됩니다. QSG는 조직이 사이버보안 자세와 관련 위험 관리를 개선할 수 있는 첫 단계로서, CSF의 특정 부분을 실천 가능한 지침으로 간결하게 제공합니다. 이 가이드는 시간에 따라 수정되며 필요에 따라 새로운 가이드가 추가됩니다.

CSF 2.0에 대한 새로운 유익한 참고 문헌 제안은 언제든지 NIST의 olir@nist.gov로 공유할 수 있습니다. NIST CSF 웹사이트에서 참조할 추가 자료 관련 제안이나 새로운 QSG 주제 등은 cyberframework@nist.gov로 보내주십시오.

5. 사이버보안 위험 소통 및 통합 개선

CSF의 사용법은 조직의 고유한 업무와 위험에 따라 다릅니다. 이해관계자의 기대, 위험 선호도, 허용 범위(거버넌스에서 설명된 바와 같이)를 이해함으로써 조직은 사이버보안 활동을 우선 순위에 따라 정렬하고 정보에 기반하여 사이버보안 지출과 조치 관련 결정을 내릴 수 있습니다. 조직은 잠재적인 영향과 가능성에 따라 위험을 완화, 이전, 회피 또는 수용하는 한 가지 이상의 방법을 선택할 수 있으며, 긍정적인 위험(전략적 기회)을 실현, 공유, 강화, 수용할 수 있습니다. 중요한 것은 조직이 자체 사이버보안 역량을 관리하기 위해 내부적으로 CSF를 사용하고, 외부적으로는 제3자와의 소통이나 감독에 CSF를 활용할 수 있다는 점입니다.

CSF의 활용 방법에 관계없이, 조직은 CSF를 지침으로 사용하여 사이버보안 위험을 이해하고 평가하며, 우선순위를 정하고 소통하는 데 도움을 받을 수 있습니다. 선택한 결과를 통해 조직은 우선순위와 사용 가능한 자원을 고려하면서 사이버보안 상태를 개선하고, 목표에 핵심이 되는 기능의 연속성을 유지하기 위한 전략적 결정에 초점을 맞출 수 있습니다.

5.1 위험 관리 소통 개선

CSF는 사이버보안에 대한 기대, 계획 및 자원에 관하여 소통을 향상시킬 수 있는 기반을 제공합니다. CSF는 조직의 우선 순위와 전략적 방향에 중점을 두는 경영진과 그 우선 순위 달성에 영향을 줄 수 있는 특정 사이버보안 위험을 관리하는 관리자 간의 양방향 정보 흐름(그림 5의 상단 부분)을 촉진합니다. CSF는 또한 기술을 실행하고 운영하는 실무자와 관리자 간의 유사한 정보 흐름(그림 5의 하단 부분)을 지원합니다. 그림의 왼쪽 부분에서는 실무자가 관리자와 경영진에게 자신의 최신 정보, 인사이트, 우려를 공유하는 것의 중요성을 볼 수 있습니다.



그림 5. CSF를 사용한 위험 관리 소통 개선

조직 프로파일을 생성하고 사용하기 위한 준비 과정에는 경영진으로부터 조직의 우선순위, 자원 및 위험 방향에 대한 정보를 수집하는 것이 포함됩니다. 그다음 관리자는 실무자와 협력하여 비즈니스 요구 사항에 관하여 소통하고 위험에 기반한 조직 프로파일을 생성합니다. 현재 프로파일과 목표 프로파일 사이에 확인된 격차를 해소하기 위한 조치는 관리자와 실무자가 실행하며, 시스템 수준 계획에 중요한 입력을 제공합니다. 시스템 수준에서 적용한 통제와 모니터링을 통해 조직 전체에서 목표 상태가 달성되면 업데이트한 결과는 위험 등록부 및 진행 보고서를 통해 공유할 수 있습니다. 관리자는 지속적인 평가를 통해 잠재 위험은 더욱 줄이고 잠재 이익은 높이는 조정이 가능한 통찰력을 가질 수 있습니다.

GOVERN 기능은 **경영진**과의 조직 위험 소통을 지원합니다. 경영진 논의에는 전략이 포함되며, 특히 사이버보안 관련 불확실성이 조직 목표 달성에 어떻게 영향을 미칠 수 있는지에 대해 중점을 둡니다. 이러한 거버넌스 논의는 위험 관리 전략(사이버보안 공급망 위험 포함), 역할, 책임, 권한, 정책, 감독 관련 대화와 합의를 지원합니다. 경영진은 이러한 필요에 기반하여 사이버보안 우선순위와 목표를 설정하고, 위험 선호도, 책임, 자원에 대한 기대를 소통합니다. 또한, 경영진은 사이버보안 위험 관리를 ERM 프로그램 및 하위 수준의 위험 관리 프로그램과 통합할 책임이 있습니다(제5.2절 참조). 그림 5의 상단에 반영된 소통은 ERM 및 하위 수준 프로그램에 대한 고려사항을 포함할 수 있으며, 이를 통해 관리자와 실무자에게 정보를 제공합니다.

경영진이 설정한 전반적인 사이버보안 목표는 **관리자**에게 전달되며, 이는 영리 기업에서는 사업 부문이나 사업 본부에 적용될 수 있습니다. 정부 기관의 경우, 이는 부서 또는 지부 수준의 고려사항일 수 있습니다. CSF를 구현할 때, 관리자는 목표 프로파일에 표현된 대로 공통 서비스, 통제 및 협업을 통해 위험 목표를 달성하는 방법에 초점을 맞추며, 행동 계획(예: 위험 등록부, 위험 세부 보고서, POA&M)에서 추적되는 조치를 통해 개선합니다.

실무자는 목표 상태를 구현하고 운영 위험의 변화를 측정하여 특정 사이버보안 활동의 계획, 수행 및 모니터링을 지원합니다. 위험이 수용 가능한 수준에서 관리될 수 있도록 통제를 구현하면서, 실무자는 경영진과 경영진에게 조직의 사이버보안 상태를 이해하고 정보에 기반한 결정을 내리며 위험 전략을 유지하거나 조정하는데 필요한 정보(예: 주요 성과 지표, 주요 위험 지표)를 제공합니다. 경영진은 이 사이버보안 위험 데이터를 조직 전반의 다른 유형의 위험 정보와 결합할 수도 있습니다. 기대치와 우선순위의 업데이트는 주기가 반복됨에 따라 업데이트된 조직 프로파일에 포함됩니다.

5.2 다른 위험 관리 프로그램과의 통합 개선

모든 조직은 다양한 종류의 ICT 위험(예: 개인정보 보호, 공급망, 인공지능 등)에 직면하며, 각 위험에 특화된 프레임워크와 관리 도구를 사용할 수 있습니다. 어떤 조직은 ERM을 사용하여 ICT 및 모든 기타 위험 관리 활동을 고수준에서 통합하는 반면, 다른 조직은 각 위험에 충분한 주의를 기울이기 위해 활동을 별도로 유지합니다. 소규모 조직은 그 특성상 기업 수준에서 위험을 모니터링할 수 있으며, 규모가 큰 기업은 ERM에 통합된 별도의 위험 관리 결과를 유지할 수 있습니다.

조직은 ERM 접근 방식을 사용하여 사이버보안을 포함한 위험 고려 사항 포트폴리오를 균형있게 관리하고 정보에 기반한 결정을 내릴 수 있습니다. 경영진은 거버넌스 및 위험 전략을 CSF의 이전 사용 결과와 통합하면서 현재 및 계획된 위험 활동에 대한 중요한 정보를 제공받습니다. CSF는 조직이 사이버보안 및 사이버보안 위험 관리에 대한 용어를 경영진이 이해할 수 있는 일반적인 언어로 번역하는 데 도움을 줍니다.

NIST가 제공하는 사이버보안 위험 관리와 ERM(기업 위험 관리) 간의 상호 관계를 설명하는 자료는 다음과 같습니다:

- [NIST 사이버보안 프레임워크 2.0 - 기업 위험 관리 퀵 스타트 가이드](#)
- NIST 기관 보고서(IR) 8286, [사이버보안과 기업 위험 관리\(ERM\) 통합](#)
- IR 8286A, [기업 위험 관리를 위한 사이버보안 위험 식별 및 추정](#)
- IR 8286B, [기업 위험 관리를 위한 사이버보안 위험 우선순위 결정](#)
- IR 8286C, [기업 위험 관리 및 거버넌스 감독을 위한 사이버보안 위험 단계 설정](#)
- IR 8286D, [비즈니스 영향 분석을 사용하여 위험 우선순위 결정 및 대응 정보 제공](#)
- SP 800-221, [정보 및 통신 기술 위험의 기업 영향: 기업 위험 포트폴리오 내에서 ICT 위험 프로그램 관리 및 거버넌스](#)
- SP 800-221A, [정보 및 통신 기술\(ICT\) 위험 결과: 기업 위험 포트폴리오와 통합된 ICT 위험 관리 프로그램](#)

조직은 개별 ICT 위험 관리 프로그램과 사이버보안 위험 관리를 통합하는 데 CSF를 유용하게 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- **사이버보안 위험 관리 및 평가:** CSF는 NIST의 위험 관리 프레임워크(RMF)에서 제공하는 [SP 800-37, 정보 시스템 및 조직을 위한 위험 관리 프레임워크](#), 및 [SP 800-30, 위험 평가 수행 가이드와 같은 기존의 사이버보안 위험 관리 및 평가 프로그램](#)과 통합될 수 있습니다. [NIST RMF와 그 관련 출판물](#)을 사용하는 조직의 경우, CSF는 RMF의 접근 방식을 보완하여 [SP 800-53, 정보 시스템 및 조직을 위한 보안 및 개인정보 보호 통제](#)에서 통제 조치를 선택하고 우선순위를 지정하는 데 사용될 수 있습니다.

- **개인정보 보호 위험:** 사이버보안과 개인정보 보호는 독립적인 분야이지만, 그림 6에서 보이듯이 특정 상황에서는 그 목표가 겹칩니다.

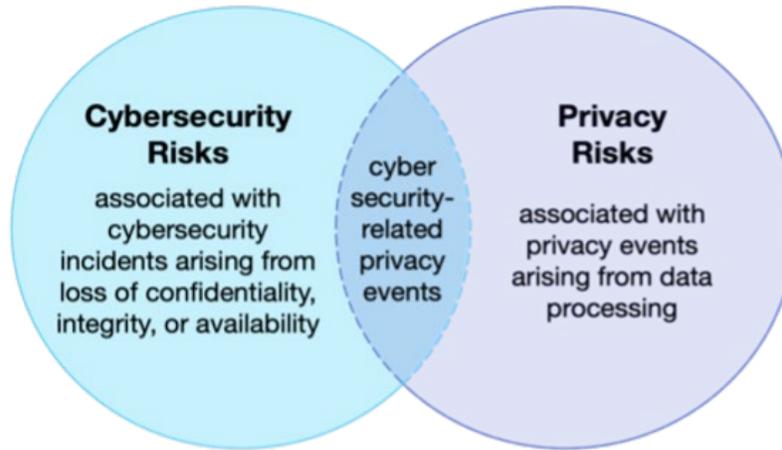


그림 6. 사이버보안과 개인정보 보호 위험 관계

사이버보안 위험 관리는 개인의 데이터의 기밀성, 무결성, 그리고 가용성 손실과 관련된 개인정보 보호 위험을 해결하는 데 필수적입니다. 예를 들어, 데이터 유출은 신원 도용으로 이어질 수 있습니다. 그러나 개인정보 보호 위험은 사이버보안 사고와 관련 없이 발생할 수도 있습니다.

조직은 임무나 비즈니스 목적을 달성하기 위해 데이터를 처리하는데, 이러한 데이터 처리의 결과로 개인이 문제를 겪을 수 있는 **개인정보 사고**가 발생할 수 있습니다. 이러한 문제는 다양한 방식으로 표현될 수 있지만, NIST는 이를 존엄성 유형의 영향(예: 수치심 또는 낙인)에서부터 더 구체적인 피해(예: 차별, 경제적 손실, 상해)에 이르기까지 다양하게 나타냅니다. [NIST의 개인정보 보호 프레임워크](#)와 사이버보안 프레임워크는 함께 사용하여 사이버보안과 개인정보 보호 위험의 다양한 측면을 해결할 수 있습니다. 또한, NIST의 [개인정보 위험 평가 방법론\(PRAM\)](#)에는 개인정보 위험 평가에 사용할 수 있는 예시 문제 카탈로그가 포함되어 있습니다.

- **공급망 위험:** 조직은 CSF를 사용하여 공급망 전반에 걸쳐 이해관계자와 사이버보안 위험 감독 및 소통을 증진할 수 있습니다. 모든 유형의 기술은 복잡하고 글로벌하게 분산된 광범위하고 상호 연결된 공급망 생태계에 의존하며, 지리적으로 다양한 경로와 다수의 아웃소싱 단계를 포함합니다. 이 생태계는 공공 및 민간 부문의 엔티티(예: 취득자, 공급업체, 개발자, 시스템 통합업체, 외부 시스템 서비스 제공업체 및 기타 기술 관련 서비스 제공업체)로 구성되어 있으며, 이들은 기술 제품 및 서비스를 연구, 개발, 설계, 제조, 취득, 전달, 통합, 운영, 유지, 폐기 및 기타 활용 또는 관리를 위해 상호 작용합니다. 이러한 상호 작용은 기술, 법률, 정책, 절차 및 관행에 의해 형성되고

영향을 받습니다.

이 생태계에서 복잡하고 상호 연결된 관계를 감안할 때, 공급망 위험 관리(SCRM)는 조직에 있어 중요합니다. 사이버보안 SCRM(C-SCRM)은 공급망 전반에 걸친 사이버보안 위험에 대한 노출을 관리하고 적절한 대응 전략, 정책, 프로세스 및 절차를 개발하는 체계적인 과정입니다. CSF의 C-SCRM 카테고리 [GV.SC] 내의 하위 카테고리는 순수하게 사이버보안에 초점을 맞춘 결과와 C-SCRM에 초점을 맞춘 결과 사이의 연결을 제공합니다. SP 800-161r1(개정판 1), [시스템 및 조직을 위한 사이버보안 공급망 위험 관리 관행](#)은 C-SCRM에 대한 심층적인 정보를 제공합니다.

- **신형 기술로 인한 위험:** 새로운 기술과 기술 응용이 등장함에 따라 새로운 위험이 나타나기도 합니다. 현대의 한 예로, 인공지능(AI)으로 인해 사이버보안 및 개인정보 보호 위험뿐만 아니라 많은 다른 유형의 위험도 같이 나타나고 있습니다. [NIST 인공지능 위험 관리 프레임워크\(AI RMF\)](#)는 이러한 위험들을 해결하기 위해 개발되었습니다. AI 위험을 기타 기업 위험(예: 재무, 사이버보안, 명성 및 개인정보 보호)과 함께 처리하는 것은 보다 통합된 결과와 조직 효율성을 제공할 것입니다. 사이버보안 및 개인정보 보호 위험 관리 고려 사항 및 접근 방식은 AI 시스템의 설계, 개발, 배치, 평가 및 사용에 적용됩니다. AI RMF 코어는 기능, 카테고리 및 하위 카테고리를 사용하여 AI 결과를 설명하고 AI 관련 위험을 관리하는 데 도움을 줍니다.

부록 A. CSF 코어

이 부록은 CSF 코어의 기능, 카테고리 및 하위 카테고리를 설명합니다. 표 1은 CSF 2.0 코어 기능 및 카테고리 이름과 고유 알파벳 식별자를 나열합니다. 표의 각 기능 이름은 부록의 해당 부분에 연결됩니다. 코어의 기능, 카테고리 및 하위 카테고리의 순서는 알파벳 순서가 아니며, 조직 내에서 위험 관리 운영을 책임지는 사람들이 가장 와 닿을 수 있도록 의도되었습니다.

표 1. CSF 2.0 코어 기능 및 카테고리 이름과 식별자

기능	카테고리	카테고리 식별자
Govern (GV) [거버넌스]	조직 맥락	GV.OC
	위험 관리 전략	GV.RM
	역할, 책임, 권한	GV.RR
	정책	GV.PO
	감독	GV.OV
	사이버보안 공급망 위험 관리	GV.SC
Identify (ID) [식별]	자산 관리	ID.AM
	위험 평가	ID.RA
	개선	ID.IM
Protect (PR) [보호]	신원 관리, 인증 및 접근 제어	PR.AA
	인식 및 교육	PR.AT
	데이터 보안	PR.DS
	플랫폼 보안	PR.PS
	기술 인프라 복원력	PR.IR
Detect (DE) [탐지]	지속적 모니터링	DE.CM
	유해 사건 분석	DE.AE
Respond (RS) [대응]	사고 관리	RS.MA
	사고 분석	RS.AN
	사고 대응 보고 및 의사소통	RS.CO
	사고 완화	RS.MI
Recover (RC) [복구]	사고 복구 계획 실행	RC.RP
	사고 복구 소통	RC.CO

CSF 코어, 유익한 참고 문헌, 구현 예는 [CSF 2.0 웹사이트](#)와 [CSF 2.0 참조 도구](#)를 통해 이용할 수 있습니다. 이 도구를 사용하면 사용자가 이를 탐색하고 인간이나 기계가 읽을 수 있는 형식으로 내보낼 수 있습니다. CSF 2.0 코어는 CSF 1.1의 [기존 형식](#)과 유사한 형태로도 제공됩니다.

GOVERN (GV): 조직의 사이버보안 위험 관리 전략, 기대치, 정책을 수립, 전달, 모니터링합니다.

- **조직 맥락(GV.OC):** 조직의 사이버보안 위험 관리 결정을 둘러싼 상황 — 임무, 이해관계자의 기대, 의존성 및 법적, 규제적, 계약적 요구 사항 — 을 이해합니다.
 - **GV.OC-01:** 조직의 임무를 이해하며 사이버보안 위험 관리를 안내합니다.
 - **GV.OC-02:** 내부 및 외부 이해관계자의 이해를 도우며, 사이버보안 위험 관리 관련한 관계가의 필요와 이해를 고려합니다.
 - **GV.OC-03:** 개인정보 보호 및 민간 자유 의무를 포함한 사이버 보안 관련 법적, 규제적, 계약적 요구 사항을 이해하고 관리합니다.
 - **GV.OC-04:** 외부 이해관계자가 의존하거나 기대하는 중요한 목표, 역량, 서비스를 이해하고 소통합니다.
 - **GV.OC-05:** 조직이 의존하는 결과, 역량 및 서비스를 이해하고 소통합니다.
- **위험 관리 전략(GV.RM):** 조직의 우선 순위, 제약 조건, 위험 허용도 및 위험 선호도 선언, 가정이 수립되고, 전달되며 운영 위험 결정을 지원하는 데 사용됩니다.
 - **GV.RM-01:** 위험 관리 목표가 조직 이해관계자에 의해 수립되고 동의됩니다.
 - **GV.RM-02:** 위험 선호도와 위험 허용도 선언을 수립, 전달, 유지합니다.
 - **GV.RM-03:** 사이버보안 위험 관리 활동 및 결과가 기업 위험 관리 프로세스에 포함됩니다.
 - **GV.RM-04:** 적절한 위험 대응 옵션을 설명하는 전략적 방향이 수립되고 전달됩니다.
 - **GV.RM-05:** 조직 전체의 사이버보안 위험, 공급업체 및 기타 제3자로부터의 위험을 포함하여 조직 전체의 의사소통 라인이 수립됩니다.
 - **GV.RM-06:** 사이버보안 위험을 계산, 문서화, 분류 및 우선 순위 지정을 위한 표준화된 방법이 수립되고 전달됩니다.
 - **GV.RM-07:** 전략적 기회(즉, 긍정적인 위험)가 특성화되며 조직의 사이버보안 위험 논의에 포함됩니다.

-
- **역할, 책임 및 권한 (GV.RR):** 사이버보안 역할, 책임 및 권한이 책임감, 성과 평가 및 지속적인 개선을 촉진하기 위해 수립되고 전달됩니다.
 - **GV.RR-01:** 조직 리더십은 사이버보안 위험에 대해 책임과 책임을 지며, 위험 인식을 윤리적이며 지속적으로 개선하는 문화를 촉진합니다.
 - **GV.RR-02:** 사이버보안 위험 관리와 관련된 역할, 책임 및 권한이 수립되고 전달되며 이해되고 집행됩니다.
 - **GV.RR-03:** 사이버보안 위험 전략, 역할, 책임 및 정책에 상응하는 충분한 자원이 배정됩니다.
 - **GV.RR-04:** 사이버보안이 인적 자원 관행에 포함됩니다.

 - **정책 (GV.PO):** 조직의 사이버보안 정책을 수립하고 전달하며 집행합니다.
 - **GV.PO-01:** 사이버보안 위험을 관리하기 위한 정책이 조직 맥락, 사이버보안 전략 및 우선 순위에 기반하여 수립되고, 전달되며 집행됩니다.
 - **GV.PO-02:** 사이버보안 위험을 관리하기 위한 정책이 요구 사항, 위협, 기술 및 조직의 임무 변화를 반영하도록 검토, 업데이트, 전달 및 집행됩니다.

 - **감독 (GV.OV):** 조직 전체의 사이버보안 위험 관리 활동과 성과 결과를 사용하여 위험 관리 전략을 정보에 기반하여 개선하고 조정합니다.
 - **GV.OV-01:** 사이버보안 위험 관리 전략의 결과를 전략 및 방향 조정을 위해 검토합니다.
 - **GV.OV-02:** 사이버보안 위험 관리 전략이 조직의 요구 사항과 위험을 포괄하도록 검토 및 조정됩니다.
 - **GV.OV-03:** 조직의 사이버보안 위험 관리 성과가 평가되고 조정이 필요한 부분에 대해 검토됩니다.

 - **사이버보안 공급망 위험 관리 (GV.SC):** 조직 이해관계자가 사이버 공급망 위험 관리 프로세스를 수립, 관리, 모니터링, 개선합니다.
 - **GV.SC-01:** 사이버보안 공급망 위험 관리 프로그램, 전략, 목표, 정책 및 프로세스가 수립되고 조직 이해관계자에 의해 동의됩니다.
 - **GV.SC-02:** 공급업체, 고객, 파트너에 대한 사이버보안 역할 및 책임을 수립하고 내부와 외부에서 소통하며 조정합니다.
 - **GV.SC-03:** 사이버보안 공급망 위험 관리가 사이버보안 및 기업 위험 관리, 위험 평가 및 개선 프로세스에 통합됩니다.

- **GV.SC-04:** 공급업체를 중요도에 따라 식별하고 우선 순위를 지정합니다.
- **GV.SC-05:** 공급망의 사이버보안 위험을 다루기 위한 요구 사항이 수립되고, 우선순위가 지정되며, 공급업체 및 기타 관련 제3자와의 계약 및 기타 유형의 협약에 통합됩니다.
- **GV.SC-06:** 공식적인 공급업체 또는 기타 제3자 관계를 맺기 전에 위험을 줄이기 위해 계획 및 실사가 수행됩니다.
- **GV.SC-07:** 공급업체의 위험과 그들의 제품 및 서비스, 그리고 기타 제3자의 위험이 이해되고, 기록되며, 우선순위가 지정되고, 평가되며, 대응되고, 관계의 전 과정에서 모니터링됩니다.
- **GV.SC-08:** 관련 공급업체 및 기타 제3자가 사고 계획, 대응 및 복구 활동에 포함됩니다.
- **GV.SC-09:** 공급망 보안 관행이 사이버보안 및 기업 위험 관리 프로그램에 통합되며, 기술 제품 및 서비스의 수명 주기 전반에 걸쳐 그 성능이 모니터링됩니다.
- **GV.SC-10:** 사이버보안 공급망 위험 관리 계획은 파트너십이나 서비스 계약 종료 후에 발생하는 활동을 위한 조항을 포함합니다.

IDENTIFY (ID): 조직의 현재 사이버보안 위험을 이해합니다.

- **자산 관리 (ID.AM):** 조직이 비즈니스 목적을 달성하는 데 필요한 자산(예: 데이터, 하드웨어, 소프트웨어, 시스템, 시설, 서비스, 인력)이 식별되고 조직 목표 및 조직의 위험 전략에 따라 그 중요성에 맞게 관리합니다.
 - **ID.AM-01:** 조직이 관리하는 하드웨어의 목록이 유지됩니다.
 - **ID.AM-02:** 조직이 관리하는 소프트웨어, 서비스, 시스템의 목록이 유지됩니다.
 - **ID.AM-03:** 조직의 승인된 네트워크 통신 및 내부 및 외부 네트워크 데이터 흐름의 표현이 유지됩니다.
 - **ID.AM-04:** 공급업체가 제공하는 서비스의 목록이 유지됩니다.
 - **ID.AM-05:** 자산은 분류, 중요도, 자원 및 목표에 미치는 영향에 따라 우선순위를 지정합니다.
 - **ID.AM-07:** 지정된 데이터 유형에 대한 데이터 및 해당 메타데이터의 목록을 유지합니다.
 - **ID.AM-08:** 시스템, 하드웨어, 소프트웨어, 서비스 및 데이터를 수명 주기 동안 관리합니다.

- **위험 평가 (ID.RA):** 조직, 자산 및 개인에 대한 사이버보안 위험을 조직이 파악합니다.
 - **ID.RA-01:** 자산의 취약점이 식별되고, 검증되며, 기록됩니다.
 - **ID.RA-02:** 정보 공유 포럼과 소스로부터 사이버 위협 정보가 수신됩니다.
 - **ID.RA-03:** 조직에 대한 내부 및 외부 위협을 식별하고 기록합니다.
 - **ID.RA-04:** 위협이 취약점을 악용할 때의 잠재적 영향과 가능성을 식별하고 기록합니다.
 - **ID.RA-05:** 위협, 취약점, 가능성 및 영향을 사용하여 내재적 위험을 이해하고 위험 대응 우선순위를 정하는 데 도움을 줍니다.
 - **ID.RA-06:** 위험 대응이 선택되고, 우선 순위가 지정되며, 계획되고, 추적되고, 소통됩니다.
 - **ID.RA-07:** 변경사항 및 예외가 관리되며, 위험 영향에 대해 평가되고, 기록되며 추적됩니다.
 - **ID.RA-08:** 취약점 공개를 받고, 분석하고, 대응하는 프로세스가 수립됩니다.
 - **ID.RA-09:** 하드웨어와 소프트웨어의 진위성 및 무결성이 선정 및 사용 전에 평가됩니다.
 - **ID.RA-10:** 중요 공급업체가 선정 전에 평가됩니다.

- **개선 (ID.IM):** 조직의 사이버보안 위험 관리 프로세스, 절차 및 활동의 개선 사항이 모든 CSF 기능에 걸쳐 식별됩니다.
 - **ID.IM-01:** 평가에서 개선 사항을 식별합니다.
 - **ID.IM-02:** 보안 테스트 및 연습을 통해 개선 사항이 식별됩니다. 이는 공급업체 및 관련 제3자와 협조하여 수행된 경우를 포함합니다.
 - **ID.IM-03:** 운영 프로세스, 절차 및 활동의 실행으로부터 개선 사항이 식별됩니다.
 - **ID.IM-04:** 사고 대응 계획 및 운영에 영향을 미치는 기타 사이버보안 계획이 수립되고, 전달되며, 유지되고 개선됩니다.

PROTECT (PR): 조직의 사이버보안 위험을 관리하기 위한 보호 조치가 사용됩니다.

- **신원 관리, 인증 및 접근 제어 (PR.AA):** 물리적 및 논리적 자산에 대한 접근은 승인된 사용자, 서비스, 하드웨어로 제한되며 무단 접근의 위험 평가에 반응하게 관리됩니다.

- **PR.AA-01:** 승인된 사용자, 서비스 및 하드웨어에 대한 신원 및 자격 증명을 조직에서 관리합니다.
 - **PR.AA-02:** 신원은 상호 작용의 맥락에 따라 자격 증명과 연결되어 검증됩니다.
 - **PR.AA-03:** 사용자, 서비스 및 하드웨어가 인증됩니다.
 - **PR.AA-04:** 신원 확인 내용은 보호되고, 전달되며, 검증됩니다.
 - **PR.AA-05:** 정책에 따라 접근 권한, 자격, 승인을 정의, 관리, 집행, 검토하며, 여기에 최소 권한 원칙과 직무 분리 원칙을 포함합니다.
 - **PR.AA-06:** 자산에 대한 물리적 접근은 위험에 상응하여 관리되고, 모니터링되며, 집행됩니다.
-
- **인식 및 교육 (PR.AT):** 조직의 인력이 사이버보안과 관련된 업무를 수행할 수 있도록 사이버보안 인식 및 교육을 제공받습니다.
 - **PR.AT-01:** 직원들이 일반적인 업무를 수행할 때 사이버보안 위험을 고려할 수 있는 지식과 기술을 갖추도록 인식 및 교육을 제공합니다.
 - **PR.AT-02:** 특수 역할을 수행하는 개인은 해당 업무를 수행할 때 사이버보안 위험을 고려할 수 있는 지식과 기술을 갖추도록 인식 및 교육을 제공받습니다.
-
- **데이터 보안 (PR.DS):** 데이터는 조직의 위험 전략에 따라 관리되어 정보의 기밀성, 무결성 및 가용성을 보호합니다.
 - **PR.DS-01:** 저장된 데이터의 기밀성, 무결성 및 가용성이 보호됩니다.
 - **PR.DS-02:** 전송 중인 데이터의 기밀성, 무결성 및 가용성이 보호됩니다.
 - **PR.DS-10:** 사용 중인 데이터의 기밀성, 무결성 및 가용성이 보호됩니다.
 - **PR.DS-11:** 데이터 백업이 생성되고, 보호되며, 유지되고, 테스트됩니다.
-
- **플랫폼 보안 (PR.PS):** 물리적 및 가상 플랫폼의 하드웨어, 소프트웨어(예: 펌웨어, 운영체제, 애플리케이션) 및 서비스는 조직의 위험 전략에 따라 관리되어 그들의 기밀성, 무결성 및 가용성을 보호합니다.
 - **PR.PS-01:** 구성 관리 관행이 수립되고 적용됩니다.
 - **PR.PS-02:** 소프트웨어는 위험에 상응하여 유지, 교체 및 제거됩니다.
 - **PR.PS-03:** 하드웨어는 위험에 상응하여 유지, 교체 및 제거됩니다.
 - **PR.PS-04:** 로그 기록이 생성되어 지속적인 모니터링에 사용할 수 있도록 제공됩니다.

- **PR.PS-05:** 승인되지 않은 소프트웨어의 설치 및 실행이 방지됩니다.
- **PR.PS-06:** 안전한 소프트웨어 개발 관행이 통합되고, 소프트웨어 개발 생명 주기 전반에 걸쳐 그 성능이 모니터링됩니다.

-
- **기술 인프라 복원력 (PR.IR):** 보안 아키텍처는 조직의 위험 전략에 따라 자산의 기밀성, 무결성, 가용성 및 조직의 복원력을 보호하기 위해 관리됩니다.
 - **PR.IR-01:** 네트워크와 환경은 무단 논리적 접근 및 사용으로부터 보호됩니다.
 - **PR.IR-02:** 조직의 기술 자산은 환경적 위협으로부터 보호됩니다.
 - **PR.IR-03:** 정상 및 불리한 상황에서 복원력 요구 사항을 달성하기 위한 메커니즘이 구현됩니다.
 - **PR.IR-04:** 가용성을 보장하기 위한 적절한 자원 용량이 유지됩니다.

DETECT (DE): 가능한 사이버보안 공격과 침해가 발견되고 분석됩니다.

- **지속적인 모니터링 (DE.CM):** 자산을 모니터링하며 이상 현상, 침해 징수, 기타 잠재적으로 유해한 사고를 발견합니다.
 - **DE.CM-01:** 네트워크와 네트워크 서비스가 잠재적으로 유해한 사고를 찾기 위해 모니터링됩니다.
 - **DE.CM-02:** 물리적 환경이 잠재적으로 유해한 사고를 찾기 위해 모니터링됩니다.
 - **DE.CM-03:** 인력 활동 및 기술 사용이 잠재적으로 유해한 사고를 찾기 위해 모니터링됩니다.
 - **DE.CM-06:** 외부 서비스 제공업체의 활동 및 서비스가 잠재적으로 유해한 사고를 찾기 위해 모니터링됩니다.
 - **DE.CM-09:** 컴퓨팅 하드웨어 및 소프트웨어, 런타임 환경 및 해당 데이터가 잠재적으로 유해한 사고를 찾기 위해 모니터링됩니다.

- **위협 이벤트 분석 (DE.AE):** 이상 현상, 침해의 징후 및 기타 잠재적으로 유해한 사고를 분석하여 사고의 특성을 파악하고 사이버보안 사고를 감지합니다.
 - **DE.AE-02:** 잠재적으로 위협적인 사고를 분석하여 관련 활동을 더 잘 이해합니다.
 - **DE.AE-03:** 여러 출처의 정보를 상관 분석합니다.

- **DE.AE-04:** 유해한 사고의 예상 영향과 범위를 이해합니다.
 - **DE.AE-06:** 유해한 사고에 대한 정보가 승인된 직원 및 도구에 제공됩니다.
 - **DE.AE-07:** 사이버 위협 인텔리전스 및 기타 맥락 정보가 분석에 통합합니다.
 - **DE.AE-08:** 유해한 사고가 정의된 사고 기준을 충족할 때 사고를 선언합니다.
-
-

RESPOND (RS): 감지된 사이버보안 사고에 대하여 조치를 취합니다.

- **사고 관리 (RS.MA):** 감지된 사이버보안 사고에 대한 대응을 관리합니다.
 - **RS.MA-01:** 사고가 선언되면 관련 제3자와 협조하여 사고 대응 계획을 실행합니다.
 - **RS.MA-02:** 사고 보고서가 분류되고 검증됩니다.
 - **RS.MA-03:** 사고가 분류되고 우선 순위가 지정됩니다.
 - **RS.MA-04:** 필요에 따라 사고가 확대되거나 상향 조정됩니다.
 - **RS.MA-05:** 사고 복구를 시작하기 위한 기준이 적용됩니다.
 - **사고 분석 (RS.AN):** 효과적인 대응을 보장하고 포렌식 및 복구 활동을 지원하기 위해 조사를 수행합니다.
 - **RS.AN-03:** 사고 중에 발생한 일과 사고의 근본 원인을 파악하기 위해 분석이 수행됩니다.
 - **RS.AN-06:** 조사 중 수행된 조치들이 기록되며, 기록의 무결성과 출처가 보존됩니다.
 - **RS.AN-07:** 사고 데이터와 메타데이터가 수집되며, 그 무결성과 출처가 보존됩니다.
 - **RS.AN-08:** 사고의 규모가 추정되고 검증됩니다.
 - **사고 대응 보고 및 소통 (RS.CO):** 법률, 규정 또는 정책에 따라 필요한 경우 내부 및 외부 이해관계자와 대응 활동을 조율합니다.
 - **RS.CO-02:** 내부 및 외부 이해관계자에게 사고를 통보합니다.
 - **RS.CO-03:** 지정된 내부 및 외부 이해관계자와 정보가 공유됩니다.
 - **사고 완화 (RS.MI):** 사고의 확대를 방지하고 그 영향을 완화하기 위한 활동이 수행됩니다.
 - **RS.MI-01:** 사고가 제한됩니다.
 - **RS.MI-02:** 사고가 근절됩니다.
-

RECOVER (RC): 사이버보안 사고에 영향을 받은 자산과 운영이 복원됩니다.

- **사고 복구 계획 및 실행 (RC.RP):** 사이버보안 사고에 영향을 받은 시스템과 서비스의 운영 가능성을 보장하기 위해 복원 활동이 수행됩니다.
 - **RC.RP-01:** 사고 대응 과정에서 시작된 사고 대응 계획의 복구 부분이 실행됩니다.
 - **RC.RP-02:** 복구 조치가 선택되고, 범위가 정의되며, 우선 순위가 지정되고, 수행됩니다.
 - **RC.RP-03:** 복원에 사용하기 전에 백업 및 기타 복원 자산의 무결성이 검증됩니다.
 - **RC.RP-04:** 사고 후 운영 규범을 설정하기 위해 중요한 임무 기능과 사이버보안 위험 관리가 고려됩니다.
 - **RC.RP-05:** 복원된 자산의 무결성이 검증되며, 시스템과 서비스가 복원되고, 정상 운영 상태가 확인됩니다.
 - **RC.RP-06:** 기준에 따라 사고 복구 종료 선언되고, 사고 관련 문서 작업이 완료됩니다.

 - **사고 복구 및 소통 (RC.CO):** 복원 활동이 내부 및 외부 당사자들과 조율됩니다.
 - **RC.CO-03:** 복구 활동과 운영 능력 복원 진행 상황을 지정된 내부 및 외부 이해관계자에게 전달합니다.
 - **RC.CO-04:** 사고 복구에 대한 공개 업데이트는 승인된 방법과 메시징을 사용하여 공유됩니다.
-

부록 B. CSF 단계

표 2는 제3절에서 논의된 CSF 단계의 개념적 일러스트레이션을 포함하고 있습니다. 이 단계는 조직의 사이버보안 위험 거버넌스 관행(거버넌)과 사이버보안 위험 관리 관행(식별, 보호, 탐지, 대응, 복구)의 엄격성을 구별합니다.

표 2. CSF 단계의 개념적 일러스트레이션

단계	사이버보안 위험 거버넌스	사이버보안 위험 관리
Tier 1: 불완전	<p>조직의 사이버보안 위험 전략 적용이 임시방편적으로 관리됩니다.</p> <p>우선순위 지정이 임의적이며 목표나 위험 환경에 기반한 공식적인 기준이 없습니다.</p>	<p>조직 수준에서 사이버보안 위험에 대한 인식이 제한적입니다.</p> <p>조직은 사고별로 불규칙적으로 사이버보안 위험 관리를 수행합니다.</p> <p>조직 내에서 사이버보안 정보를 공유할 수 있는 프로세스가 없을 수 있습니다.</p> <p>조직은 일반적으로 자신의 공급업체 및 취득하고 사용하는 제품 및 서비스와 관련된 사이버보안 위험을 인식하지 못합니다.</p>
Tier 2: 위험 인식	<p>위험 관리 관행은 경영진에 의해 승인되었지만, 조직 전체의 정책으로 확립되지는 않았습니다.</p> <p>사이버보안 활동 및 보호 필요성의 우선 순위는 조직의 위험 목표, 위험 환경 또는 비즈니스/임무 요구에 직접적으로 정보를 제공받습니다.</p>	<p>조직 수준에서 사이버보안 위험에 대한 인식은 있지만, 조직 전체적으로 사이버보안 위험을 관리하는 접근 방식이 확립되지 않았습니다.</p> <p>조직의 목표와 프로그램에서 사이버보안을 고려하는 것은 일부 조직 수준에서만 발생할 수 있습니다. 조직 및 외부 자산의 사이버 위험 평가는 발생하지만 일반적으로 반복 가능하거나 반복적이지 않습니다.</p> <p>사이버보안 정보는 조직 내에서 비공식적으로 공유됩니다.</p> <p>조직은 공급업체 및 취득하고 사용하는 제품 및 서비스와 관련된 사이버보안 위험을 인식하고 있지만, 그러한 위험에 대해 일관되거나 공식적으로 대응하지 않습니다.</p>
Tier 3: 재현 가능	<p>조직의 위험 관리 관행이 공식적으로 승인되어 정책으로 표현됩니다.</p> <p>위험에 기반한 정책, 프로세스 및 절차가 정의되어 의도대로 실행되며 검토됩니다.</p> <p>조직의 사이버보안 관행은 비즈니스/임무 요구, 위험 및 기술 환경의 변화에 따라 위험 관리 프로세스 적용을 바탕으로 정기적으로</p>	<p>조직 전체적인 접근 방식을 통해 사이버보안 위험을 관리합니다. 사이버보안 정보는 조직 전체에 정기적으로 공유됩니다.</p> <p>위험 변화에 효과적으로 대응하기 위한 일관된 방법이 마련되어 있습니다. 직원은 자신의 역할과 책임을 수행하기 위한 지식과 기술을 갖추고 있습니다.</p> <p>조직은 자산의 사이버보안 위험을 지속적으로 정확하게 모니터링합니다. 사이버보안 및 비사이버보안 경영진은 사이버보안 위험에 대해 정기적으로 소통합니다.</p>

	<p>업데이트됩니다.</p>	<p>경영진은 조직의 모든 운영 라인에서 사이버보안을 고려하도록 합니다.</p> <p>조직의 위험 전략은 공급업체와 조직이 취득하고 사용하는 제품 및 서비스와 관련된 사이버보안 위험에 의해 정보를 제공받습니다. 직원들은 기준 요구 사항을 전달하는 서면 계약, 거버넌스 구조(예: 위험 위원회), 정책 실행 및 모니터링과 같은 메커니즘을 통해 이러한 위험에 공식적으로 대응합니다. 이러한 조치들은 일관되게 의도대로 실행되며 지속적으로 모니터링되고 검토됩니다.</p>
<p>Tier 4: 적합</p>	<p>조직 전체적인 접근 방식을 통해 사이버보안 위험을 관리합니다. 이는 위험에 기반한 정책, 프로세스 및 절차를 사용하여 잠재적인 사이버보안 사고에 대응합니다. 사이버보안 위험과 조직 목표 간의 관계는 명확히 이해되고 의사 결정 시 고려됩니다.</p> <p>경영진은 사이버보안 위험을 재무 및 기타 조직적 위험과 동일한 맥락에서 모니터링합니다. 조직 예산은 현재 및 예측된 위험 환경과 위험 허용도에 대한 이해에 기반합니다. 사업 부서는 경영진의 비전을 실행하고 조직의 위험 허용도 맥락에서 시스템 수준의 위험을 분석합니다.</p> <p>사이버보안 위험 관리는 조직 문화의 일부로, 이전 활동에 대한 인식과 조직 시스템 및 네트워크에서의 지속적인 활동에 대한 인식에서 발전합니다.</p> <p>조직은 비즈니스/임무 목표의 변화에 대해 위험 접근 방식과 소통 방식을 신속하고 효율적으로 반영할 수 있습니다.</p>	<p>조직은 이전 및 현재의 사이버보안 활동을 바탕으로 사이버보안 관행을 조정합니다. 여기에는 교훈과 예측 지표를 포함합니다. 고급 사이버보안 기술과 관행을 통합하는 지속적인 개선 과정을 통해 조직은 변화하는 기술 환경에 적극적으로 적응하며 진화하는 정교한 위험에 신속하고 효과적으로 대응합니다.</p> <p>조직은 실시간 또는 거의 실시간 정보를 사용하여 공급업체 및 취득하고 사용하는 제품 및 서비스와 관련된 사이버보안 위험을 이해하고 일관되게 대응합니다.</p> <p>사이버보안 정보는 조직 내부 및 승인된 제3자와 지속적으로 공유됩니다.</p>

부록 C. 용어집

CSF 카테고리

CSF 기능을 구성하는 관련 사이버보안 결과의 그룹입니다.

CSF 커뮤니티 프로파일

여러 조직 간의 공유된 관심사와 목표를 해결하기 위해 생성 및 발행되는 CSF 결과의 기준선입니다. 커뮤니티 프로파일은 일반적으로 특정 부문, 하위 부문, 기술, 위협 유형 또는 기타 사용 사례를 위해 개발합니다. 조직은 커뮤니티 프로파일을 자체 목표 프로파일의 기초로 사용할 수 있습니다.

CSF 코어

어떤 조직이든 자신의 사이버보안 위험을 관리하는 데 도움이 될 수 있는 고위 수준의 사이버보안 결과 분류입니다. 그 구성요소는 각 결과를 자세히 설명하는 기능, 카테고리, 하위 카테고리의 계층 구조로 되어 있습니다.

CSF 현재 프로파일

조직이 현재 달성하고 있는 (또는 달성하려고 시도하는) 코어 결과를 명시하고, 각 결과가 어떻게 또는 어느 정도로 달성되고 있는지를 특성화하는 조직 프로파일의 일부입니다.

CSF 기능

사이버보안 결과를 위한 최상위 조직 수준입니다. CSF 기능에는 거버넌, 식별, 보호, 탐지, 대응, 복구의 여섯 가지가 있습니다.

CSF 구현 예시

CSF 코어 결과 달성을 돕기 위한 간결하고 실천적인 개념적 일러스트레이션입니다.

CSF 참고 자료

CSF 코어 결과와 기존 표준, 지침, 규정 또는 기타 콘텐츠 간의 관계를 나타내는 매핑입니다.

CSF 조직 프로파일

조직의 현재 및/또는 목표 사이버보안 자세를 CSF 코어의 결과 측면에서 기술하는 메커니즘입니다.

CSF 킷 스타트 가이드

CSF 관련 특정 주제에 대한 간결하고 실천적인 지침을 제공하는 보조 자료입니다.

CSF 하위 카테고리

CSF 카테고리를 구성하는 보다 구체적인 기술 및 관리 사이버보안 활동의 결과 그룹입니다.

CSF 목표 프로파일

조직이 선택하고 우선 순위를 지정한 원하는 코어 결과를 명시하는 조직 프로파일의 일부로, 조직의 사이버보안 위험 관리 목표를 달성하기 위해 설정됩니다.

CSF 단계

조직의 사이버보안 위험 거버넌스 및 관리 관행의 엄격성을 특성화합니다. 불완전(Tier 1), 위험 인식(Tier 2), 재현 가능(Tier 3), 적합(Tier 4) 단계, 이렇게 네 가지 단계가 있습니다.

해당 프레임워크에서는 실험 절차를 적절하게 명시하기 위해 특정 상업 장비, 기기, 소프트웨어, 자재, 상업 및 비상업성이 언급됩니다. 이러한 언급은 NIST에서 어떤 제품이나 서비스를 추천한다거나 승인한다는 것을 의미하지 않으며, 언급한 자재나 장비가 해당 목적에 있어 최적이라는 것을 의미하는 것도 아닙니다.

NIST 기술 시리즈 정책

[저작권, 사용 및 라이선스 선언](#)

[NIST 기술 시리즈 출판물 식별자 구문](#)

NIST 기술 시리즈 출판물을 인용하는 방법:

미국 국립표준기술연구소 (2024) NIST 사이버보안 프레임워크 (CSF) 2.0. (미국 국립표준기술연구소, Gaithersburg, MD), NIST 사이버보안 백서 (CSWP) NIST CSWP 29 kor.

<https://doi.org/10.6028/NIST.CSWP.29.kor>

연락처 정보

cyberframework@nist.gov

미국 국립표준기술연구소

귀하: 응용 사이버보안 부서, 정보기술 연구소 앞

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

모든 의견은 정보공개법(FOIA)에 따라 공개될 수 있습니다.