핵심 인프라 사이버보안 개선을 위한 프레임워크

버전 1.1

국립 표준 기술 연구소
(National Institute of Standards and Technology)

2018 년 4 월 16 일

https://doi.org/10.6028/NIST.CSWP.6.kor

번역: 곽병현, 임경찬 (University of Tennessee in Knoxville)
감독: 김두원 교수님 (University of Tennessee in Knoxville)

Translated by Byounghyeun Kwak, Kyoungchan Lim (University of Tennessee in Knoxville)
Reviewed by Prof. Doowon Kim (University of Tennessee in Knoxville) and TaikaTranslations LLC.
Official U.S. Government translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.6.

개선 사항에 대한 노트

해당 사이버보안 프레임워크 버전 1.1 은 2014 년 2 월에 발표된 버전 1.0 을 더욱 세밀화하고 명확화 하였습니다. 이 버전의 두 개의 초안에 대한 의견들을 통합하여 반영하였습니다. 버전 1.1 은 기존에 해당 프레임워크를 사용하던 사용자나 처음으로 이 프레임워크를 이용하는 사용자 모두가 구현할 수 있도록 만들어졌습니다. 기존 사용자가 버전 1.1 을 전혀 막힘 없이 사용할 수 있도록 버전 1.0 과의 호환성을 주요 목표로 하였습니다.

표 NTR-1 – 프레임워크 버전 1.0 과 버전 1.1 사이의 변경 요약

업데이트	업데이트에 대한 설명
"컴플라이언스"와 같은 다양한 프레임워크 이해당사자들에게 매우 다른 의미를 가질 수 있는 단어들의 뜻을 명확히 하였습니다.	프레임워크가 조직의 자체 사이버 보안 요구 사항들을 조직화하고 표현하는 구조적 언어로서 이용할 수 있도록 프레임워크에 사용하는 단어들에 명확성을 추가하였습니다. 그러나 조직이 프레임워크를 사용하는 다양한 방법들로 인해 "프레임워크에 대한 컴플라이언스"와 같은 구절들은 혼란스러울 수 있습니다.
자가 평가에 관한 새로운 섹션	섹션 4.0 '프레임워크를 사용한 사이버보안 위험 자가평가'를 추가하여 조직이 어떻게 프레임워크를 사용하여 자신의 사이버보안 위험을 이해하고 평가할 수 있는지 측정할 수 있도록 하였습니다.
사이버 공급망 위험 관리 목적으로 프레임워크를 사용하는 방법에 대한 설명을 크게 확장하였습니다.	확장된 섹션 3.3 '이해당사자와의 사이버보안 요구사항 소통'은 사용자들이 사이버 공급망 위험 관리(Cyber Supply Chain Risk Management, SCRM)를 더 잘 이해하도록 도와주며, 새로운 섹션 3.4 '구매 결정'은 상용 제품 및 서비스와 관련된 위험을 이해하는 데 프레임워크의 사용을 강조합니다. 구현 단계(Implementation Tiers)에 추가적인 사이버 SCRM 기준이 추가되었습니다. 마지막으로, 프레임워크 핵심(Core)에 공급망 위험 관리 분류(Supply Chain Risk Management Category)와 여러 하위 분류가 추가되었습니다.
인증, 권한 부여, 그리고 신원 증명을 더 잘 고려하기 위한 세부 조정	접근 제어 분류의 대한 설명이 인증, 권한 부여 및 신원 증명을 더 잘 고려하도록 세밀화 되었습니다. 이를 위해, 인증 및 신원 증명 각각에 대한 하위 분류를 하나씩 추가하였습니다. 또한, 해당 분류의 이름이 해당 분류와 관련 하위 분류의 범위를 더 잘 나타내기 위해 신원 관리 및 접근 제어 (PR.AC)로 변경되었습니다.

구현 단계(Implementation Tiers)와 프로필(Profiles) 사이의 관계에 대한 더 나은 설명	섹션 3.2 '사이버보안 프로그램 설립 또는 개선'을 프레임워크 구현 단계(Tiers)에서 사용하도록 설명하였습니다. 조직의 위험 관리 프로그램 내에서의 프레임워크 고려 사항의 통합을 반영하기 위해 프레임워크 단계(Tiers)를 추가하였습니다. 프레임워크 단계의 개념 또한 세밀화 되었습니다. 그림 2.0 을 업데이트하여 프레임워크 단계에서의 행동들을 포함시켰습니다.
조정된 취약점 공개에 대한 고려	취약점 공개 라이프사이클과 관련된 하위 분류가 추가되었습니다.

버전 1.0 과 마찬가지로, 버전 1.1 사용자들은 조직의 개별적 가치를 극대화하기 위해 프레임워크를 맞춤화 하는 것을 권장합니다.

감사의 글

이 출판물은 산업계, 학계, 정부 간의 지속적인 협력의 결과물입니다. 국립 표준 기술 연구소(NIST)는 2013 년 사립 및 공공 부문의 조직과 개인들을 모아 프로젝트를 시작하였습니다. 2014 년에 출판되고 2017 년과 2018 년 동안 수정된 이 *'핵심 인프라 사이버보안 개선을 위한 프레임워크'*는 미국의 모든 분야와 전 세계의 많은 분야의 이해당사자들과의 수천 번의 직접적인 상호작용, 여덟 번의 공개 워크숍, 다수의 의견 및 정보 요청을 통해 만들어졌습니다.

버전 1.0 을 변경하는 계기와 이 버전 1.1 에 나타나는 변경 사항은 다음에 기반합니다:

- 프레임워크 버전 1.0 발표 이후 NIST 에 제출된 피드백 및 자주 묻는 질문;
- 2015 년 12 월 정보 요청(RFI), 핵심 인프라 사이버보안 개선을 위한 프레임워크에 대한 의견에 대한 105 개의 응답;
- 2017 년 12 월 5 일 제안된 버전 1.1 의 두 번째 초안에 대한 85 개 이상의 코멘트;
- 2017 년 1 월 10 일 제안된 버전 1.1 의 첫 번째 초안에 대한 120 개 이상의 코멘트;
- 2016 년과 2017 년 프레임워크 워크숍에 참석한 1,200 명 이상의 참가자들의 의견.

또한, NIST 는 이전에 사이버보안 프레임워크의 버전 1.0 을 핵심 인프라 사이버보안 개선을 위한 NIST 로드맵이라는 동반 문서와 함께 발표하였습니다. 이 로드맵은 추가 개발, 조정 및 협업을 위한 주요 "개선 영역"을 강조하였습니다. 사립 및 공공 부문의 노력을 통해 일부 개선 영역은 이 프레임워크 버전 1.1 에 포함될 정도로 충분히 발전하였습니다.

NIST 는 이 프레임워크에 기여한 모든 분들에게 감사의 말씀을 전합니다.

핵심 요약

핵심 인프라 기능의 신뢰성은 미국의 기반입니다. 사이버보안 위협은 중요한 인프라 시스템의 증가된 복잡성과 연결성을 악용하여 국가의 안보, 경제, 대중의 안전 및 건강을 위태롭게 합니다. 재무적 및 평판 위험과 마찬가지로, 사이버보안 위험은 회사의 기반에 영향을 줍니다. 이는 비용을 증가시키고 수익에 영향을 줄 수 있습니다. 이는 조직의 혁신과 고객을 얻고 유지하는 능력에 해를 끼칠 수 있습니다. 사이버보안은 조직의 전반적인 위험 관리의 중요한 구성 요소이며 그 중요성은 점점 커지고 있습니다.

이러한 위험을 더 잘 다루기 위해, 2014 년 사이버보안 강화 법(CEA)[1] 은 국립 표준 및 기술 연구소(NIST)의 역할을 핵심 인프라의 소유자 및 운영자가 자발적으로 사용할 수 있는 사이버보안 프레임워크를 식별하고 개발하는 것으로 확장했습니다. CEA 에 의해서, NIST 는 "핵심 인프라의 소유자 및 운영자가 자발적으로 사용할 수 있는 우선 순위를 고려하고, 유연하며, 반복 가능하고, 수행 기반의, 경제적인 접근 방식의 정보 보안 측정 및 제어방법으로 그들이 사이버 위험을 식별, 평가 및 관리하는 데 도움을 주는 방법"을 찾아야 했습니다. 이는 NIST 의 이전 작업인 "중요한 인프라 사이버보안 개선"을 위한 행정 명령 13636(2013 년 2 월)에 따라 프레임워크 버전 1.0 을 개발을 공식화하였으며, 미래의 프레임워크 발전을 위한 지침을 제공했습니다. EO 13636 하에 개발된 프레임워크는 CEA 에 의해 계속 발전하며, 비즈니스와 조직의 필요를 기반으로 추가적인 규제 요구 사항을 기업에 부과하지 않으면서, 경제적인 방식으로 사이버보안 위험을 다루기 위한 일반적인 언어를 사용합니다.

프레임워크는 사이버보안 활동을 하나의 비즈니스 영향요소로서 인지하도록 초점을 맞추며, 조직의 위험 관리 프로세스의 일부로 사이버보안 위험을 고려합니다. 프레임워크는 프레임워크 코어, 구현 단계 및 프레임워크 프로필의 세 부분으로 구성됩니다. 프레임워크 코어는 여러 부문과 핵심 인프라 간에 공통인 사이버보안 활동, 결과 및 유익한 참조 정보들의 집합입니다. 프레임워크 코어의 요소들은 개별 조직 프로필을 개발하기 위한 상세한 지침을 제공합니다. 프로필의 사용을 통해, 프레임워크는 조직이 비즈니스/임무 요구 사항, 위험 허용도 및 자원에 따라 사이버보안 활동을 조정하고 우선순위를 지정하는 데 도움을 줄 것입니다. 각각의 단계는 조직이 사이버보안 위험 관리 접근법의 특성을 보고 이해하는 데 도움을 주는 메커니즘을 제공합니다.

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

이 문서는 핵심 인프라의 사이버보안 위험 관리를 개선하기 위해 개발되었지만, 이 프레임워크는 어떠한 부문이나 커뮤니티의 조직에서도 사용될 수 있습니다. 이 프레임워크는 조직의 크기, 사이버보안 위험의 정도 또는 사이버보안의 전문성에 관계없이 위험 관리의 원칙과 모범 사례를 적용하여 보안과 회복탄력성을 향상시키는 데 도움을 줍니다.

프레임워크는 현재 효과적으로 작동하는 표준, 지침, 및 관행을 모아 사이버보안에 대한 다양한 접근법에 대한 공통의 조직 구조를 제공합니다. 또한, 프레임워크는 사이버보안을 위한 전세계적으로 인정받는 표준을 참조하기 때문에 핵심 인프라 뿐만 아니라 다른 부문과 커뮤니티에서의 사이버보안 강화를 위한 국제 협력의 모델로서 기능할 수 있습니다.

프레임워크는 물리적, 사이버 공간적 및 인간 차원에서의 사이버보안의 영향을 포함하여 사이버보안을 다루는 유연한 방법을 제공합니다. 이 프레임워크는 정보 기술(IT), 산업 제어 시스템(ICS), 사이버-물리 시스템(CPS), 사물인터넷(IoT)과 같은 더 일반적인 연결기기들과 관련 있는 조직에 적용할 수 있습니다. 프레임워크는 고객, 직원 및 다른 이해당사자들의 개인정보에 영향을 주는 사이버보안을 다루는 조직들을 도와줄 수 있습니다. 또한 프레임워크의 결과는 인력 개발 및 교육 활동의 대상으로 제공됩니다.

프레임워크는 핵심 인프라의 사이버보안 위험을 관리하기 위한 일률적인 접근법이 아닙니다. 조직은 여전히 각각의 다양한 위협, 취약점, 위험 허용도에 따라 고유한 위험을 가지고 있을 것입니다. 그들은 또한 해당 프레임워크를 어떻게 맞춤화 하는지에 따라 차이를 보일 것입니다. 조직은 중요한 서비스 제공에 필요한 활동을 결정하고 우선 순위 화하여, 조직의 리소스 투입의 효과를 극대화할 수 있습니다. 궁극적으로, 프레임워크는 사이버보안 위험을 감소시키고 더 잘 관리하는 것을 목표로 합니다.

조직의 고유한 사이버보안 요구 사항을 다루기 위해 프레임워크를 사용하는 다양한 방법이 있습니다. 어떻게 적용할 것인지에 대한 결정은 실행 조직에게 맡겨져 있습니다. 예를 들어, 어떤 조직은 구상한 위험 관리 프로그램을 명확히 하기 위해 프레임워크의 구현 단계를 사용할 수 있습니다. 또 다른 조직은 전체 위험 관리 포트폴리오를 분석하기 위해 프레임워크의 다섯 가지 기능을 사용할 수 있습니다; 해당 분석은 제어 카탈로그와 같은 보다 상세한 지침에 의존할 수도 있고 그렇지 않을 수도 있습니다. "프레임워크 준수"에 대한 토론이 종종 있지만, 프레임워크는 조직의 고유한 사이버보안 요구 사항과 준수를 조직화하고 표현하기 위한 구조 및 언어로서의 유용성이 있습니다. 그럼에도 불구하고, 조직에서 프레임워크를 사용하는 다양한 방법 때문에 "프레임워크 준수"와 같은 구절이 다양한 이해당사자에게 혼란을 야기하고, 매우 다른 의미로 받아드려 질 수 있음을 의미합니다.

프레임워크는 산업 현장에서 구현하고 제공한 피드백에 따라 지속적으로 업데이트되고 개선되는 살아있는 문서입니다. NIST 는 모든 수준에서 민간부문 및 정부 기관과의 협력을 계속 이어 나갈 것입니다. 프레임워크가 더 널리 실천됨에 따라, 추가적인 교훈은 미래의 버전에 통합될 것입니다. 이것은 새로운 위협, 위험 및 해결책들이 역동하는 도전적인 환경에서 중요한 인프라 소유자 및 운영자의 필요를 충족시키려 함입니다.

이 자발적인 프레임워크의 확장, 효과적인 사용 및 최선의 실행 경험의 대한 공유는 우리 국가의 핵심 인프라의 사이버 보안을 향상시키기 위한 다음 단계입니다 – 개별 조직을 위한 향상된 지침을 제공하는 동시에 국가의 핵심 인프라 및 더 넓은 경제 및 사회의 사이버 보안에 대한 태도를 향상시킵니다.

목 차

그림 목록

테이블 목록

1.0 프레임워크 소개

핵심 인프라 기능의 신뢰성은 미국의 기반입니다. 사이버보안 위협은 중요한 인프라 시스템의 증가된 복잡성과 연결성을 악용하여 국가의 안보, 경제, 대중의 안전 및 건강을 위태롭게 합니다. 재무적 및 평판 위험과 마찬가지로, 사이버보안 위험은 회사의 기반에 영향을 줍니다. 이는 비용을 증가시키고 수익에 영향을 줄 수 있습니다. 이는 조직의 혁신과 고객을 얻고 유지하는 능력에 해를 끼칠 수 있습니다. 사이버보안은 조직의 전반적인 위험 관리의 중요한 구성 요소이며 그 중요성은 점점 커지고 있습니다.

이 인프라의 복원력을 강화하기 위하여 2014 년 사이버보안 강화법(CEA)[2] 은 국립 표준 기술 연구소(NIST)의 역할을 갱신하여 사이버보안 위험 프레임워크의 개발을 촉진하고 지원하도록 하였습니다. "핵심 인프라의 소유자 및 운영자가 자발적으로 사용할 수 있는 우선 순위를 고려하고, 유연하며, 반복 가능하고, 수행 기반의, 경제적인 접근 방식의 정보 보안 측정 및 제어방법으로 그들이 사이버 위험을 식별, 평가 및 관리하는 데 도움을 주는 방법"을 찾아야 했습니다. 이는 NIST 의 이전 작업인 "중요한 인프라 사이버보안 개선"을 위한 행정 명령 13636(2013 년 2 월)[3] 에 따라 프레임워크 버전 1.0 을 개발을 공식화하였으며, 미래의 프레임워크 발전을 위한 지침을 제공했습니다.

핵심 인프라[4] 는 2001 년 미국 애국법[5] 에 따라 "미국의 중요한 시스템 및 자산으로, 물리적이든 가상이든, 그러한 시스템 및 자산의 무력화나 파괴가 국가의 안보, 국가 경제 안보, 국가 공공 건강 또는 안전에 치명적인 영향을 미칠 것"으로 정의되어 있습니다. 외부 및 내부 위협의 증가로 인해, 핵심 인프라를 담당하는 조직들은 사이버보안 위험을 식별, 평가 및 관리하기 위한 일관되고 반복적인 접근 방식이 필요합니다. 이러한 접근 방식은 조직의 크기, 위협 노출 또는 현재의 사이버보안 전문성에 관계없이 필요합니다.

---

[2] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

[5] See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: https://www.congress.gov/bill/107th-congress/house-bill/3162

핵심 인프라 커뮤니티에는 미국의 인프라를 보호하는 역할을 하는 공공 및 민간 소유주, 운영자 및 기타 기관들이 포함됩니다. 각 핵심 인프라 분야의 구성원들은 정보 기술(IT), 산업 제어 시스템(ICS), 사이버-물리 시스템(CPS), 그리고 일반적으로 연결된 장치, 즉 사물 인터넷(IoT)을 포함한 광범위한 기술 범주를 지원하는 기능을 수행합니다. 이러한 기술, 통신 및 상호 연결성에 대한 의존은 잠재적 취약점을 변경하고 확장 시키며 인프라 운영에 대한 잠재적 위험을 증가시켰습니다. 예를 들어, 기술과 그것이 생산하고 처리하는 데이터가 점점 더 중요한 서비스를 제공하고 비즈니스/임무 결정을 지원하는 데 사용됨에 따라 조직, 개인의 건강과 안전, 환경, 지역 사회, 그리고 보다 넓은 경제와 사회에 대한 사이버보안 사고의 잠재적 영향을 고려해야 합니다.

사이버보안 위험을 관리하기 위해서는 조직의 비즈니스 원동력과 조직이 사용하는 구체적인 기술의 보안 고려사항에 대한 명확한 이해가 필요합니다. 각 조직의 위험, 우선순위 및 시스템이 모두 다르기 때문에, 프레임워크에 의해 설명된 결과를 달성하기 위해 사용되는 도구와 방법 또한 모두 다를 것입니다.

보다 큰 공공의 신뢰를 만들기 위해 개인 정보 보호와 시민의 자유의 대한 역할을 인식하여, 프레임워크에는 핵심 인프라 조직이 사이버보안 활동을 수행할 때 개인의 정보 보호와 시민의 자유를 보호하는 방법론이 포함되어 있습니다. 많은 조직들은 이미 개인 정보와 시민의 자유를 다루기 위한 프로세스를 가지고 있습니다. 이 방법론은 그러한 프로세스를 보완하고 사이버보안 위험 관리에 대한 조직의 접근 방식과 일관성 있는 개인 정보 위험 관리를 촉진하기 위한 지침을 제공하기 위해 설계되었습니다. 개인 정보와 사이버보안을 통합은 고객 신뢰를 높이고, 정보 공유를 더 표준화 하며, 법적 체제를 넘나드는 작업을 단순화함으로써 조직에 이익을 줄 수 있습니다.

프레임워크는 기술 중립적이면서도 기술과 함께 발전하는 다양한 기존의 표준, 지침, 및 실무를 참조하기 때문에 효과적으로 유지되고 기술 혁신을 지원합니다. 산업이 개발, 관리 및 업데이트하는 그러한 글로벌 표준, 지침 및 실무에 의존함으로써, 프레임워크 결과를 달성하기 위해 사용할 수 있는 도구와 방법은 국경을 넘어 확대되며, 사이버보안 위험의 글로벌 특성을 인정하고 기술의 발전 및 비즈니스 요구 사항과 함께 발전할 것입니다. 기존 및 신흥 표준의 사용은 규모의 경제를 가능하게 하며, 확인된 시장 요구 사항을 충족하는 효과적인 제품, 서비스 및 실무의 개발을 촉진할 것입니다. 시장 경쟁은 또한 이러한 기술과 실무의 더 빠른 확산과 이러한 분야의 이해 관계자에 의한 많은 이익의 실현을 촉진합니다.

해당 기준, 지침 및 관행에서 출발하여, 프레임워크는 조직들이 수행할 수 있는 공통된 분류 체계와 메커니즘을 제공합니다:

1) 현재의 사이버보안 상태를 기술;

2) 사이버보안에 대한 목표를 기술;
3) 지속적이고 반복 가능한 프로세스의 맥락에서 개선 기회를 식별하고 우선순위 선정;
4) 목표로의 진전을 평가;
5) 사이버보안 위험에 대해 내부 및 외부 이해관계자들과 소통.

프레임워크는 핵심 인프라의 사이버보안 위험을 관리하기 위한 일률적인 접근법이 아닙니다. 조직은 여전히 각각의 다양한 위협, 취약점, 위험 허용도에 따라 고유한 위험을 가지고 있을 것입니다. 그들은 또한 해당 프레임워크를 어떻게 맞춤화 하는지에 따라 차이를 보일 것입니다. 조직은 중요한 서비스 제공에 필요한 활동을 결정하고 우선 순위 화하여, 조직의 리소스 투입의 효과를 극대화할 수 있습니다. 궁극적으로, 프레임워크는 사이버보안 위험을 감소시키고 더 잘 관리하는 것을 목표로 합니다.

조직의 고유한 사이버보안 요구 사항을 다루기 위해 프레임워크를 사용하는 다양한 방법이 있습니다. 어떻게 적용할 것인지에 대한 결정은 실행 조직에게 맡겨져 있습니다. 예를 들어, 어떤 조직은 구상한 위험 관리 프로그램을 명확히 하기 위해 프레임워크의 구현 단계를 사용할 수 있습니다. 또 다른 조직은 전체 위험 관리 포트폴리오를 분석하기 위해 프레임워크의 다섯 가지 기능을 사용할 수 있습니다; 해당 분석은 제어 카탈로그와 같은 보다 상세한 지침에 의존할 수도 있고 그렇지 않을 수도 있습니다. "프레임워크 준수"에 대한 토론이 종종 있지만, 프레임워크는 조직의 고유한 사이버보안 요구 사항과 준수를 조직화하고 표현하기 위한 구조 및 언어로서의 유용성이 있습니다. 그럼에도 불구하고, 조직에서 프레임워크를 사용하는 다양한 방법 때문에 "프레임워크 준수"와 같은 구절이 다양한 이해당사자에게 혼란을 야기하고, 매우 다른 의미로 받아드려 질 수 있음을 의미합니다.

프레임워크는 조직의 위험 관리 프로세스 및 사이버보안 프로그램을 보완하며, 이를 대체하지 않습니다. 조직은 현재의 프로세스를 활용하고 프레임워크를 이용하여 사이버보안 위험 관리를 강화하고 산업 관행에 맞춰 자신의 프로그램과 비교할 수 있는 기회를 가집니다. 또는 기존의 사이버보안 프로그램이 없는 조직은 프레임워크를 참조하여 새로운 프로그램을 수립할 수 있습니다.

프레임워크는 핵심 인프라와 관련된 사이버보안 위험 관리를 개선하기 위해 개발되었지만, 경제나 사회의 어떤 분야의 조직에서도 사용될 수 있습니다. 이는 기업, 정부 기관, 비영리 조직의 목표나 크기에 관계없이 유용하도록 설계되었습니다. 또한 제공하는 표준, 지침 및 관행의 공통 분류 체계는 특정 국가에 국한되지 않습니다. 미국 외부의 조직들도 자체 사이버보안 노력을 강화하기 위해 프레임워크를 사용할 수 있으며, 프레임워크는 핵심 인프라 사이버보안에 대한 국제적 공통 언어를 개발하는 데 기여할 수 있습니다.

1.1 프레임워크의 개요

프레임워크는 사이버보안 위험을 관리하기 위한 위험 기반 접근법으로, 프레임워크 코어(Core), 프레임워크 구현 단계(Implementation Tiers), 그리고 프레임워크 프로파일(Profiles)의 세 부분으로 구성됩니다. 각 프레임워크 구성 요소는 사업/임무 동기와 사이버보안 활동 간의 연결을 강화합니다. 이러한 구성 요소들은 아래에 설명하였습니다.

- 프레임워크 코어(Core)는 모든 핵심 인프라 부문에 걸쳐 공통적인 사이버보안 활동, 목표 결과 및 적용 가능한 참조들로 구성된 세트입니다. 코어는 산업 표준, 지침 및 관행을 전사적으로, 관리/감독 수준에서 구현/운영 수준까지 사이버보안 활동 및 결과를 소통할 수 있도록 제시합니다. 프레임워크 코어는 동시에 지속적인 다섯 가지 기능—식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)—으로 구성됩니다. 이 기능들을 함께 고려할 때, 조직의 사이버보안 위험 관리의 생명주기에 대한 고차원적이고 전략적인 관점을 제공합니다. 그 다음 프레임워크 코어는 각 기능에 대해 개별적인 결과인 주요 범주와 하위 범주를 식별하고, 각 하위 범주에 대해 기존 표준, 지침, 그리고 관행 등의 예시 참조 자료를 매칭합니다.

- 프레임워크 구현 단계("Tiers")는 조직이 사이버보안 위험을 어떻게 인식하고 그 위험을 관리하기 위해 어떤 과정을 갖추고 있는지에 대한 맥락을 제공합니다. 단계(Tiers)는 조직의 사이버보안 위험 관리 관행이 프레임워크에서 정의한 특성들(예: 위험 및 위협 인식, 반복 가능, 적용 가능 등)을 어느 정도로 나타내는지 설명합니다. 단계(Tiers)는 부분(Partial, 1 단계)부터 적용(Adaptive, 4 단계)에 이르기까지 조직의 실행을 범위 내에서 특성화 합니다. 이러한 단계(Tiers)들은 비공식적이고 수동적인 대응에서부터 민첩하고 위험에 기반한 선제적인 접근으로의 진전을 반영합니다. 단계(Tiers) 선택 과정에서 조직은 자체 위험 관리 관행, 위협 환경, 법적 및 규제 요구사항, 사업/임무 목표, 조직적 제약 사항들을 고려해야 합니다.

- 프레임워크 프로파일("Profile")은 조직이 사업 요구에 기반하여 프레임워크 범주 및 하위 범주에서 사용하기로 선택한 결과를 나타냅니다. 프로파일(Profile)은 특정 구현 시나리오에서 프레임워크 코어에 표준, 지침, 및 수행을 일치시킨 것입니다. 프로파일(Profile)은 "현재" 프로파일("있는 그대로" 상태)과 "목표" 프로파일("되고자 하는" 상태)을 비교하여 사이버보안 상태를 개선할 기회를 식별하는데 사용됩니다. 프로파일(Profile)을 개발하기 위해서 조직은 모든 범주와 하위 범주를 검토하고, 사업/임무 동기와 위험 평가에 기반하여 가장 중요한 것을 결정할 수 있으며, 조직의 위험을 다루기 위해 필요한 경우 범주 및 하위 범주를 추가할 수 있습니다. 현재 프로파일은 경제성 및 혁신을 포함한 기타 사업 요구사항을 고려하여 목표 프로파일을 향한 우선순위 설정과

진행 상황 측정을 지원하는 데 사용됩니다. 또한, 프로파일(Profile)은 자체 평가를 수행하고 조직 내부 또는 조직 간에 의사소통을 하는 데 사용됩니다.

1.2 사이버보안 프레임워크과 위험 관리

위험 관리는 위험을 식별, 평가, 대응하는 지속적인 과정입니다. 위험을 관리하기 위해서 조직은 사건이 발생할 가능성과 그로 인한 잠재적 영향을 이해해야 합니다. 이 정보를 바탕으로, 조직은 그들의 목표를 달성하기 위해 수용 가능한 위험 수준을 결정할 수 있으며, 이를 위험 허용치로 표현할 수 있습니다. 위험 허용치를 이해함으로써, 조직은 사이버보안 활동을 우선 순위에 따라 조정할 수 있으며, 이를 통해 사이버보안에 대한 비용에 대해 정보에 근거한 결정을 내릴 수 있습니다.

위험 관리 프로그램의 실행은 조직이 사이버보안 프로그램에 대한 정량화된 조정을 할 수 있는 능력을 제공합니다. 조직은 중요 서비스 제공에 미칠 잠재적 영향에 따라 위험을 완화하거나, 이전하거나, 피하거나, 수용하는 등 다양한 방법으로 위험을 처리할 수 있습니다. 프레임워크는 조직이 사이버보안과 관련된 결정을 정보에 근거하여 우선순위를 정하고 조정할 수 있도록 위험 관리 프로세스를 사용합니다. 이는 조직이 사이버보안 활동의 목표 상태를 선택하고 반복적인 위험 평가 및 비즈니스 동기의 검증을 지원하여, 원하는 결과를 반영하도록 도와줍니다. 따라서 프레임워크는 조직이 IT 및 ICS 환경의 사이버보안 위험 관리를 동적으로 선택하고 직접적으로 개선할 수 있는 능력을 제공합니다.

프레임워크는 광범위한 사이버보안 위험 관리 프로세스에 사용될 수 있도록 유연하고 위험 기반(선제적인)의 구현을 제공합니다. 사이버보안 위험 관리 프로세스의 예로는 국제표준화기구(International Organization for Standardization, ISO) 31000:2009[6], ISO/국제전기기술위원회(International Electrotechnical Commission, IEC) 27005:2011[7], NIST(국립표준기술연구소) 특별출판물(SP) 800-39[8], 전기 부문 사이버보안 위험 관리 프로세스(Risk Management Process, RMP) 지침[9] 등이 있습니다.

[6] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[9] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

1.3 문서 개요

이 문서의 나머지 부분은 다음과 같은 구역과 부록으로 구성되어 있습니다:

- 구역 2 는 프레임워크 구성요소를 설명합니다: 프레임워크 코어, 계층(Tiers), 프로필(Profiles)에 대해 설명합니다.
- 구역 3 은 프레임워크 사용 예를 제시합니다.
- 구역 4 는 자체 평가 및 사이버보안 측정을 통한 시연 방법을 설명합니다.
- 부록 A 는 표 형식의 프레임워크 코어를 제시합니다: 기능(Functions), 범주(Categories), 하위 범주(Subcategories), 그리고 참조 정보(Informative References)를 나타냅니다.
- 부록 B 는 선택된 용어에 대한 용어집을 포함합니다.
- 부록 C 는 이 문서에서 사용되는 약어 목록을 나열합니다.

2.0 프레임워크 기초

프레임워크는 내부 및 외부 이해관계자에게 사이버보안 위험을 이해, 관리 및 표현하는 공통 언어를 제공합니다. 이는 사이버보안 위험을 줄이기 위한 행동을 식별하고 우선 순위를 정하는 데 도움이 될 수 있으며, 정책, 사업 및 기술 접근 방식을 위험 관리와 일치시키는 도구로 사용될 수 있습니다. 이 프레임워크는 전체 조직의 사이버보안 위험을 관리하거나 조직 내 중요 서비스 제공에 중점을 둘 수 있습니다. 부문 조정 구조, 협회 및 조직을 포함한 다양한 유형의 기관에서 프레임워크를 공통 프로필 생성을 포함한 다양한 목적으로 사용할 수 있습니다.

2.1 프레임워크 코어

프레임워크 코어는 특정 사이버보안 결과를 달성하기 위한 일련의 활동을 제공하며, 그 결과를 달성하기 위한 지침 예시를 참조합니다. 코어는 수행해야 할 체크리스트가 아닙니다. 이는 이해관계자들이 사이버보안 위험 관리에 도움이 된다고 식별한 주요 사이버보안 결과를 제시합니다. 코어는 네 가지 요소로 구성됩니다: 기능(Functions), 범주(Categories), 하위 범주(Subcategories), 그리고 참조 정보(Informative References), 이는 **그림 1** 에 나타나 있습니다:

그림 1: 프레임워크 코어 구조

프레임워크 코어 요소들은 다음과 같이 함께 작동합니다:

- **기능(Functions)**은 가장 높은 수준에서 기본적인 사이버보안 활동을 조직합니다. 이러한 기능에는 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)가 있습니다. 이 기능들은 정보를 조직화하고, 위험 관리 결정을 가능하게 하며, 위협에 대응하고, 이전 활동을 바탕으로 개선함으로써 조직이 사이버보안 위험 관리를 표현하는 데 도움을 줍니다. 또한 기능들은 사건 관리에 대한 기존 방법론과도 일치하며, 사이버보안에 대한 투자의 영향을 보여주는 데 도움을 줍니다. 예를 들어, 계획 및 연습에

대한 투자는 시기적절한 대응 및 복구 조치를 지원하여 서비스 제공에 미치는 영향을 감소시킵니다.

- **범주(Categories)**는 기능(Function)을 프로그램 요구와 특정 활동과 밀접하게 연결된 사이버보안 결과 그룹으로 세분화한 것입니다. 범주의 예로는 "자산 관리(Asset Management)", "신원 관리 및 접근 제어(Identity Management and Access Control)", "탐지 프로세스(Detection Processes)" 등이 있습니다.
- **하위 범주(Subcategories)**는 범주를 기술적 및 관리 활동의 구체적인 결과로 더 세분화합니다. 이들은 모든 결과를 포괄하는 것은 아니지만, 각 범주에서의 목표 달성을 지원하는 일련의 결과들을 제공합니다. 하위 범주의 예로는 "외부 정보 시스템이 목록화됨", "정지 상태의 데이터가 보호됨", "탐지 시스템의 알림이 조사됨" 등이 있습니다.
- **참조 정보(Informative References)**는 각 하위 범주와 관련된 목표를 달성하기 위한 방법을 설명하는 핵심 인프라 부문에서 공통적인 표준, 지침 및 관행의 구체적인 섹션들입니다. 프레임워크 코어에 제시된 참조 정보는 예시이며, 전체를 포괄하는 것은 아닙니다. 이는 프레임워크 개발 과정 중 가장 자주 참조된 부문 간 지침을 기반으로 하고 있습니다.

다음은 다섯 가지 프레임워크 코어 기능에 대한 정의입니다. 이 기능들은 순서대로 수행해서 정해진 바람직한 결과를 이끄는 것을 목적으로 하는 것이 아닙니다. 오히려 이 기능들은 동시에 지속적으로 수행되어야 하며, 사이버보안 위험의 역동성을 다루는 문화를 형성해야 합니다. 완전한 프레임워크 코어 목록은 **부록 A** 를 참조하십시오.

- **식별(Identify)** - 시스템, 사람, 자산, 데이터 및 가능성에 대한 사이버보안 위험을 관리하는 조직적 이해를 개발합니다.
  식별 기능의 활동은 프레임워크를 효과적으로 사용하기 위한 기초입니다. 비즈니스 맥락, 중요 기능을 지원하는 자원, 관련된 사이버보안 위험을 이해함으로써, 조직은 위험 관리 전략과 비즈니스 요구에 일관되게 자신의 노력을 집중하고 우선순위를 정할 수 있습니다. 이 기능 내의 결과 범주 예시에는 자산 관리(Asset Management), 비즈니스 환경(Business Environment), 거버넌스(Governance), 위험 평가(Risk Assessment), 위험 관리 전략(Risk Management Strategy) 등이 있습니다.
- **보호(Protect)** - 중요 서비스의 제공을 보장하기 위한 적절한 보호 조치를 개발하고 구현합니다.
  보호 기능은 잠재적인 사이버보안 사건의 영향을 제한할 수 있는 능력을 지원합니다. 이 기능 내의 결과 범주 예시에는 신원 관리 및 접근 제어(Identity Management and Access Control), 인식 및 교육(Awareness and Training), 데이터 보안(Data Security), 정보 보호

프로세스 및 절차(Information Protection Processes and Procedures), 유지 관리(Maintenance), 보호 기술(Protective Technology) 등이 있습니다.

- **탐지(Detect)** - 사이버보안 사건의 발생을 식별하기 위한 적절한 활동을 개발하고 구현합니다.
  탐지 기능은 사이버보안 사건을 신속하게 발견할 수 있게 합니다. 이 기능 내의 결과 범주 예시에는 이상 현상 및 사건(Anomalies and Events), 보안 지속 모니터링(Security Continuous Monitoring), 탐지 프로세스(Detection Processes) 등이 있습니다.
- **대응(Respond)** - 탐지된 사이버보안 사건에 대응하기 위한 적절한 활동을 개발하고 구현합니다.
  대응 기능은 잠재적인 사이버보안 사건의 영향을 제한하는 능력을 지원합니다. 이 기능 내의 결과 범주 예시에는 대응 계획(Response Planning), 의사소통(Communications), 분석(Analysis), 완화(Mitigation), 개선(Improvements) 등이 있습니다.
- **복구(Recover)** - 복원력을 유지하기 위한 계획과 사이버보안 사건으로 인해 손상된 모든 기능이나 서비스를 복구하기 위한 적절한 활동을 개발하고 구현합니다.
  복구 기능은 사이버보안 사건으로부터의 영향을 줄이기 위해 정상 운영으로의 신속한 복구를 지원합니다. 이 기능 내의 결과 범주 예시에는 복구 계획(Recovery Planning), 개선(Improvements), 의사소통(Communications) 등이 있습니다.

2.2 프레임워크 구현 단계

프레임워크 구현 단계("Tier")는 조직이 사이버보안 위험을 어떻게 바라보고 그 위험을 관리하기 위한 프로세스가 어떻게 마련되어 있는지에 대한 맥락을 제공합니다. 불완전(Partial, 1 단계)에서부터 적합(Adaptive, 4 단계)에 이르기까지, 단계들은 사이버보안 위험 관리 수행의 엄밀함과 정교함이 증가하는 정도를 설명합니다. 이들은 사이버보안 위험 관리가 사업의 요구사항을 어느 정도까지 반영하고, 조직의 전체적인 위험 관리 관행에 얼마나 통합되어 있는지를 결정하는 데 도움이 됩니다. 위험 관리 고려사항에는 사이버보안의 여러 측면이 포함되며, 이에는 개인정보 보호 및 시민의 자유에 대한 고려사항이 조직의 사이버보안 위험 관리 및 잠재적인 위험 대응에 얼마나 통합되어 있는지도 포함됩니다.

단계 선택 과정에서는 조직의 현재 위험 관리 수행 수준, 위협 환경, 법적 및 규제 요구사항, 정보 공유 관행, 사업/임무 목표, 공급망 사이버보안 요구사항, 조직적 제약사항 등을 고려합니다. 조직은 원하는 단계를 결정해야 하며, 선택된 단계가 조직 목표에 부합하고 구현이 가능하며 조직에 수용 가능한 수준으로 중요 자산과 자원에 대한 사이버보안 위험을 감소시키는지 확인해야 합니다. 조직은 연방 정부 부서 및 기관, 정보 공유 및 분석 센터(ISACs), 정보 공유 및 분석 조직(ISAOs), 기존 성숙도 모델 또는 기타 소스로부터 얻은 외부 지침을 활용하여 원하는 단계를 결정하는 데 도움을 받을 수 있습니다.

1 단계(불완전)로 식별된 조직들은 2 단계 이상으로 이동하는 것을 고려하도록 권장되지만, 단계는 성숙도 수준을 나타내는 것이 아닙니다. 단계는 조직이 사이버보안 위험을 어떻게 관리할 것인지, 그리고 조직의 어떤 부문이 더 높은 우선순위를 가지고 추가 자원을 받을 수 있는지에 대한 조직적 의사결정을 지원하기 위한 것입니다. 비용-편익 분석이 사이버보안 위험의 현실적이고 비용 효과적인 감소를 나타내는 경우, 더 높은 단계로의 진전이 권장됩니다.

프레임워크의 성공적인 구현은 단계 결정이 아닌, 조직의 목표 프로파일(들)에 기술된 결과를 달성하는 데 기반합니다. 그럼에도 불구하고, 단계 선택 및 지정은 자연스럽게 프레임워크 프로파일에 영향을 미칩니다. 비즈니스/프로세스 수준 관리자들의 단계 추천이 고위 경영진에 의해 승인되면, 조직 내에서 사이버보안 위험이 어떻게 관리될 것인지에 대한 전반적인 기조를 설정하는 데 도움이 되며, 그 후에는 목표 프로파일 내의 우선순위 설정 및 격차 해소에 대한 진전 평가에 영향을 미쳐야 합니다.

각 단계에 대한 정의는 아래와 같습니다:

단계 1: 불완전

- **위험 관리 프로세스** - 조직의 사이버보안 위험 관리 수행 능력은 정형화되지 않았으며, 위험은 임시적이고 수동적인 방식으로 관리됩니다. 우선 순위의 사이버보안 활동이 조직의 위험 목표, 위협 환경 또는 사업/임무 요구사항을 직접적으로 반영하지 않을 수 있습니다.
- **통합된 위험 관리 프로그램 -** 조직 수준에서 사이버보안 위험에 대한 인식이 제한적입니다. 조직은 다양한 경험 또는 외부 소스에서 얻은 정보에 따라 비 정기적이고 사례별로 사이버보안 위험 관리를 수행합니다. 조직 내에서 사이버보안 정보를 공유할 수 있는 프로세스가 없을 수도 있습니다.
- **외부 참여 -** 조직은 자신의 의존성 또는 의존 대상과 관련하여 더 큰 생태계 내에서의 역할을 이해하지 못합니다. 조직은 다른 이해관계자들(예: 구매자, 공급자, 의존성, 의존 대상, ISAOs, 연구자, 정부 등)과 협력하거나 정보(예: 위협 인텔리전스, 최선의 관행, 기술 등)를 받지 않으며, 정보를 공유하지도 않습니다. 조직은 일반적으로 제공하고 사용하는 제품 및 서비스의 사이버 공급망 위험에 대해 인식하지 못합니다.

단계 2: 위험 인식

- **위험 관리 프로세스** - 위험 관리 수행은 관리진에 의해 승인되었지만, 조직 전체의 정책으로 확립되지 않았을 수 있습니다. 우선 순위의 사이버보안 활동 및 방어를 위한 조치들은 조직의 위험 목표, 위협 환경 또는 사업/임무 요구사항을 직접적으로 반영합니다.
- **통합 위험 관리 프로그램** - 조직 수준에서 사이버보안 위험에 대한 인식은 있지만, 조직 전체의 사이버보안 위험 관리 접근 방식은 확립되지 않았습니다. 사이버보안 정보는

비공식적으로 조직 내에서 공유됩니다. 조직의 목표와 프로그램에서 사이버보안을 고려하는 것은 조직의 일부 수준에서는 일어나지만 모든 수준에서는 그렇지 않습니다. 조직 및 외부 자산에 대한 사이버 위험 평가는 수행되지만, 일반적으로 반복 가능하거나 주기적인 것은 아닙니다.

- **외부 참여** - 일반적으로 조직은 자신의 의존성 또는 의존 대상과 관련하여 더 큰 생태계 내에서의 자신의 역할을 이해하지만, 둘 다를 동시에 이해하는 것은 아닙니다. 조직은 다른 이해관계자들과 협력하며 일부 정보를 받고 자체적으로 일부 정보를 생성하지만, 다른 이들과 정보를 공유하지 않을 수 있습니다. 또한, 조직은 제공하고 사용하는 제품 및 서비스와 관련된 사이버 공급망 위험을 인식하지만, 그러한 위험에 대해 일관되거나 공식적으로 대응하지는 않습니다.

단계 3: 재현 가능

- **위험 관리 프로세스** - 조직의 위험 관리 업무는 공식적으로 승인되어 정책으로 표현됩니다. 조직의 사이버보안 업무는 사업/임무 요구사항의 변화와 변화하는 위협 및 기술 환경에 대한 위험 관리 프로세스의 적용을 기반으로 정기적으로 업데이트됩니다.
- **통합 위험 관리 프로그램** - 전반적인 사이버보안 위험을 관리하기 위한 조직이 있습니다. 위험에 기반한 정책, 프로세스, 및 절차는 정의되어 의도대로 구현되고 검토됩니다. 위험의 변화에 효과적으로 대응하기 위한 일관된 방법이 마련되어 있습니다. 직원들은 자신의 역할과 책임을 수행하는 데 필요한 지식과 기술을 갖추고 있습니다. 조직은 조직 자산의 사이버보안 위험을 일관되고 정확하게 모니터링합니다. 사이버보안 및 비사이버보안의 업무를 수행하는 고위 경영진은 정기적으로 사이버보안 위험에 대해 소통합니다. 고위 경영진은 조직의 모든 운영 라인에서 사이버보안을 고려하도록 합니다.
- **외부 참여** - 조직은 더 큰 생태계에서 자신의 역할, 의존성 및 의존 대상을 이해하며, 커뮤니티에 위험에 대한 보다 넓은 이해에 기여할 수 있습니다. 조직은 다른 이해관계자들과 정기적으로 협력하며, 내부에서 생성된 정보를 보완하는 정보를 받고 다른 이해관계자들과 정보를 공유합니다. 조직은 자신이 제공하고 사용하는 제품 및 서비스와 관련된 사이버 공급망 위험을 인식하고 있습니다. 또한, 일반적으로 이러한 위험에 대해 공식적으로 대응하며, 기준 요구사항을 전달하는 서면 계약, 거버넌스 구조(예: 위험 위원회), 정책 구현 및 모니터링과 같은 메커니즘을 가집니다.

단계 4: 적합

- **위험 관리 프로세스** - 조직은 과거 및 현재의 사이버보안 활동을 바탕으로 사이버보안 업무를 조정합니다. 이는 학습한 교훈과 예측 지표를 포함합니다. 고급 사이버보안

기술과 관행을 통합한 지속적인 개선 과정을 통해, 조직은 변화하는 위협 및 기술 환경에 적극적으로 적응하고 발전하는 복잡한 위협에 신속하고 효과적으로 대응합니다.

- **통합 위험 관리 프로그램** - 조직 전체의 사이버보안 위험 관리 접근 방식이 있으며, 이는 잠재적 사이버보안 사건을 다루기 위해 위험에 기반한 정책, 프로세스 및 절차를 사용합니다. 사이버보안 위험과 조직 목표 간의 관계가 명확히 이해되며, 결정을 내릴 때 고려됩니다. 고위 경영진은 사이버보안 위험을 재무 위험 및 기타 조직적 위험과 동일한 맥락에서 모니터링합니다. 조직 예산은 현재 및 예측된 위험 환경 및 위험 허용도에 대한 이해를 바탕으로 합니다. 사업 부문은 경영진의 비전을 구현하고 조직의 위험 허용도 맥락에서 시스템 수준의 위험을 분석합니다. 사이버보안 위험 관리는 조직 문화의 일부이며, 이전 활동에 대한 인식과 시스템 및 네트워크에서의 지속적인 활동에 대한 인식에서 진화합니다. 조직은 사업/임무 목표의 변화에 따라 위험 접근 방식과 소통 방식을 신속하고 효율적으로 조정할 수 있습니다.
- **외부 참여** - 조직은 더 큰 생태계에서 자신의 역할, 의존성 및 의존 대상을 이해하고 커뮤니티에 위험에 대한 보다 넓은 이해에 기여합니다. 위협 및 기술 환경이 변화함에 따라 자신의 위험에 대한 지속적인 분석을 통해 우선 순위가 높은 정보를 수신, 생성 및 검토합니다. 조직은 그 정보를 내부적으로 및 외부 협력자들과 공유합니다. 조직은 실시간 또는 거의 실시간 정보를 사용하여 제공하는 제품 및 서비스와 사용하는 제품 및 서비스와 관련된 사이버 공급망 위험을 이해하고 일관되게 대응합니다. 또한, 조직은 형식적(예: 협약) 및 비형식적 메커니즘을 사용하여 강력한 공급망 관계를 개발하고 유지하기 위해 적극적으로 소통합니다.

2.3 프레임워크 프로파일

프레임워크 프로파일("Profile")은 조직의 사업 요구사항, 위험 허용도 및 자원과 기능, 범주, 하위 범주를 일치시키는 것입니다. 프로파일을 통해 조직은 조직 및 부문 목표에 잘 부합하고, 법적/규제 요구사항 및 업계 최선의 관행을 고려하며, 사이버보안 위험 감소를 위해 위험 관리 우선순위를 반영하는 로드맵을 설정할 수 있습니다. 많은 조직이 복잡성을 가지고 있기 때문에, 특정 구성 요소에 맞추고 각각의 개별적인 요구사항을 인식하여 여러 프로파일을 가질 수도 있습니다. 프레임워크 프로파일은 특정 사이버보안 활동의 현재 상태 또는 원하는 목표 상태를 기술하는 데 사용될 수 있습니다. 현재 프로파일은 달성중인 사이버보안 결과를 나타냅니다. 목표 프로파일은 원하는 사이버보안 위험 관리 목표를 달성하기 위해 필요한 결과를 나타냅니다. 프로파일은 사업/임무 요구사항을 지원하고 조직 내부 및 조직 간 위험 소통에 도움을 줍니다. 이 프레임워크는 프로파일 템플릿을 지정하지 않아 구현 시 유연성을 제공합니다.

프로파일들의 비교(예: 현재 프로파일과 목표 프로파일)는 사이버보안 위험 관리 목표를 충족시키기 위해 해결해야 할 격차를 드러낼 수 있습니다. 주어진 범주 또는 하위 범주를 충족하기 위해 이러한 격차를 해결하기 위한 행동 계획은 위에서 설명한 로드맵에 기여할 수 있습니다. 격차 완화의 우선 순위는 조직의 사업 요구와 위험 관리 프로세스에 의해 결정됩니다. 이 위험 기반 접근 방식은 조직이 경제적이고 우선 순위에 따라 사이버보안 목표를 달성하기 위해 필요한 자원(예: 인력, 자금)을 평가할 수 있게 합니다. 더욱이, 프레임워크는 위험 기반 접근 방식으로, 주어진 하위 범주의 적용 및 충족은 프로파일의 범위에 따라 달라집니다.

2.4 프레임워크 구현 조정

그림 2는 조직 내 다음 수준에서 정보와 의사결정의 일반적인 흐름을 설명합니다:

- 경영진
- 사업/프로세스
- 구현/운영

경영진은 사업/프로세스 수준에 임무 우선순위, 사용 가능한 자원, 전체적인 위험 허용도를 전달합니다. 사업/프로세스 수준은 이 정보를 위험 관리 프로세스에 입력으로 사용하고, 구현/운영 수준과 협력하여 사업 요구사항을 전달하고 프로파일을 생성합니다. 구현/운영 수준은 프로파일 구현 진행 상황을 사업/프로세스 수준에 전달합니다. 사업/프로세스 수준은 이 정보를 사용하여 영향 평가를 수행합니다. 사업/프로세스 수준 관리는 그 영향 평가의 결과를 경영진에 보고하여 조직의 전체적인 위험 관리 프로세스에 정보를 제공하고, 사업 영향에 대한 인식을 위해 구현/운영 수준에 보고합니다.

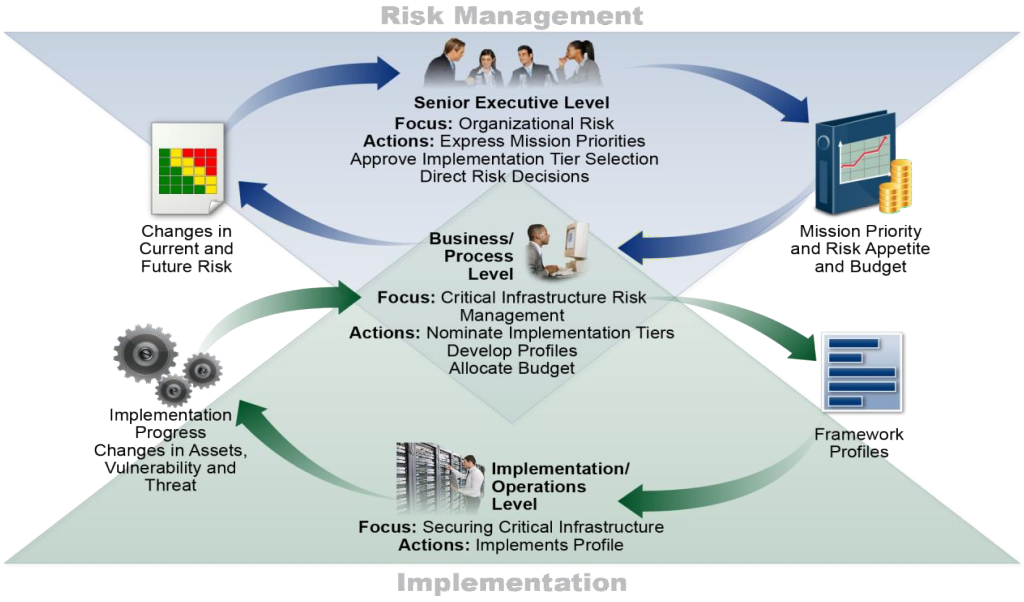

그림 2: 조직 내의 개념적 정보 및 의사결정 흐름

3.0 프레임워크 사용 방법

조직은 프레임워크를 사이버보안 위험을 식별, 평가, 관리하는 체계적인 프로세스의 핵심 부분으로 사용할 수 있습니다. 프레임워크는 기존 프로세스를 대체하기 위해 설계된 것이 아니며, 조직은 현재 프로세스를 사용하고 이를 프레임워크에 중첩시켜 현재 사이버보안 위험 접근 방식에서의 격차를 파악하고 개선을 위한 로드맵을 개발할 수 있습니다. 프레임워크를 사이버보안 위험 관리 도구로 사용함으로써, 조직은 중요한 서비스 제공에 가장 중요한 활동을 결정하고 투자의 영향을 극대화하기 위해 지출을 우선 순위에 따라 정할 수 있습니다.

프레임워크는 기존의 사업 및 사이버보안 운영을 보완하기 위해 설계되었습니다. 새로운 사이버보안 프로그램의 기초로 사용되거나 기존 프로그램을 개선하기 위한 메커니즘으로 활용될 수 있습니다. 프레임워크는 비즈니스 파트너 및 고객에게 사이버보안 요구사항을 표현하는 수단을 제공하고, 조직의 사이버보안 관행에서의 격차를 식별하는 데 도움이 될 수 있습니다. 또한, 사이버보안 프로그램의 맥락에서 일반적인 개인정보 보호 및 시민의 자유에 관한 고려사항과 프로세스를 제공합니다.

프레임워크는 계획, 설계, 구축/구매, 배포, 운영 및 폐기의 생명주기 단계 전반에 걸쳐 적용될 수 있습니다. 계획 단계는 어떠한 시스템의 순환주기를 시작하며, 이후 모든 것을 위한 기초를 마련합니다. 최상위 사이버보안 고려사항은 가능한 한 명확하게 선언되고 설명되어야 합니다. 계획은 이러한 고려사항과 요구사항이 생명주기의 나머지 기간 동안 진화할 가능성을 인식해야 합니다. 설계 단계에서는 사이버보안 요구사항을 보다 큰 다분야 시스템 엔지니어링 프로세스의 일부로 고려해야 합니다.[10] 설계 단계의 주요 이정표는 시스템 사이버보안 사양이 프레임워크 프로파일에 포착된 조직의 필요와 위험 성향과 일치하는지를 검증하는 것입니다. 목표 프로파일에서 우선적으로 목표로 하는 사이버보안 결과는 a) 시스템을 구축하는 단계와 b) 시스템을 구매하거나 아웃소싱 하는 단계에서 통합되어야 합니다. 동일한 목표 프로파일은 시스템을 배포할 때 모든 기능이 구현되었는지를 평가하기 위한 시스템 사이버보안 기술 목록으로 사용됩니다. 프레임워크를 사용하여 결정된 사이버보안 결과는 시스템의 지속적인 운영을 위한 기초로 사용되어야 합니다. 이에는 간헐적인 재평가와 현재 프로파일에 결과를 기록하여 사이버보안 요구사항이 여전히 충족되는지를 확인하는 것이 포함됩니다. 일반적으로 시스템 간에 복잡한 의존성(예: 상쇄 및 공통 컨트롤)이 있기 때문에 관련 시스템의 목표 프로파일에 문서화된 결과는 시스템이 폐기됨에 따라 신중하게 고려되어야 합니다.

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

다음 섹션에서는 조직이 프레임워크를 사용할 수 있는 다양한 방법을 제시합니다.

3.1 사이버보안 업무의 기본 검토

프레임워크는 조직의 현재 사이버보안 활동을 프레임워크 코어에 주요 활동과 비교하는 데 사용될 수 있습니다. 현재 프로파일을 생성함으로써 조직은 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)와 같은 다섯 가지 고위급 기능에 맞춰 코어의 범주와 하위 범주에서 기술된 결과를 얼마나 달성하고 있는지 검토할 수 있습니다. 조직은 이미 원하는 결과를 달성하여 알려진 위험에 상응하는 사이버보안 관리를 하고 있을 수 있습니다. 반대로 조직은 개선할 기회가 있거나 필요할 수 있음을 발견할 수도 있습니다. 조직은 이 정보를 사용하여 기존의 사이버보안 업무를 강화하고 사이버보안 위험을 줄이기 위한 행동 계획을 개발할 수 있습니다. 또한 조직은 특정 결과를 달성하기 위해 과도한 투자를 하고 있을 수 있습니다. 조직은 이 정보를 사용하여 자원을 다시 우선순위화 할 수 있습니다.

이 다섯 가지 고위급 기능은 위험 관리 프로세스를 대체하지는 않지만, 고위 경영진 및 기타 관계자들이 사이버보안 위험의 기본 개념을 간결하게 정리하여 식별된 위험이 어떻게 관리되는지, 그리고 그들의 조직이 기존의 사이버보안 표준, 지침 및 업무에 대비하여 높은 수준에서 어떻게 비교되는지를 평가할 수 있는 방법을 제공합니다. 프레임워크는 또한 조직이 기본적인 질문에 답하는 데 도움이 될 수 있습니다. 예를 들어, "우리는 어떻게 하고 있나요?" 그런 다음 필요하다고 판단되는 경우와 장소에서 사이버보안 업무를 보다 정보에 근거하여 강화할 수 있습니다.

3.2 사이버보안 프로그램의 수립 또는 개선

다음 단계들은 조직이 프레임워크를 사용하여 새로운 사이버보안 프로그램을 만들거나 기존 프로그램을 개선하는 방법을 보여줍니다. 이러한 단계들은 지속적으로 사이버보안을 개선하기 위해 필요에 따라 반복되어야 합니다.

단계 1: 우선 순위 설정 및 범위 정의. 조직은 사업/임무 목표와 최상위 수준의 조직 우선 순위를 식별합니다. 이 정보를 바탕으로 조직은 사이버보안 구현과 관련하여 전략적 결정을 내리고 선택된 사업 라인이나 프로세스를 지원하는 시스템 및 자산의 범위를 결정합니다. 프레임워크는 조직 내 다른 사업 라인 또는 프로세스에 맞게 조정될 수 있으며, 이들은 서로 다른 비즈니스 요구와 관련된 위험 허용도를 가질 수 있습니다. 위험 허용도는 목표 구현 단계에서 반영될 수 있습니다.

단계 2: 방향 설정. 사업 라인 또는 프로세스에 대한 사이버보안 프로그램의 범위가 결정되면, 조직은 관련 시스템과 자산, 규제 요구사항 및 전반적인 위험 접근 방식을 식별합니다. 그 후 조직은 해당 시스템과 자산에 적용 가능한 위협과 취약점을 식별하기 위해 다양한 정보원을 참조합니다.

단계 3: 현재 프로파일 생성. 조직은 프레임워크 코어의 범주 및 하위 범주 결과 중 현재 달성하고 있는 것들을 표시함으로써 현재 프로파일을 개발합니다. 결과가 부분적으로 달성된 경우, 이 사실을 기록하는 것은 기초 정보를 제공함으로써 후속 단계를 지원하는 데 도움이 됩니다.

단계 4: 위험 평가 수행. 이 평가는 조직의 전체 위험 관리 프로세스나 이전의 위험 평가 활동에 의해 안내될 수 있습니다. 조직은 운영 환경을 분석하여 사이버보안 사건의 가능성과 그 사건이 조직에 미칠 수 있는 영향을 파악합니다. 조직이 신흥 위험을 식별하고 내부 및 외부 소스로부터 사이버 위협 정보를 활용하여 사이버보안 사건의 가능성 및 영향에 대한 더 나은 이해를 갖는 것이 중요합니다.

단계 5: 목표 프로파일 생성. 조직은 프레임워크 범주 및 하위 범주 평가에 중점을 둔 목표 프로파일을 생성합니다. 이는 조직이 원하는 사이버보안 결과를 기술합니다. 조직은 고유한 조직적 위험을 고려하기 위해 자체적인 추가 범주와 하위 범주를 개발할 수도 있습니다. 조직은 목표 프로파일을 생성할 때 독립 부서, 고객, 비즈니스 파트너와 같은 외부 이해관계자의 영향과 요구사항을 고려할 수도 있습니다. 목표 프로파일은 목표 구현 단계 내의 적절한 기준을 반영해야 합니다.

단계 6: 격차 결정, 분석 및 우선 순위 지정. 조직은 현재 프로파일과 목표 프로파일을 비교하여 격차를 결정합니다. 이어서, 목표 프로파일의 결과를 달성하기 위해 임무 동기, 비용과 이익, 그리고 위험을 반영하는 우선 순위가 있는 행동 계획을 만들어 격차를 해소합니다. 그 후, 조직은 격차를 해결하는 데 필요한 자원, 포함하여 자금과 인력을 결정합니다. 이러한 방식으로 프로파일을 사용함으로써 조직은 사이버보안 활동에 대해 정보에 기반한 결정을 내리고, 위험 관리를 지원하며, 경제적이고 목표 지향적인 개선을 수행할 수 있습니다.

단계 7: 행동 계획 시행. 조직은 이전 단계에서 식별된 격차(있는 경우)를 해결하기 위해 취할 조치를 결정한 다음, 목표 프로파일을 달성하기 위해 현재의 사이버보안 업무를 조정합니다. 추가적인 지침을 위해, 프레임워크는 범주와 하위 범주에 대한 예시 적인 참조 정보를 제시하지만, 조직은 부문별로 구체화된 표준, 지침 및 관행을 포함하여 자신의 필요에 가장 적합한 것을 결정해야 합니다.

조직은 필요에 따라 이러한 단계들을 반복하여 지속적으로 자신의 사이버보안을 평가하고 개선합니다. 예를 들어, 조직은 방향 설정 단계를 더 자주 반복함으로써 위험 평가의 품질을 향상시킬 수 있습니다. 또한, 조직은 현재 프로파일에 대한 반복적인 업데이트를 통해 진행 상황을 모니터링하고, 이후에 현재 프로파일을 목표 프로파일과 비교할 수 있습니다. 조직은 이 프로세스를 사용하여 자신의 사이버보안 프로그램을 원하는 프레임워크 구현 단계와 일치시킬 수도 있습니다.

3.3 이해관계자들과의 사이버보안 요구사항 소통

프레임워크는 필수적인 핵심 인프라 제품 및 서비스의 제공에 책임이 있는 상호 의존적 이해관계자들 간의 요구사항을 소통하기 위한 공통 언어를 제공합니다. 예시는 다음과 같습니다:

- 조직은 외부 서비스 제공업체(예: 데이터를 보내는 클라우드 제공업체)에게 사이버보안 위험 관리 요구사항을 표현하기 위해 목표 프로파일을 사용할 수 있습니다.
- 조직은 현재 프로파일을 통해 자신의 사이버보안 상태를 결과 보고나 조달 요구사항과 비교하기 위해 사용할 수 있습니다.
- 핵심 인프라 소유주/운영자는 해당 인프라에 의존하는 외부 파트너를 식별한 후, 필요한 범주와 하위 범주를 전달하기 위해 목표 프로파일을 사용할 수 있습니다.
- 핵심 인프라 부문은 구성원들이 기초 프로파일로 사용하고 자신의 맞춤형 목표 프로파일을 구축할 수 있는 목표 프로파일을 설정할 수 있습니다.
- 조직은 핵심 인프라와 더 넓은 디지털 경제에서의 자신의 위치를 구현 단계를 사용하여 평가함으로써 이해관계자들 사이의 사이버보안 위험을 더 잘 관리할 수 있습니다.

공급망을 따라 이해관계자 간의 소통은 특히 중요합니다. 공급망은 복잡하고 전 세계적으로 분포되어 있으며, 여러 조직 수준 간의 자원 및 프로세스가 상호 연결된 세트입니다. 공급망은 제품 및 서비스의 조달로 시작하여 설계, 개발, 제조, 처리, 취급 및 최종 사용자에게 제품 및 서비스를 제공하는 단계에 이르기까지 확장됩니다. 이러한 복잡하고 상호 연결된 관계를 고려할 때, 공급망 위험 관리(SCRM)는 중요한 조직 기능입니다.[11]

사이버 공급망 위험 관리(SCRM)는 외부 당사자와 관련된 사이버보안 위험을 관리하기 위해 필요한 일련의 활동을 말합니다. 보다 구체적으로, 사이버 SCRM 은 조직이 외부 당사자에게 미치는 사이버보안 영향과 외부 당사자가 조직에 미치는 사이버보안 영향을 모두 다룹니다.

[11] Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.

사이버 SCRM 의 주요 목표는 "잠재적으로 악의적인 기능을 포함할 수 있거나, 위조되었거나, 사이버 공급망 내의 불량한 제조 및 개발 관행으로 인해 취약한 제품 및 서비스를 식별, 평가 및 완화하는 것" 입니다. 사이버 SCRM 활동에는 다음이 포함될 수 있습니다:

- 공급업체에 대한 사이버보안 요구사항 결정,
- 공식적인 계약(예: 계약)을 통한 사이버보안 요구사항 실행,
- 공급업체에게 사이버보안 요구사항이 어떻게 검증 및 검증될지에 대해 소통,
- 다양한 평가 방법론을 통해 사이버보안 요구사항이 충족되었는지 검증,
- 위 활동의 관리 및 거버넌스.

그림 3 에서 나타난 바와 같이, 사이버 SCRM 은 기술 공급업체 및 구매자 뿐만 아니라 비기술 공급업체 및 구매자도 포함하며, 여기서 기술은 정보 기술(IT), 산업 제어 시스템(ICS), 사이버-물리 시스템(CPS), 일반적으로 연결된 장치(IoT 포함)로 구성됩니다. 그림 3 은 조직을 단일 시점에서 나타냅니다. 그러나 일반적인 비즈니스 운영 과정을 통해 대부분의 조직은 다른 조직이나 최종 사용자와 관련하여 상류 공급업체 및 하류 구매자가 될 것입니다.

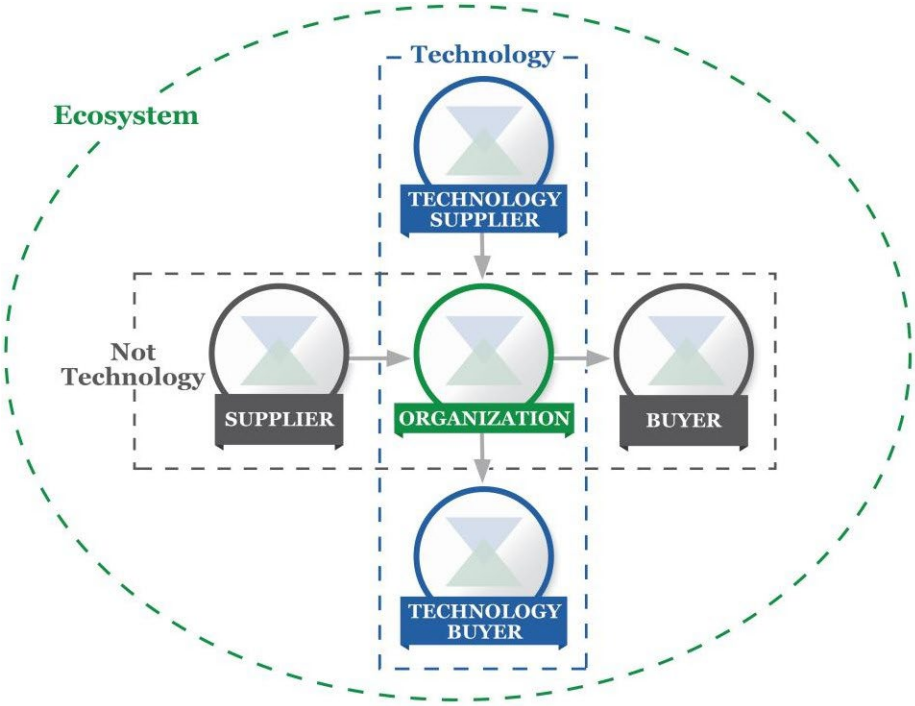

그림 3: 사이버보안 공급망 관계도

[12] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

그림 3 에서 설명된 당사자들은 조직의 사이버보안 생태계를 구성합니다. 이러한 관계는 핵심 인프라와 보다 넓은 디지털 경제에서 사이버보안 위험을 해결하는 데 있어 사이버 SCRM 의 중요한 역할을 강조합니다. 이러한 관계, 그들이 제공하는 제품 및 서비스, 그리고 그들이 제시하는 위험은 조직의 보호 및 탐지 능력 뿐만 아니라 그들의 대응 및 복구 프로토콜에 식별되고 고려되어야 합니다.

위 그림에서 "구매자(Buyer)"는 조직으로부터 특정 제품이나 서비스를 소비하는 하류의 사람들 또는 조직을 의미합니다. 이는 영리 및 비영리 조직 모두를 포함합니다. "공급업체(Supplier)"는 조직의 내부 목적(예: IT 인프라)을 위해 사용되거나 구매자에게 제공되는 제품이나 서비스에 통합되는 상류 제품 및 서비스 제공자를 포함합니다. 이러한 용어는 기술 기반 및 비 기술 기반 제품과 서비스 모두에 적용됩니다.

코어의 개별 하위 범주를 고려하든 프로파일의 종합적 고려사항을 고려하든, 프레임워크는 조직과 그 파트너들이 새로운 제품이나 서비스가 중요한 보안 결과를 달성하는 데 도움이 되는 방법을 제공합니다. 먼저 맥락에 관련된 결과(예: 개인식별정보(PII) 전송, 임무 중요 서비스 제공, 데이터 검증 서비스, 제품 또는 서비스 무결성)를 선택한 후, 조직은 그 기준에 대해 파트너를 평가할 수 있습니다. 예를 들어, 운영 기술(OT)의 비정상적 네트워크 통신을 모니터링하기 위해 시스템을 구매하는 경우, 가용성은 특히 중요한 사이버보안 목표일 수 있으며 적용 가능한 하위 범주(예: ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5)로 기술 공급업체 평가를 주도해야 합니다.

3.4 구매 결정

프레임워크 목표 프로파일이 조직의 우선 순위에 따른 사이버보안 요구사항 목록인 경우, 목표 프로파일은 제품 및 서비스 구매 결정에 대한 정보를 제공하는 데 사용될 수 있습니다. 이 과정은 3.3 절에서 다룬 '이해관계자와의 사이버보안 요구사항 소통'과 다릅니다. 이 경우에는 공급업체에 사이버보안 요구사항 세트를 부과하는 것이 불가능할 수 있습니다. 목표는 신중하게 결정된 사이버보안 요구사항 목록을 고려하여 여러 공급업체 중 최선의 구매 결정을 하는 것입니다. 종종 이는 여러 제품 또는 서비스를 목표 프로파일에 대한 격차와 비교하면서 일정 수준의 타협점을 찾는 것을 의미합니다.

제품이나 서비스가 구매되면, 프로파일은 잔여 사이버보안 위험을 추적하고 해결하는 데도 사용될 수 있습니다. 예를 들어, 구매한 서비스 또는 제품이 목표 프로파일에 기술된 모든 목표를 충족시키지 못한 경우, 조직은 다른 관리 조치를 통해 잔여 위험을 해결할 수 있습니다. 프로파일은 또한 주기적인 검토 및 테스트 메커니즘을 통해 제품이 사이버보안 결과를 충족하는지 평가하는 방법을 조직에 제공합니다.

3.5 새로운 또는 개정된 참조 정보 기회 식별

프레임워크는 조직이 새롭게 부각되는 요구사항을 해결하기 위해 추가적인 참조 정보가 도움이 될 수 있는 새로운 또는 개정된 표준, 지침 또는 관행에 대한 기회를 식별하는 데 사용될 수 있습니다. 특정 하위 범주를 구현하거나 새로운 하위 범주를 개발하는 조직은 관련 활동에 대한 참조 정보가 거의 없거나 전혀 없음을 발견할 수 있습니다. 이러한 필요를 해결하기 위해, 조직은 기술 리더 및/또는 표준 기관과 협력하여 표준, 지침 또는 관행을 초안, 개발 및 조정할 수 있습니다.

3.6 개인정보 보호 및 시민 자유 보호 방법론

이 섹션은 사이버보안으로 인해 발생할 수 있는 개인정보 보호와 시민 자유에 대한 영향을 다루는 방법론을 설명합니다. 이 방법론은 개인정보 보호와 시민 자유의 영향이 부문별로 또는 시간에 따라 다를 수 있고, 조직이 이러한 고려사항과 프로세스를 다양한 기술적 구현으로 처리할 수 있기 때문에, 일반적인 고려사항 및 프로세스를 목표로 합니다. 그럼에도 불구하고, 사이버보안 프로그램의 모든 활동이 개인정보 보호와 시민 자유 고려사항을 야기하는 것은 아닙니다. 개인정보 보호를 위한 기술적 표준, 지침 및 추가적인 최선의 관행이 개발되어야 할 수도 있습니다.

개인정보 보호와 사이버보안은 강한 연결을 가지고 있습니다. 조직의 사이버보안 활동은 개인 정보를 사용, 수집, 처리, 유지 또는 공개할 때 개인정보 보호와 시민 자유에 위험을 초래할 수 있습니다. 예를 들어, 개인 정보의 과도한 수집이나 보유로 이어지는 사이버보안 활동; 사이버보안 활동과 관련이 없는 개인 정보의 공개 또는 사용; 서비스 거부 또는 다른 유사한 잠재적 부정적 영향을 초래하는 사이버보안 완화 활동; 표현의 자유나 결사의 자유를 억제할 수 있는 일부 사고 탐지 또는 모니터링 유형 등이 있습니다.

정부와 그 대리인은 사이버보안 활동에서 발생하는 시민 자유를 보호할 책임이 있습니다. 아래에 설명된 방법론에서 참조된 바와 같이, 핵심 인프라를 소유하거나 운영하는 정부 또는 그 대리인은 적용 가능한 개인정보 보호 법률, 규정 및 헌법 요구사항에 따라 사이버보안 활동의 준수를 지원하는 프로세스를 갖추어야 합니다.

개인정보 보호 영향을 다루기 위해 조직은 사이버보안 프로그램이 다음과 같은 개인정보 보호 원칙을 어떻게 통합할 수 있는지 고려할 수 있습니다: 사이버보안 사건과 관련된 개인 정보의 수집, 공개 및 보유에서 데이터 최소화; 사이버보안 활동을 위해 특별히 수집된 정보에 대한 사이버보안 활동 외의 사용 제한; 특정 사이버보안 활동에 대한 투명성; 사이버보안 활동에서 개인 정보 사용으로 인해 발생하는 부정적 영향에 대한 개인 동의 및 구제; 데이터 품질, 무결성 및 보안; 책임감 및 감사.

조직이 부록 A 의 프레임워크 코어를 평가함에 따라, 위에서 언급한 개인정보 보호 및 시민 자유 영향을 다루기 위한 다음과 같은 프로세스 및 활동을 고려할 수 있습니다:

사이버보안 위험 관리 거버넌스

- 조직의 사이버보안 위험 평가 및 잠재적 위험 대응은 사이버보안 프로그램의 개인정보 보호 영향을 고려합니다.
- 사이버보안 관련 개인정보 보호 책임을 가진 직원은 적절한 관리진에게 보고하며 적절한 교육을 받습니다.
- 사이버보안 활동이 적용 가능한 개인정보 보호 법률, 규정 및 헌법 요구사항을 준수하도록 지원하는 프로세스가 마련되어 있습니다.
- 위 조직 조치 및 통제의 구현을 평가하는 프로세스가 마련되어 있습니다.

조직 자산 및 시스템에 대한 개인의 식별, 인증 및 권한 부여 접근 방식

- 개인 정보의 수집, 공개 또는 사용을 포함하는 범위에서 신원 관리 및 접근 제어 조치의 개인정보 보호 영향을 식별하고 해결하기 위한 조치가 취해집니다.

인식 및 교육 조치

- 조직의 개인정보 보호 정책에서 적용 가능한 정보가 사이버보안 근로자 교육 및 인식 활동에 포함됩니다.
- 조직을 위해 사이버보안 관련 서비스를 제공하는 서비스 제공업체는 조직의 적용 가능한 개인정보 보호 정책에 대해 알고 있습니다.

비정상 활동 탐지 및 시스템 및 자산 모니터링

- 조직의 비정상 활동 탐지 및 사이버보안 모니터링에 대한 개인정보 보호 검토를 수행하는 프로세스가 마련되어 있습니다.

대응 활동, 정보 공유 또는 기타 완화 노력

- 사이버보안 정보 공유 활동의 일부로 조직 외부에 개인 정보가 공유되는지, 언제, 어떻게, 어느 정도로 공유되는지를 평가하고 해결하는 프로세스가 마련되어 있습니다.
- 조직의 사이버보안 완화 노력에 대한 개인정보 보호 검토를 수행하는 프로세스가 마련되어 있습니다.

4.0 프레임워크를 사용한 사이버보안 위험 자체 평가

사이버보안 프레임워크는 조직 목표에 대한 사이버보안 위험 관리를 향상시켜 위험을 감소시키기 위해 설계되었습니다. 이상적으로, 프레임워크를 사용하는 조직은 위험을 측정하고, 위험을 수용 가능한 수준으로 줄이기 위한 조치의 비용과 이익에 값을 할당할 수 있습니다. 조직이 사이버보안 전략 및 조치의 위험, 비용 및 이익을 더 잘 측정할수록, 그들의 사이버보안 접근 방식과 투자는 더 합리적이고 효과적이며 가치 있게 됩니다.

시간이 지남에 따라, 자가 평가 및 측정은 투자 우선순위에 대한 의사결정을 개선하는 데 도움이 될 수 있습니다. 예를 들어, 조직의 사이버보안 상태와 시간에 따른 추세의 측면을 측정하거나 적어도 강력하게 특징화하는 것은 해당 조직이 의존하는 업체, 공급업체, 구매자 및 기타 당사자들에게 의미 있는 위험 정보를 이해하고 전달할 수 있게 합니다. 조직은 이를 내부적으로 수행하거나 제 3 자 평가를 통해 이루어질 수 있습니다. 제대로 수행되고 한계를 인식한다면, 이러한 측정은 조직 내부 및 외부에서 강력한 신뢰 관계를 위한 기반을 제공할 수 있습니다.

투자의 효과성을 검토하기 위해, 조직은 먼저 자신의 조직 목표, 그 목표와 지원되는 사이버보안 결과 사이의 관계, 그리고 그러한 개별적인 사이버보안 결과가 어떻게 구현되고 관리되는지에 대한 명확한 이해가 필요합니다. 이러한 모든 항목의 측정은 프레임워크의 범위를 벗어나지만, 프레임워크 코어의 사이버보안 결과는 다음과 같은 방법으로 투자 효과성과 사이버보안 활동의 자가 평가를 지원합니다:

- 사이버보안 운영의 다양한 부분이 목표 구현 단계의 선택에 어떻게 영향을 미칠지에 대한 선택을 하는 것,
- 현재 구현 단계를 결정함으로써 조직의 사이버보안 위험 관리 접근 방식을 평가하는 것,
- 목표 프로파일을 개발함으로써 사이버보안 결과에 우선 순위를 두는 것,
- 현재 프로파일을 평가함으로써 특정 사이버보안 조치가 원하는 사이버보안 결과를 얼마나 달성하는지 결정하는 것,
- 참조 정보로 나열된 컨트롤 카탈로그 또는 기술 지침의 구현 정도를 측정하는 것.

사이버보안 성과 지표 개발은 진화하고 있습니다. 조직은 자신들이 사이버보안 위험 관리 개선에서 현재 상태와 진전을 나타내는 인공적인 지표에 의존하지 않으면서, 측정을 사용하여 최적화를 달성하는 방법에 대해 신중하고 창의적이며 주의 깊게 생각해야 합니다. 사이버 위험을 판단하는 것은 규율을 요구하며 정기적으로 재검토되어야 합니다. 프레임워크

프로세스의 일부로 측정이 사용될 때마다, 조직은 이러한 측정이 왜 중요하고 어떻게 사이버보안 위험 관리 전반에 기여할 것인지 명확하게 식별하고 알아야 합니다. 또한 사용되는 측정의 한계에 대해서도 명확해야 합니다.

예를 들어, 보안 조치와 사업 결과를 추적하는 것은 조직 목표 달성에 미세한 보안 제어 변경이 어떤 영향을 미치는지에 대한 의미 있는 통찰을 제공할 수 있습니다. 일부 조직 목표의 달성을 검증하기 위해서는 그 목표가 달성되었어야 할 시점 이후에 데이터를 분석해야 합니다. 이러한 유형의 지연된 측정은 더 절대적입니다. 그러나 종종 사이버보안 위험이 발생할 수 있는지, 그리고 그것이 어떤 영향을 미칠 수 있는지를 선행 지표를 사용하여 예측하는 것이 더 가치 있습니다.

조직은 프레임워크 적용에 측정을 통합하는 방법을 혁신하고 맞춤화 할 것을 권장되며, 그 유용성과 한계를 충분히 이해해야 합니다.

부록 A: 프레임워크 코어

이 부록은 프레임워크 코어를 제시합니다: 모든 핵심 인프라 부문에서 공통적인 특정 사이버보안 활동을 설명하는 기능, 범주, 하위 범주 및 참조 정보 목록입니다. 프레임워크 코어에 대한 선택된 표현 형식은 특정 구현 순서를 제안하거나 범주, 하위 범주 및 참조 정보의 중요도를 시사하지 않습니다. 이 부록에 제시된 프레임워크 코어는 사이버보안 위험 관리를 위한 공통 활동 세트를 대표합니다. 프레임워크가 완벽하지는 않지만 확장 가능하여 조직, 부문 및 기타 엔티티가 경제적이고 효율적인 하위 범주 및 참조 정보를 사용하여 자신의 사이버보안 위험을 관리할 수 있습니다. 프로파일 생성 과정에서 프레임워크 코어에서 활동을 선택하고 추가 범주, 하위 범주 및 참조 정보를 프로파일에 추가할 수 있습니다. 조직의 위험 관리 프로세스, 법적/규제 요구사항, 사업/임무 목표 및 조직적 제약사항이 프로파일 생성 중 이러한 활동 선택을 안내합니다. 개인정보는 보안 위험과 보호를 평가할 때 범주에서 언급된 데이터 또는 자산의 구성요소로 간주됩니다.

IT 및 ICS 에 대해 기능, 범주 및 하위 범주에서 식별된 의도된 결과는 동일하지만, IT 와 ICS 의 운영 환경 및 고려사항은 다릅니다. ICS 는 물리적 세계에 직접적인 영향을 미치며, 개인의 건강 및 안전에 대한 잠재적 위험과 환경에 대한 영향을 포함합니다. 또한, ICS 는 IT 와 비교하여 독특한 성능 및 신뢰성 요구사항을 가지며, 사이버보안 조치를 구현할 때 안전과 효율성 목표를 고려해야 합니다.

사용 편의를 위해 프레임워크 코어의 각 구성요소는 고유 식별자를 가집니다. 기능과 범주는 표 1 에 나타난 것처럼 각각 고유의 알파벳 식별자를 가집니다. 각 범주 내의 하위 범주는 숫자로 참조되며, 각 하위 범주의 고유 식별자는 표 2 에 포함되어 있습니다.

프레임워크와 관련된 추가 지원 자료, 유용한 참조 정보는 http://www.nist.gov/cyberframework/ 웹사이트에서 찾을 수 있습니다.

표 1: 기능 및 범주 고유 식별자

기능 고유 식별자	기능	범주 고유 식별자	범주
ID	Identify (식별)	ID.AM	자산 관리(Asset Management)
		ID.BE	비즈니스 환경(Business Environment)
		ID.GV	거버넌스(Governance)
		ID.RA	위험 평가(Risk Assessment)
		ID.RM	위험 관리 전략(Risk Management Strategy)
		ID.SC	공급망 위험 관리(Supply Chain Risk Management)
PR	Protect (보호)	PR.AC	신원 관리 및 접근 제어 (Identity Management and Access Control)
		PR.AT	인식 및 교육(Awareness and Training)
		PR.DS	데이터 보안(Data Security)
		PR.IP	정보 보호 프로세스 및 절차 (Information Protection Processes and Procedures)
		PR.MA	유지 관리(Maintenance)
		PR.PT	보호 기술(Protective Technology)
DE	Detect (탐지)	DE.AE	이상 현상 및 사건(Anomalies and Events)
		DE.CM	보안 지속 모니터링(Security Continuous Monitoring)
		DE.DP	탐지 프로세스(Detection Processes)
RS	Respond (대응)	RS.RP	대응 계획(Response Planning)
		RS.CO	커뮤니케이션(Communications)
		RS.AN	분석(Analysis)
		RS.MI	완화(Mitigation)
		RS.IM	개선(Improvements)
RC	Recover (복구)	RC.RP	복구 계획(Recovery Planning)
		RC.IM	개선(Improvements)
		RC.CO	커뮤니케이션(Communications)

Table 2: Framework Core

기능	범주	하위 범주	참조 정보
식별 (IDENTIFY) (ID)	**자산 관리** **Asset Management (ID.AM):** 조직이 사업 목적을 달성하기 위해 필요한 데이터, 인력, 장치, 시스템 및 시설은 조직 목표에 위한 상대적 중요도와 조직의 위험 전략에 일관되게 식별되고 관리됩니다.	**ID.AM-1:** 조직 내의 물리적 장치 및 시스템이 목록 화됩니다.	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: 조직 내의 소프트웨어 플랫폼 및 응용 프로그램이 목록 화됩니다.	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: 조직의 커뮤니케이션 및 데이터 흐름이 대응 됩니다.	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 외부 정보 시스템이 카탈로그 화됩니다.	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: 자원(예: 하드웨어, 장치, 데이터, 시간, 인력, 소프트웨어)은 분류, 중요도 및 비즈니스 가치에 따라 우선 순위가 지정됩니다.	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: 전체 인력 및 제 3 자 이해관계자(예: 공급업체, 고객, 파트너)에 대한 사이버보안 역할 및 책임이 설정됩니다.	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

기능	범주	하위 범주	참조 정보
			ISA 62443-2-1:2009 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	비즈니스 환경 **Business Environment (ID.BE):** 조직의 임무, 목표, 이해관계자 및 활동이 이해되고 우선 순위가 지정됩니다. 이 정보는 사이버보안 역할, 책임 및 위험 관리 결정을 안내하는 데 사용됩니다.	**ID.BE-1:** 조직의 공급망 내 역할이 식별되고 소통됩니다.	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: 조직의 핵심 인프라 및 산업 부문 내 위치가 식별되고 소통됩니다.	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: 조직의 임무, 목표 및 활동에 대한 우선 순위가 설정되고 소통됩니다.	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: 중요 서비스 제공을 위한 의존성 및 핵심 기능이 설정됩니다.	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에서 중요 서비스 제공을 지원하기 위한 복원력 요구사항이 설정됩니다.	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	거버넌스 **Governance (ID.GV):** 조직의 규제, 법적, 위험, 환경 및 운영 요구사항을 관리하고 모니터링하기 위한 정책, 절차 및 프로세스가 이해되며,	**ID.GV-1:** 조직의 사이버보안 정책이 설정되고 소통됩니다.	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families

기능	범주	하위 범주	참조 정보
	이는 사이버보안 위험 관리에 대한 정보를 제공합니다.	**ID.GV-2:** 사이버보안 역할 및 책임은 내부 역할 및 외부 파트너와 조율되고 일치됩니다.	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: 사이버보안과 관련된 법적 및 규제 요구사항, 개인정보 보호 및 시민 자유의 권리를 포함하여 이해되고 관리됩니다.	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: 거버넌스 및 위험 관리 프로세스는 사이버보안 위험을 다룹니다.	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	위험 평가 **Risk Assessment (ID.RA):** 조직은 조직 운영(임무, 기능, 이미지 또는 명성 포함), 조직 자산 및 개인에 대한 사이버보안 위험을 이해합니다.	**ID.RA-1:** 자산 취약점이 식별되고 문서화됩니다.	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: 사이버 위협 정보는 정보 공유 포럼 및 소스로부터 수신됩니다.	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

기능	범주	하위 범주	참조 정보
		ID.RA-3: 내부 및 외부 위협이 식별되고 문서화됩니다.	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: 잠재적인 비즈니스 영향 및 가능성이 식별됩니다.	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: 위협, 취약점, 가능성 및 영향은 위험을 결정하는 데 사용됩니다.	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: 위험 대응은 식별되고 우선 순위가 지정됩니다.	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	위험 관리 전략 **Risk Management Strategy (ID.RM):** 조직의 우선 순위, 제약 사항, 위험 허용도 및 가정이 운영 위험 결정을 지원합니다.	**ID.RM-1:** 위험 관리 프로세스는 조직 이해관계자에 의해 설정되고 관리되며 합의됩니다.	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: 조직의 위험 허용도가 결정되고 명확하게 표현됩니다.	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** PM-9

기능	범주	하위 범주	참조 정보
		ID.RM-3: 조직의 위험 허용도 결정은 핵심 인프라에서의 역할과 부문별 위험 분석에 의해 정보를 제공받습니다.	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	공급망 위험 관리 **Supply Chain Risk Management (ID.SC):** 조직의 우선 순위, 제약 사항, 위험 허용도 및 가정은 공급망 위험 관리와 관련된 위험 결정을 지원하기 위해 설정되고 사용됩니다. 조직은 공급망 위험을 식별, 평가 및 관리하기 위한 프로세스를 수립하고 구현합니다.	**ID.SC-1:** 사이버 공급망 위험 관리 프로세스는 조직 이해관계자에 의해 식별되고, 수립되며, 평가되고, 관리되고, 합의됩니다.	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: 정보 시스템, 구성 요소 및 서비스의 공급업체 및 제 3 자 파트너는 사이버 공급망 위험 평가 프로세스를 사용하여 식별되고, 우선 순위가 지정되며, 평가됩니다.	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: 공급업체 및 제 3 자 파트너와의 계약은 조직의 사이버보안 프로그램 및 사이버 공급망 위험 관리 계획의 목표를 충족하기 위한 적절한 조치를 구현하는 데 사용됩니다.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: 공급업체 및 제 3 자 파트너는 정기적으로 감사, 테스트 결과 또는 기타 형태의 평가를 사용하여 계약 의무를 충족하고 있는지 확인합니다.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

기능	범주	하위 범주	참조 정보
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: 공급업체 및 제 3 자 제공업체와 함께 대응 및 복구 계획 수립과 테스트가 수행됩니다.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
보호 **PROTECT (PR)**	신원 관리 및 접근 제어 **Identity Management, Authentication and Access Control (PR.AC):** 물리적 및 논리적 자산 및 관련 시설에 대한 접근은 승인된 사용자, 프로세스 및 장치로 제한되며, 승인된 활동 및 거래에 대한 무단 접근으로 평가된 위험과 일관되게 관리됩니다.	**PR.AC-1:** 승인된 장치, 사용자 및 프로세스에 대한 신원 및 자격 증명은 발급, 관리, 검증, 취소 및 감사됩니다.	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: 자산에 대한 물리적 접근은 관리되고 보호됩니다.	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: 원격 접근은 관리됩니다.	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

기능	범주	하위 범주	참조 정보
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: 접근 권한 및 승인은 최소 권한 원칙과 직무 분리 원칙을 포함하여 관리됩니다.	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: 네트워크 무결성이 보호됩니다. (네트워크 분리, 네트워크 세분화)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: 신원은 증명되고 자격 증명과 연결되며 상호 작용됩니다.	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: 사용자, 장치 및 기타 자산은 거래의 위험에 상응하여 인증됩니다. (개인의 보안 및 개인정보 보호 위험 및 기타 조직적 위험)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

기능	범주	하위 범주	참조 정보
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	인식 및 교육 **Awareness and Training (PR.AT):** 조직의 인력 및 파트너들은 사이버보안 인식 교육을 받고 관련 정책, 절차 및 협약에 일치하는 사이버보안 관련 업무 및 책임을 수행하기 위해 훈련됩니다.	**PR.AT-1:** 모든 사용자들은 정보를 제공받고 훈련됩니다.	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: 특별한 권한을 가진 사용자들은 자신의 역할과 책임을 이해합니다.	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: 제 3 자 이해관계자(예: 공급업체, 고객, 파트너)는 자신의 역할과 책임을 이해합니다.	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: 고위 경영진은 자신의 역할과 책임을 이해합니다.	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: 물리적 및 사이버보안 인력은 자신의 역할과 책임을 이해합니다.	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

기능	범주	하위 범주	참조 정보
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	데이터 보안 **Data Security (PR.DS):** 정보 및 기록(데이터)은 조직의 위험 전략에 일치하게 관리되어 정보의 기밀성, 무결성 및 가용성을 보호합니다.	**PR.DS-1:** 휴지 상태의 데이터는 보호됩니다.	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: 전송 중인 데이터는 보호됩니다.	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: 자산은 제거, 이전 및 처분 전반에 걸쳐 공식적으로 관리됩니다.	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: 가용성을 보장하기 위한 충분한 용량이 유지됩니다.	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: 데이터 유출에 대한 보호 조치가 구현됩니다.	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

기능	범주	하위 범주	참조 정보
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: 소프트웨어, 펌웨어 및 정보 무결성을 검증하기 위해 무결성 검사 메커니즘이 사용됩니다.	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: 개발 및 테스트 환경은 생산 환경과 분리됩니다.	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: 하드웨어 무결성을 검증하기 위해 무결성 검사 메커니즘이 사용됩니다.	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	정보 보호 프로세스 및 절차 Information Protection Processes and Procedures (PR.IP): 보안 정책(목적, 범위, 역할, 책임, 관리의 헌신 및 조직 부서 간의 조정을 다루는 정책), 프로세스 및 절차는 유지되고 정보 시스템 및 자산의 보호를 관리하기 위해 사용됩니다.	**PR.IP-1:** 최소 기능성 개념과 같은 보안 원칙을 통합하여 정보 기술/산업 제어 시스템의 기본 설정이 생성되고 유지됩니다.	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: 시스템을 관리하기 위한 시스템 개발 수명 주기가 구현됩니다.	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

기능	범주	하위 범주	참조 정보
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: 구성 변경 제어 프로세스가 마련되어 있습니다.	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: 정보의 백업이 수행되며, 유지되고, 테스트됩니다.	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: 조직 자산의 물리적 운영 환경에 관한 정책 및 규정이 준수됩니다.	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: 데이터는 정책에 따라 파기됩니다.	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

기능	범주	하위 범주	참조 정보
		PR.IP-7: 보호 프로세스가 개선됩니다.	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: 보호 기술의 효과성이 공유됩니다.	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: 대응 계획(사고 대응 및 비즈니스 연속성)과 복구 계획(사고 복구 및 재해 복구)이 마련되어 관리됩니다.	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: 대응 및 복구 계획이 테스트됩니다.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: 사이버보안이 인적 자원 관행(예: 권한 해지, 인력 검증)에 포함됩니다.	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

기능	범주	하위 범주	참조 정보
		PR.IP-12: 취약점 관리 계획이 개발되고 구현됩니다.	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	유지 관리 **Maintenance (PR.MA):** 산업 제어 및 정보 시스템 구성 요소의 유지보수 및 수리가 정책 및 절차에 따라 수행됩니다.	**PR.MA-1:** 조직 자산의 유지보수 및 수리가 통제된 도구를 사용하여 승인되고 수행되며 기록됩니다.	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: 조직 자산의 원격 유지보수는 무단 접근을 방지하는 방식으로 승인되고 기록되며 수행됩니다.	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	보호 기술 **Protective Technology (PR.PT):** 기술 보안 솔루션은 관련 정책, 절차 및 협약에 일치하며 시스템 및 자산의 보안 및 복원력을 보장하기 위해 관리됩니다.	**PR.PT-1:** 감사/로그 기록은 정책에 따라 결정되고 문서화되며 구현되고 검토됩니다.	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: 이동식 미디어는 보호되며 정책에 따라 사용이 제한됩니다.	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

기능	범주	하위 범주	참조 정보
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: 필수 기능만 제공하도록 시스템을 구성하여 최소 기능성 원칙이 통합됩니다.	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: 통신 및 제어 네트워크가 보호됩니다.	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: 정상 및 불리한 상황에서 복원력 요구사항을 달성하기 위해 메커니즘(예: 장애 복구, 부하 분산, 핫 스왑)이 구현됩니다.	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
감지 **DETECT (DE)**		**DE.AE-1:** 사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

기능	범주	하위 범주	참조 정보
	이상 현상 및 사건 Anomalies and Events (DE.AE): 이상 활동이 탐지되며 사건의 잠재적 영향이 이해됩니다.	흐름의 기준선이 설정되고 관리됩니다.	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: 탐지된 사건은 공격 대상 및 방법을 이해하기 위해 분석됩니다.	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: 다양한 소스 및 센서로부터 사건 데이터가 수집되고 상관관계가 분석됩니다.	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: 사건의 영향이 결정됩니다.	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: 사고 경보 임계값이 설정됩니다.	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	보안 지속 모니터링 Security Continuous Monitoring (DE.CM): 정보 시스템과 자산은 사이버보안 사건을 식별하고 보호 조치의 효과성을 검증하기 위해 모니터링됩니다.	**DE.CM-1:** 네트워크는 잠재적 사이버보안 사건을 탐지하기 위해 모니터링됩니다.	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

기능	범주	하위 범주	참조 정보
		DE.CM-2: 물리적 환경은 잠재적 사이버보안 사건을 탐지하기 위해 모니터링됩니다.	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: 인력 활동은 잠재적 사이버보안 사건을 탐지하기 위해 모니터링됩니다.	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: 악성 코드가 탐지됩니다.	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: 승인되지 않은 모바일 코드가 탐지됩니다.	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: 외부 서비스 제공업체 활동은 잠재적 사이버보안 사건을 탐지하기 위해 모니터링됩니다.	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: 승인되지 않은 인력, 연결, 장치 및 소프트웨어에 대한 모니터링이 수행됩니다.	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: 취약점 스캔이 수행됩니다.	**CIS CSC** 4, 20

기능	범주	하위 범주	참조 정보
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	탐지 프로세스 **Detection Processes (DE.DP):** 이상 사건에 대한 인식을 보장하기 위해 탐지 프로세스 및 절차가 유지되고 테스트됩니다.	**DE.DP-1:** 탐지에 대한 역할 및 책임이 잘 정의되어 책임을 보장합니다.	**CIS CSC** 19 **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: 탐지 활동은 모든 적용 가능한 요구사항을 준수합니다.	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: 탐지 프로세스가 테스트됩니다.	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: 사건 탐지 정보가 소통됩니다.	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: 탐지 프로세스는 지속적으로 개선됩니다.	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

기능	범주	하위 범주	참조 정보
대응 **RESPOND (RS)**	**대응 계획** **Response Planning (RS.RP):** 탐지된 사이버보안 사건에 대응하기 위해 대응 프로세스 및 절차가 실행되고 유지됩니다.	**RS.RP-1:** 사건 발생 중이나 후에 대응 계획이 실행됩니다.	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	커뮤니케이션 **Communications (RS.CO):** 대응 활동은 내부 및 외부 이해관계자(예: 법 집행 기관으로부터의 외부 지원)와 조율됩니다.	**RS.CO-1:** 대응이 필요할 때 직원들은 자신의 역할과 운영 순서를 알고 있습니다.	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: 사건은 설정된 기준에 따라 보고됩니다.	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: 정보는 대응 계획에 따라 공유됩니다.	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: 이해관계자와의 조율은 대응 계획에 따라 일관되게 발생합니다.	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: 더 넓은 사이버보안 상황 인식을 달성하기 위해 외부 이해관계자와 자발적인 정보 공유가 발생합니다.	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

기능	범주	하위 범주	참조 정보
	분석 **Analysis (RS.AN):** 효과적인 대응 및 복구 활동을 지원하고 보장하기 위한 분석이 수행됩니다.	**RS.AN-1:** 탐지 시스템으로부터의 통지 내용이 조사됩니다.	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: 사건의 영향을 이해합니다.	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: 포렌식이 수행됩니다.	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: 대응 계획에 따라 사건이 범주화 됩니다.	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: 내부 및 외부 소스(예: 내부 테스트, 보안 공지사항, 보안 연구원)에서 조직에게 공개된 취약점을 수신, 분석 및 대응하기 위한 프로세스가 수립됩니다.	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	완화 **Mitigation (RS.MI):** 사건 확산을 방지하고 영향을 완화하며 사건을 해결하기 위한 활동이 수행됩니다.	**RS.MI-1:** 사건을 억제합니다.	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

기능	범주	하위 범주	참조 정보
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: 사건이 완화됩니다.	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: 새로 발견된 취약점이 완화되거나 수용된 리스크로 문서화됩니다.	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	개선 **Improvements (RS.IM):** 현재 및 이전의 탐지/대응 활동에서 얻은 교훈을 포함하여 조직의 대응 활동이 개선됩니다.	**RS.IM-1:** 대응 계획이 교훈을 포함합니다.	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: 대응 전략이 업데이트됩니다.	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
복구 **RECOVER (RC)**	**복구 계획** **Recovery Planning (RC.RP):** 사이버 보안 사건으로 영향을 받은 시스템 또는 자산을 복구하기 위해 복구 프로세스와 절차가 실행 및 유지됩니다.	**RC.RP-1:** 사이버 보안 사건 중 또는 이후에 복구 계획이 실행됩니다.	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	개선 **Improvements (RC.IM):** 복구 계획 및 프로세스는 향후 활동에 교훈을 통합함으로써 개선됩니다.	**RC.IM-1:** 복구 계획에는 교훈이 통합됩니다.	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: 복구 전략이 업데이트됩니다.	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

기능	범주	하위 범주	참조 정보
	커뮤니케이션 **Communications (RC.CO):** 복구 활동은 내부 및 외부 당사자와 조정됩니다(예: 조정 센터, 인터넷 서비스 제공자, 공격 시스템 소유자, 피해자, 기타 CSIRT 및 공급 업체)	**RC.CO-1:** 공공 관계는 관리됩니다.	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: 사건 후 평판이 회복됩니다.	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: 회복 활동은 내부 및 외부 이해 관계자 뿐만 아니라 경영진과 경영팀에게도 전달됩니다.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

부록 A 에 기재된 참조 정보의 관한 내용은 아래 위치에서 찾을 수 있습니다:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. 정보 참고 자료는 통제 수준(control level)에만 대응되며, 그러나 어떤 통제 개선사항이 하위 범주 결과를 달성하는 데 유용할 수 있습니다.

프레임워크 코어 하위 범주와 참조 정보 자료 사이의 대응은 특정 참조 정보 자료 섹션과 하위 범주 결과를 정확하게 결정하는 데 사용되지 않습니다. 참조 정보 자료는 모든 요소(예: 통제, 요구 사항)가 프레임워크 코어 하위 범주와 대응되지 않으므로 각각의 하위 범주와 참조 정보 자료 간에 완전한 일치가 없을 수 있습니다.

부록 B: 용어 사전

이 부록은 출판물에서 사용되는 일부 용어를 정의합니다.

표 3: 프레임워크 용어사전

Buyer	구매자	주어진 제품이나 서비스를 소비하는 개인 또는 기관입니다.
Category	범주	기능을 하위 그룹으로 나누어, 프로그램적 필요와 특정 활동과 밀접하게 관련된 사이버 보안 결과입니다. 범주의 예로는 "자산 관리," "신원 관리 및 접근 제어," "탐지 프로세스"가 있습니다.
Critical Infrastructure	핵심 인프라	미국에 매우 중요한 물리적 또는 가상의 시스템과 자산으로, 이러한 시스템과 자산의 무능력화 또는 파괴가 사이버 보안, 국가 경제 안보, 국가 공중 보건 또는 안전, 또는 이러한 사항들의 조합에 심각한 영향을 미칠 수 있는 것.
Cybersecurity	사이버 보안	공격을 방지하고 탐지하며 대응하여 정보를 보호하는 과정.
Cybersecurity Event	사이버 보안 사건	조직의 운영(임무, 능력 또는 평판)에 영향을 미칠 수 있는 사이버 보안 변경사항.
Cybersecurity Incident	사이버 보안 사고	조직에 영향을 미치는 것으로 판단되어 응답과 회복이 필요한 사이버 보안 사고.
Detect (function)	탐지	사이버 보안 사건의 발생을 식별하기 위한 적절한 활동을 개발하고 실행합니다.
Framework	프레임워크	사이버 보안 위험을 감소시키기 위한 위험 기반 접근 방식으로 구성된 것으로, 프레임워크 코어, 프레임워크 프로필 및 프레임워크 구현 티어로 구성됩니다. 또한 "사이버 보안 프레임워크"로도 알려져 있습니다.
Framework Core	프레임워크 코어	다양한 핵심 기반 구조 부문에서 공통으로 나타나는 사이버 보안 활동 및 참고 자료로, 프레임워크 코어에는 기능, 범주, 하위 범주 및 참조 정보 항목의 네 가지 유형의 요소가 포함됩니다.
Framework Implementation Tier	프레임워크 구현 티어	조직의 리스크 관리 접근 방식 및 사이버 보안 리스크 관리를 수행하는 프로세스를 볼 때의 특성을 나타내는 요소입니다.

Framework Profile	프레임워크 프로파일	특정 시스템 또는 조직이 프레임워크의 범주와 하위 범주에서 선택한 결과를 나타내는 것입니다.
Function	기능	프레임워크의 주요 구성 요소 중 하나입니다. 기능은 기본 사이버 보안 활동을 범주와 하위 범주로 구성하는 데 가장 높은 수준의 구조를 제공합니다. 다섯 가지 기능은 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)입니다.
Identify (function)	식별	시스템, 자산, 데이터 및 능력에 대한 사이버 보안 리스크를 관리하기 위한 조직의 이해를 개발합니다.
Informative Reference	참조 정보	핵심 인프라 섹터에서 공통으로 사용되는 표준, 지침 및 관행의 특정 섹션으로, 각 하위 범주와 관련된 결과를 달성하기 위한 방법을 설명합니다. 참조 정보의 예로는 "ISO/IEC 27001 Control A.10.8.3"이 있으며, 이것은 "보호(Protect)" 기능의 "데이터 보안(Data Security)" 범주에 속하는 "데이터 전송 중 보호(Data-in-transit is protected)" 하위 범주를 지원합니다.
Mobile Code	모바일 코드	스크립트, 매크로, 또는 기타 이식 가능한 지시문 등의 프로그램으로, 변경 없이 다양한 플랫폼에 전송되어 동일한 의미로 실행될 수 있는 것.
Protect (function)	보호	핵심 인프라 서비스의 제공을 보장하기 위해 적절한 보호 조치를 개발하고 구현하는 것.
Privileged User	특별한 권한 사용자	보안 관련 기능을 수행할 수 있는 권한(그리고 따라서 신뢰)을 부여 받은 사용자로, 일반 사용자가 수행할 수 없는 기능을 수행할 수 있는 사람.
Recover (function)	회복	사이버보안 사건으로 인해 손상된 기능이나 서비스를 복원하고 복원력을 유지하기 위한 계획을 개발하고 구현하는 것.
Respond (function)	대응	감지된 사이버보안 사건에 대해 조치를 취하기 위한 적절한 활동을 개발하고 구현하는 것.
Risk	위험	개체가 잠재적인 상황이나 사건에 의해 위협받는 정도를 나타내는 척도로, 일반적으로 다음 두 가지 기능에 의해 결정됩니다: (i) 해당 상황이나 사건이 발생했을 때 발생할 수 있는 부정적인 영향; (ii) 발생 가능성.
Risk Management	위험 관리	위험을 식별, 평가하고 대응하는 과정.

Subcategory	하위범주	카테고리를 기술적 및/또는 관리적 활동의 구체적인 결과로 세분화한 것. 하위 범주의 예시로는 "외부 정보 시스템의 목록화", "저장된 데이터의 보호", "탐지 시스템의 알림 조사" 등이 있습니다.
Supplier	공급업체	조직의 내부 목적(예: IT 인프라)에 사용되거나 해당 조직의 구매자에게 제공되는 제품 또는 서비스에 통합되는 제품 및 서비스 제공자.
Taxonomy	분류체계	분류의 체계 또는 방식.

부록 C: 줄임말

이 부록은 해당 출판물에서 사용되는 일부 약어를 정의합니다.

ANSI	American National Standards Institute	미국 국가 표준 협회
CEA	Cybersecurity Enhancement Act of 2014	2014 년 사이버보안 강화법
CIS	Center for Internet Security	인터넷 보안 센터
COBIT	Control Objectives for Information and Related Technology	정보 및 관련 기술을 위한 통제 목표
CPS	Cyber-Physical Systems	사이버-물리 시스템
CSC	Critical Security Control	주요 보안 제어
DHS	Department of Homeland Security	국토 안보부
EO	Executive Order	행정명령
ICS	Industrial Control Systems	산업용 제어 시스템
IEC	International Electrotechnical Commission	국제 전기 표준 기구
IoT	Internet of Things	사물 인터넷
IR	Interagency Report	범부처간 보고서
ISA	International Society of Automation	국제 자동화 협회
ISAC	Information Sharing and Analysis Center	정보 공유 및 분석 센터
ISAO	Information Sharing and Analysis Organization	정보 공유 및 분석 조직
ISO	International Organization for Standardization	국제 표준화 기구
IT	Information Technology	정보 기술
NIST	National Institute of Standards and Technology	미국 국립 표준 기술 연구소
OT	Operational Technology	운영 기술
PII	Personally Identifiable Information	개인 식별 정보
RFI	Request for Information	정보 요청
RMP	Risk Management Process	위험 관리 프로세스
SCRM	Supply Chain Risk Management	공급망 위험 관리
SP	Special Publication	특별 출판