TTA Technical Report

기술보고서

TTAR.xx-xx.xxxx

제정일: 2019년 12월 11일

의료기관 정보인프라의 사이버 보안 참조 모델 (기술보고서)

Reference Model of Cyber Security for Information Infra-structure in HDOs (Technical Reports)

한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 바이오인식 프로젝트그룹(PG505)

기술보고서안 심의 위원회 정보보호 기술위원회(TCx)

	성명	소 속	직위	위원회 및 직위	기술보고서 번호
기술보고서(과제) 제안	한태화	연세의료원	연구교수	-	TTAR.xx-xx.xxxx
기술보고서 초안 작성자	한태화	연세의료원	연구교수	-	TTAR.xx-xx.xxxx
	황인정	명지병원	수석	-	TTAR.xx-xx.xxxx
사무국 담당	김재웅	단장	사무국	-	
	문서연	선임	사무국	-	

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2019.10

서 문

1 기술보고서의 목적

이 기술보고서의 목적은 의료정보 시스템 인프라의 신뢰성을 확보할 수 있는 활용지침과 의료정보 시스템의 사이버보안 위험은 인프라의 증가에 따라 복잡성, 연결성이 증가하여 발생할 수 있음. 그러므로 위험을 줄이기 위해 활용지침 개발을 시작하였음.
본 기술보고서는 의료정보 시스템의 사이버보안 참조모델과 실행방안 및 평가에 관한 것으로서 본문 총 4 장으로 구성되어 있음.

1) KISA
정보보호 및 개인정보보호 (ISMS-P) 인증기준 안내서 (2019.1)
클라우드 서비스 보안인증제 안내서 (2019.3)
2) HIPPA
외국 건강정보보호 제도 현황분석 및 관련 법률, 2007.6. 대한의무기록협회
보건의료정보화를 위한 진료정보교류 기반 구축 및 활성화
병원 의료정보 가이드라인

2 주요 내용 요약

이 기술보고서는 의료정보시스템 사이버보안 활용지침을 2014년 사이버보안에 관한 (미)국립표준기술연구소에서 발표한 운영지침과 국내 의료기관용 정보보호 및 보안에 관한 지침, HIPAA 중 보안에 관한 지침을 통합하여 부록으로 소개하였음
운영지침은 (미)사이버 보안 운영지침이 개념적으로 정리되어 있어 부합화하였고, 국내에서도 의료기관 용으로 개발된 것을 HIPAA (Health Insurance Portability and Accountability Act)와 연동하여 정리하였음
미국의 운영지침은 의료시스템 뿐만 아니라2014년 사이버보안에 관한 미국 법률에 따라 (미)국립표준기술연구소(National Institute of Standards and Technology,NIST)는 사이버보안 위험 프레임워크를 개발하여 주요 인프라 보유자 및 운영자가 자발적으로 사용할 수 있도록 함. 사이버보안 법률에 의하면 국립표준기술연구소는 “주요 인프라 보유자 및 운영자가 사이버 위험을 식별하고 평가 및 관리, 정보보안 조치 및 통제를 포함한 프레임워크에 의해 사용이 유연하고 반복적 사용이 용이하며 보안 성능의 개선과 비용 효율적인 접근법”을 제시하도록 함.
이는 행정 명령 (미)13636에 따라 국립표준기술연구소의 “주요 인프라 사이버보안” 버전 1.0을 공식화하였고 그 이후 개정된 보안 참조 모델을 제공함. 행정 명령 (미)13636에 따라 개발된 사이버보안 참조 모델은 추가적인 규제 요구사항 부여 없이 사업 및 기관 요구사항에 기반하며 비용 대비 효율적인 방법으로 사이버보안을 운영하고 관리하기 위하여 공통 기능을 사용함.

프레임워크는 사이버보안 활동을 이끄는 사업적 동인과 기관의 위험관리 프로세스의 일부분으로서 사이버보안 위험을 고려함. 프레임워크는 총 3개의 장으로 구성되며 각 장은 첫 번째, 프레임워크 코어 두 번째 구현 단계, 마지막은 프레임워크 프로필임. 프레임워크 코어는 주요 인프라에서 일반적인 사이버보안 활동과 결과 그리고 참고 문건의 모음이며, 각 기관이 프로필을 선택할 수 있도록 가이드라인을 제공함. 각 기관은 프레임워크 내 프로필을 사용하여 사이버보안 프로젝트의 목표, 위험수용수준 및 사이버보안 자원 운용 현황에 따라 단계별 우선순위를 정함. 프레임워크는 각 단계에서 기관이 사이버보안 위험을 관리하고 조회하며 이해할 수 있는 운영 원리를 제공하며 사이버보안 목표를 우선 순위화 하고 달성하는 것을 지원함

본 기술보고서는 주요 인프라의 사이버보안 위험 관리를 향상하도록 개발되었지만, 프레임워크는 사이버보안의 모든 영역 또는 부분 영역에서 사용될 수 있음. 프레임워크는 주요 인프라의 보안 및 유연성 개선을 위하여 기관의 크기, 사이버보안 위험의 수준 혹은 사이버보안 성숙도에 따라 기관의 위험 관리 원칙 및 대표 사례를 적용하도록 함

프레임워크는 현재 효과적으로 적용하고 있는 표준, 가이드라인 및 활동 정보를 수집하여 사이버보안에 관한 여러 가지의 접근법 중 공통적인 구조를 제시함. 더불어, 프레임워크는 사이버보안에 대해 세계적으로 인정되는 표준을 참고하므로 주요 인프라를 사용하는 각 분야에서 사이버보안 강화에 대한 국제적 협력 모델로 볼 수 있음

프레임워크는 물리적 환경, 사이버공간 및 사용자 관점, 사이버보안에 미치는 영향을 포함하기 때문에 적용시 유연한 방법을 제공하며 보안이 필요한 기술적 기관에 적용됨. 프레임워크의 적용시 사이버보안 초점이 주로 정보기술(IT), 산업통제시스템(ICS), 사이버물리시스템(CPS) 혹은 사물인터넷(IoT)과 같은 일반적인 기술분야로서 시스템과 연동된 특별한 기기를 포함하지 않음. 프레임워크는 고객, 근로자 및 기타 관계자들의 정보 보호에 영향을 미치는 사이버보안을 다루는데 있어 기관을 지원할 수 있음. 프레임워크의 결과는 인력 개발 및 개선 활동에 사용됨

프레임워크는 주요 인프라 내 사이버보안 위험 관리의 만능 해결책은 아니며, 기관은 고유한 위험 (고유 위협/취약점/위험수용성)을 가짐. 또한 기관마다 프레임워크에 명시된 활동의 구현 방법이 상이함. 기관은 주요 서비스 제공에 필요한 효과적인 보안 활동을 결정할 수 있으며 투자 비용의 최대치를 회수할 수 있도록 우선순위를 정할 수 있음. 궁극적으로 프레임워크는 사이버보안 위험의 감소 및 효과적인 관리를 목적으로 함.

기관에 필요한 사이버보안 요구사항을 운영하기 위해 프레임워크 적용방법은 다양하며 프레임워크 적용방법에 대한 결정은 구현하는 기관이 선택함. 예를 들어, 한 기관은 목표로 하는 위험 관리 활동을 적용하기 위해 프레임워크 구현 단계의 수준을 선택할 수 있고 다른 기관은 전체 위험 관리 포트폴리오를 분석하기 위해 프레임워크 내 분류된 다섯 가지 기능을 사용할 수 있음; 이러한 분석은 통제 메뉴처럼 제공되는 가이드라인을 참고할 수 있음.

프레임워크 기능의 “준수”에 관하여 논의가 있으며 프레임워크는 기관이 필요한 사이버 보안 요구사항 “준수”의 기관화 및 표현형식에 대해 융통성을 가지고 있음. 기관에 의해 프레임워크가 활용될 수 있는 다양한 방법은 “프레임워크에 대한 준수”라고 할 수 있으나, 이해관계자에 따라 여러 가지 의미로 사용될 수 있음
프레임워크는 현행 문서로 산업계에서 구현에 대한 피드백이 전달될 때 마다 갱신되고 개선될 것임. 국립표준기술연구소(NIST)는 모든 민간 기관 및 정부기관과도 조정할 것임. 프레임워크가 더 넓은 보안 활동에 사용됨에 따라, 추가적인 교육은 향후 버전에 반영될 것임. 이는 프레임워크가 새로운 위험관리 솔루션의 사이버 환경 내 주요 인프라 보유자 및 운영자의 요구를 반영하고자 함

본 프레임워크의 보안 활동에 대해 확장되고 효과적인 사용 및 공유는 국가의 주요 인프라 사이버보안을 향상시키는 단계임 - 각각의 기관에게 개정되는 가이드라인을 제공하는 것은 전체적으로 국가의 주요 인프라 및 경제, 사회 분야의 사이버보안 상태를 개선시키는 것임

3 인용 기술보고서와의 비교

해당사항 없음

Preface

1 Purpose

The purpose of this technical report is to provide practical guidelines for ensuring the reliability of medical information system infrastructure and cybersecurity risks of medical information system. Therefore, the development of the guidelines has begun to reduce the risk.
This technical report is about cyber security reference model, medical practice and evaluation of medical information system. It consists of 4 chapters.

2 Summary

Although this Technical Report was developed to improve cybersecurity risk management of key infrastructures, the framework can be used in all or part of cybersecurity. The framework will apply the organization's risk management principles and best practices based on the size of the organization, the level of cybersecurity risk, or the level of cybersecurity maturity to improve the security and flexibility of key infrastructures.

Expanded and effective use and sharing of the security activities of this framework is a step in improving national key infrastructure cybersecurity. Providing revised guidelines for each agency is to improve the state of cybersecurity in the country's major infrastructure, economy and society as a whole.

3 Relationship to Reference Standards

None

목 차(

의료기관 정보인프라의 사이버 보안 참조 모델 (기술보고서)
Reference Model of Cyber Security for Information Infra-structure in HDOs (Technical Reports)

1 적용 범위

이 기술보고서는 의료기관 또는 관련기관의 사이버보안 활용가이드를 제시하였으며 가이드는 3부분으로 구성되었음. 그리고 의료관련 가이드라인인 HITRUST 9.2 중 버전 이력 부분을 추가하여 의료관련 사이버보안의 기능 개선부분을 이해할 수 있도록 하였음.
활용가이드의 3부분은 사이버보안 활동, 구현 단계, 현재수준과 목표수준으로 분류하였음.

활용가이드의 사이버보안 기능은 인프라의 사이버보안을 위한 활동, 활동에 의한 결과와 참고 정보가 포함됨. 사이버보안 기능 부분에 각 기관의 현재와 목표에 맞게 개발하기 위한 활용가이드도 포함되어 있음

사이버보안 기능을 통해 각 기관은 사이버보안의 목표를 정하고, 위험 수용수준을 측정하며 사이버보안 활동을 위한 자원 배분을 우선 순위화할 수 있도록 지원함. 사이버보안을 위한 각 단계는 각 기관의 사이버보안의 위험관리와 인프라의 운영관리의 원칙을 제공함. 이것은 각 기관의 사이버보안 목표를 달성하기 위해 우선순위 결정과 보안 활동을 지원하는 것임.

2 인용 표준

해당 사항 없음

3 용어 정의

해당 사항 없음

4 약어

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication

5 사이버보안 활용가이드

5.1 사이버보안 활용가이드 개요

활용가이드는 사이버보안 위험관리를 위한 위험기반 접근법이며 3개의 부분으로 구성되어 있음: 활용가이드의 기능, 활용가이드 구현 단계, 현재 및 목표수준 임. 활용가이드는

사이버보안 운영 이유와 사이버보안 활동 간 연결성을 강화하여 구성함. 구성요소는 아래에서 설명함

1) 활용가이드의 기능부분은 인프라의 사이버보안 활동, 요구사항 및 적용되는 참고정보의 집합임. 기능부분은 사이버보안 하위 수준에서부터 구현 및 운영에 이르기까지 기관 전체에 걸쳐 사이버보안 활동 및 결과에 대한 의사소통을 가능케 하는 산업 표준과 가이드라인 및 활동을 제시함.
   활용가이드의 사이버보안 기능은 5개로 구성되어 있으며 구성된 기능은 서로 연관을 가지고 있음 - 5개의 기능은 식별(identify), 보호(protect), 탐지(detect), 응답(respond), 회복(recover) 임. 기능은 위험관리 생태계관점으로 분류하였음.
   사이버보안 기능은 각 기능별 주요 항목 및 하위항목으로 되어 있음. 또한, 각 하위항목에 관련된 사이버 보안표준과 가이드라인 등 참고 정보가 포함되어 있음

2) 사이버보안 구현 단계("단계")는 사이버보안 위험에 대해 기관의 관점과 위험의 운영관리를 위한 단계별 프로세스를 제시함 각 단계는 기관의 사이버보안 위험관리 활동을 활용가이드에서 정의한 기준에 의해 비교함 (예: 위험 및 위협 인식 단계, 부분적, 반복적, 적용적) 사이버 수준 단계는 부분적(1단계)에서 적용적(4단계)으로 사이버보안 활동을 분류함. 이러한 단계는 비공식적이고 위험에 의한 반응적인 응답(하위단계)에서 민첩하고 체계적이며 적용이 수행된 위험 기반 접근법으로의 전환을 유도함. 단계 수준의 목표는 기관은 현행 위험 관리 활동, 위협 환경, 법적 및 규제적 요구사항, 경영/사업 목표 및 한계점을 고려해야 함

3) 활용가이드 현재 및 목표수준은 기관이 선정한 사이버보안 운영 결과를 나타냄. 현황 수준 및 목표 수준은 구현 시나리오에서 활용가이드 5개 기능에 대한 표준, 프로세스 및 활동에 의한 보안 상태에 따라 결정됨. 수준은 "현재"와 ("현재 상태")와 "목표" ("달성" 상태)을 비교함. 사이버보안 수준을 평가하기 위해 기관은 모든 항목 및 하위항목을 검토할 수 있으며 보안 운영의 필요성 및 위험 평가에 기반하여 현재 수준과 목표 수준을 결정할 수 있음; 기관은 사이버보안 위험을 다루기 위해 필요한 항목 및 하위항목을 추가할 수 있음. 현재 수준("현재 상태")은 비용-효과성 및 혁신, 보안 운영 요구사항을 고려하여 구축을 위한 우선순위를 결정하고 목표 수준을 결정하는데 사용될 수 있음. 현재 및 목표 수준은 자가 평가 및 기관의 내외부적인 의사소통을 지원하는데 사용될 수 있음

5.2 위험 관리 및 사이버보안 활용가이드

위험 관리는 위험에 대한 식별, 평가 및 응답의 현재 진행 중인 프로세스를 나타냄. 위험을 관리하기 위해서 기관은 사이버보안 사건이 발생할 가능성과 잠재적인 영향에 대하여 인지해야 함. 이러한 정보를 가지고 기관은 사이버보안의 수용 가능한 목표 수준을 결정할 수 있으며 이를 위험 수용도로 표현할 수 있음.
위험 수용도에 대한 이해를 기반으로 기관은 사이버보안 운영에 대해 정량적인 평가로 사이버보안 구축 및 운영에 대해 우선 순위를 정할 수 있음. 위험관리 활용 가이드라인

으로 기관은 사이버보안 프로세스의 정량화를 가능하게 함. 기관은 인프라 운영시 잠재적인 영향에 따라 위험 완화, 위험 전송, 위험 회피 혹은 위험수용과 같이 여러 방법으로 위험을 해결할 수 있음.
활용가이드는 기관이 사이버보안에 대해 공지하고 우선 순위화 하여 구축할 수 있도록 위험관리 프로세스를 제공함. 기관에 요구되는 결과를 반영한 사이버보안 활동의 목표 선정은 반복된 위험 평가 및 사이버보안 운영으로 검증할 수 있음. 이에, 활용가이드는 IT 및 사이버보안 환경 내 위험관리의 개선을 능동적으로 설정할 수 있는 정보를 제공함.

활용가이드는 다양한 범위의 사이버보안 위험 관리 프로세스에 적용될 수 있도록 표준의 예제들을 제시하였음. 예제는 ISO 31000:2009, ISO/IEC 27005:2011, NIST SP 800-39 및 RMP 가이드라인 등에 있으며 HITRUST 의 버전 변경 히스토리를 추가하였음.

본 문서는 다음의 부분 및 부속서를 포함함:

1) 5장에서는 활용가이드 구성요소인 기능, 구현단계 및 현재 수준과 목표수준을 설명하였고, HITRUST 의 버전 변경 이력을 설명함,
2) 6장에서는 활용가이드 사용 예제를 제시함
3) 7장에서는 사이버보안 자가평가 및 증명을 위한 활용가이드 사용방법을 설명함.
4) 부록 1은 표 형식으로 프레임워크 기능을 제시함: 기능, 항목, 하위항목 및 참고정보 수록
5) 부록 2 국내 의료에 관한 법률과 HIPAA 기준과의 매핑 수록
6) 부록 3 국내 EMR 인증 기준 중, 정보보호에 관한 사항의 초기버전 수록

HITRUST 변경이력

버전	변경사항/설명		저자	게시일자
1.0	초판의 최종 버전		HITRUST	2009년 9월 11일
2.0	◦NIST SP 800-53 r2 ◦PCI-DSS v1.2 ◦HITECH ◦ISO/IEC 27002 Rework	- 미국 국립표준기술연구소(NIST) 보안 및 보호에 관한 문건 도입 - 신용카드 데이터 보안기준 - 미국 EHR인센티브제도의 보안기능 도입 - 보안포준 도입	HITRUST	2010년 1월 12일
2.1	◦(State of Mass.) 201 CMR 17.00	-메사추세츠 거주자에 대한 개인정보 저장과 사용에 관한 규약 도입	HITRUST	2010년 3월 1일
2.2	◦Cloud Security Alliance Controls Matrix v1.0	-의료기관 인증, 클라우드 보안에 관한 내용 추가	HITRUST	2010년 9월 10일

	◦Joint Commission (formerly JCAHO) Information Management State of Nevada (NRS 603A)	-개인정보 보호에 관한 네바다주 법령 도입		
3.0	◦CMS IS ARS v1-Appendix A (HIGH)	-CMS(Centers for Medicare & Medicaid Services)의 리스크 세이프가드의 보안 정보	HITRUST	2010년 12월 1일
3.1	◦PCI-DSS v2.0	-신용카드 데이터 보안기준	HITRUST	2011년 8월 4일
4.0	◦ NIST SP 800-53 r3 ◦ HIE WG Recommendations ◦ NIST-ISO-HIPAA Harmonization	-NIST 문건 도입 -Health Information Exchange 워킹그룹의 조언 -NIST문건과 의료에 관한 정보보호 및 보안에 관한 규정과의 협업	HITRUST	2011년 12월 28일
5.0	◦NIST SP 800-53 R4 (Feb 2012 IPD) ◦HITECH (MU Stage 2) ◦CAQH Committee on Operating Rules for Information Exchange (CORE) ◦NIST-CMS Harmonization Implementation Requirement Harmonization for HITRUST CSF 2013 Certification-required Controls	-NIST의 문건 보안제어 및 평가절차 도입 -HITECH EHR인센티브 프로그램의 사용요구사항 -CAQH 코어: 헬스케어의 비즈니스 운영 규칙 - NIST 문건과 HITRUST CSF 2013과의 협업에 의한 인증 요구사항	HITRUST	2013년 1월 28일
6.0	◦NIST SP 800-53 R4 (Apr 2013 Final) ◦CMS IS ARS v1.5 (2012)	-NIST SP 800-53에 의한 변경 -CMS 에 의한 변경 - 텍사스 행정법으로서 건강 정보의 전자 교환 및 표준	HITRUST	2014년 2월 12일

	◦Title 1 TX Admin. Code 390.2 (TX Standards), including privacy requirements to support TX certification of the HIPAA Privacy Rule ◦NIST-CMS Harmonization (Publication Updates) NIST-CMS 업데이트	에 관한 규정, HIPAA 요구사항 지원 - NIST CMS(세이프가드 보안정보) 업데이트		
6.1	◦PCI-DSS v3.0 ◦HIPAA Omnibus Rule ◦NIST Cybersecurity Framework v1 ◦ISO/IEC 27001:2013 ◦ISO/IEC 27002:2013	- PCI 업데이트 - HIPAA(Health Insurance Portability and Accountability Act) 의 개인정보 보호 및 보안에 관한 시행규칙 룰 도입 -NIST 의 사이버보안 프레임워크 v1 도입 - 표준 정보보안 경영시스템 및 보안기술 도입	HITRUST	2014년 4월 25일
7.0	◦CMS IS ARS v2 (2013) ◦HIPAA Omnibus Rule (Rework - Updated Category 13 - Privacy Practices) ◦NIST SP 800-53 R4 Appendix J ◦MARS-E v1.0 ◦IRS Pub 1075 (2014)	- CMS 업데이트 - HIPAA 의 업데이트 룰 도입 - NIST 문건 도입 - MARS-E는 환자보호 및 치료법의 지원을 위해 IT시스템의 구축과 운영에 과한 보안지침을 제공함 - 미국 정보기관과 에이전트의 연방조세정보를 보호하기 위한 지침 제공	HITRUST	2015년 1월 31일
8.0	◦AICPA Trust Services Principles & Criteria for	-회계서비스 제공에 대한 보안지침 제공	HITRUST	2016년 6월 30일

	Security, Confidentiality & Availability ◦HITRUST De-Identification Framework v1 ◦PCI DSS v3.1 ◦CSA CCM v3.0.1 ◦CIS CSC v6 ◦PMI DSP Principles & Framework v1 Authoritative Source Mappings to the Individual HITRUST CSF Implementation Specification (Available in MyCSF)	- HITRUST 의 익명화 프레임워크 도입 - PCI 업데이트 - CSA 클라우드 보안 규칙 업데이트₩ - CIS의 보안 제어 도입 - PMI 프레임 워크와 HITRUST CSF 의 구현사양과의 소스매핑 (MyCSF 에서 사용가능)		
8.1	◦AICPA Trust Services Principles & Criteria for Security, Confidentiality & Availability (2016 updates) ◦PCI DSS v3.2 ◦MARS-E v2	-회계서비스 제공에 대한 보안지침 업데이트 - PCI 업데이트 - MARS-E 업데이트	HITRUST	2016년 2월 4일
9.0	◦DHS CRR ◦EHNAC (Additional Requirements to Support EHNAC Accreditation Assessments) ◦Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures (Added Electronic Records) FedRAMP ◦FFIEC IT Examination Handbook -	DHS(The Department of Homeland Security, 국가안보부)는 CRR(Cyber Resilience Review, 사이버 복구 리뷰) 반영 - NIST 문건 (패스워드 요구사항)업데이트 반영 - HIPAA 보안 요구사항 반영	HITRUST	2017년 9월 8일

	Information Security, Sep 2016 ◦NIST SP 800-63B (Updated Password Requirements in Advance of NIST SP 800-53 r5) ◦OCR Audit Protocol Phase II (Clarification of HIPAA Security Requirements)			
9.1	◦European Union GDPR (General Data Protection Regulation) ◦Title 23 NYCRR 500 (New York Department of Financial Services)	-유럽의 일반 데이터 보호 규정 반영 - 뉴욕 금융서비스 반영	HITRUST	
9.2	◦Category 13 restructure (Language to reflect general privacy) ◦EU GDPR Control plain-language requirements ◦HIPAA/Healthcare requirements moved to separate industry segment ◦Singapore Personal Data Protection Act (PDPA)	-13개 카타고리 재구성(개인정보에 관한 언어영향 반영) - 유럽 GDPR 제어 요구사항반영 - HIPAA의 헬스케어 요구사항 분류 및 이동 - 싱가포르의 개인정보 보호법 반영	HITRUST	2019년 1월

6 활용가이드 기본사항

6.1 활용가이드 기능

활용가이드의 기능은 사이버보안 목표를 달성하기 위한 활동의 집합이며 목표달성을 위한 참고 예제를 포함하고 있음. 기능은 실행해야 할 활동에 대한 목록이 아니라 산업계에서 사이버보안 위험관리에 유용하다고 분류한 사이버보안 목표를 나타낸 것임. 기능은 그림6-1에서와 같이 4가지 요소로 구성되어 있음: 기능, 항목, 하위항목 및 참고 정보임. 자세한 사항은 부록1에 표기함

프레임워크 기능		항목	하위항목	참고 정보
	식별 ID			
	보호 PR	항목	하위항목	참고 정보
	탐지 DE	항목	하위항목	참고 정보
	응답 RS	항목	하위항목	참고 정보
	복구 RC	항목	하위항목	참고 정보

(그림 6-1) 활용가이드의 기능 구조

활용가이드 기능은 다음과 같이 적용함:

1) 기능은 상위 수준에서 사이버보안 활동을 분류함. 기능은 식별, 보호, 탐지, 응답 및 복구임. 이것은 위험 관리를 위한 정보의 분류와 판단, 사이버 보안의 위험관리를 위한 생태계의 기능을 나타냄. 또한, 기능은 사이버 보안 이벤트 관리에 방법과 투자대비 효과를 알 수 있음.
2) 예를 들어, 계획 및 활동에 대한 투자는 적절한 응답 및 복구 활동을 도우며 서비스 제공에 미치는 영향을 최소화 시킴.
3) 항목은 기능의 하위항목으로 수요 및 특정 활동에 긴밀한 연관이 있는 사이버보

안 결과 집합임. 항목의 예제는 “자원 관리”, “신원 관리 및 접근통제”와 “탐지 프로세스”가 있음.

4) 하위항목은 항목을 추가적으로 기술적 및 관리 활동의 구체적인 목표로 분류함. 이것은 포괄적이지 않지만 각 항목 내 목표 지원을 위한 정보를 제공함. 하위항목의 예제는 “외부 정보시스템은 내부와 분류되어 있다”, “레스트 상태의 데이터가 보호되고 있다”와 “탐지시스템은 공지는 확인하고 있다. ”.등 임.
5) 참고 정보는 각 하위항목과 연관된 목표를 달성하는 방법을 명시하는 주요 인프라 분야 의 표준, 가이드라인 및 활동에 대한 구체적인 정보임. 활용가이드 기능에 제시된 참고 정보는 설명적임. 이것은 활용가이드를 개발하는 동안 참고되었던 정보임.

5개의 활용가이드 기능은 아래와 같이 명시되어 있음. 이러한 기능은 순차적으로 구축하는 것을 제안하지 않음. 각 기능은 동적인 사이버보안 위험관리를 위해 구축하고 동시적, 연속적으로 운영할 수 있음. 활용가이드 기능 목록은 부록 1 에 나타냄.

1) 식별 – 시스템, 자원, 데이터 및 저장공간에 대한 사이버보안 위험을 관리하기 위한 기능
   식별 기능의 활동들은 프레임워크의 효과적인 사용을 위한 것임. 보안 운영, 주요 기능을 지원하는 자원 및 관련 사이버보안 위험에 대한 이해는 기관으로 하여금 위험 관리 전략 및 보안운영 요구사항에 의해 우선순위를 정하도록 함. 이 기능에서의 결과항목 예제는 다음을 포함함: 자원 관리; 운영환경; 정책; 위험 평가 및 위험 관리 전략임.
2) 보호 – 주요 인프라 서비스 제공을 보장하기 위한 적절한 보호조치 개발 및 구현에 대한 기능
   보호 기능은 잠재적인 사이버보안 이벤트의 영향을 제한하거나 방지하는 기능임. 이 기능 목표 항목의 예제는 다음과 같음. : 식별 관리 및 접근 통제; 인식 및 훈련; 데이터 보안; 정보 보호 프로세스 및 절차; 유지보수 및 보호적 기술임
3) 탐지 – 사이버보안 위험 발생을 식별하는 적절한 활동 개발 및 구현
   탐지 기능은 사이버보안 위험 발견을 가능하게 함. 이 기능의 결과 항목 예제는 다음을 포함함: 비정상 및 이벤트; 연속적 보안 모니터링 및 탐지 프로세스.
4) 응답 – 탐지된 사이버보안 이벤트에 관하여 행동을 취하기 위한 적절한 활동 개발 및 구현
   응답 기능은 잠재적인 사이버보안 이벤트의 영향을 방지하는 기능을 지원함. 이 기능의 항목에 대한 예제는 다음과 같음: 응답; 의사소통; 분석; 위험 완화 및 빠른 응답, 등
5) 복구 – 복구 계획 유지 및 사이버보안 이벤트로 인해 손상된 기능 혹은 서비스를 복구하기 위한 활동 개발 및 구현
   복구 기능은 사이버보안 이벤트로부터 영향을 최소화하기 위한 운영을 지원함. 이 기능의 목표 항목 예제는 다음을 포함함: 복구 계획; 개선 및 의사소통.

6.2 활용가이드 구현단계

활용가이드 구현 단계(이하 “단계”)는 기관의 사이버보안 위험 관리에 대한 정량적인 수행 단계를 제공함. 위험관리 단계는 부분적(1단계)에서부터 적용적(4단계)까지로 구성됨. 각 단계는 사이버보안 위험관리 활동 영역의 증가에 따라 분류함. 위험관리 요구사항에 의해 기관은 종합적인 위험 관리 활동을 결정할 수 있음. 위험 관리를 위한 요구사항은 개인정보 보호 및 보안 등 기관의 사이버보안 위험 대응의 종합적인 관리를 의미함.

각 단계의 결정은 기관의 현재 위험 관리 활동, 위협 환경, 법률적 및 규제적 요구사항, 정보 공유 활동, 비즈니스/사업 목표, 관련 기관의 사이버보안 요구사항 및 기관적 한계점을 고려해야 함.
기관은 현재의 수준을 파악하고 기관이 사이버보안 위험을 기관이 수용 가능할 정도로 감소시키고 자원을 효율적으로 관리하는 수준으로 목표 단계를 결정해야 함. 기관은 목표 단계를 결정할 때 사이버보안 관련 연방정부, 정보 공유 및 분석 센터(ISAC), 정보 공유 및 분석기관(ISAO) 및 기존의 성숙도 모델 또는 외부 조언을 활용해야 함.

1단계(부분적)로 확인된 기관은 2단계 혹은 그 이상의 단계로 이동하는 것이 권장되지만, 단계 자체가 성숙도를 의미하지 않음. 단계는 사이버보안 위험 관리 및 우선순위를 결정하는데 도움을 줌. 높은 단계의 구축은 비용대비 효과를 나타나고 비용대비 효과가 정량적, 정성적 분석이 가능할 때 권장함.

활용가이드를 이용한 성공적인 구현은 단계 결정이 아니라, 기관의 목표 수준에 명시된 활동을 달성하는 것임. 단계 선정 및 목표는 활용가이드의 현황 및 목표수준에 영향을 줌. 비즈니스/프로세스의 수준은 운영진이 선정한 단계이며 승인된 수준은 기관 내 사이버보안 위험 관리방안에 대한 종합적인 수준을 설정하는 데 도움을 되며 목표 프로필과의 차이점은 개선 활동에서 우선순위를 정하는 데 영향을 줌.

단계에 대한 정의는 다음과 같음:

1단계: 부분적

1) 위험 관리 프로세스 – 기관의 사이버보안 위험 관리 활동은 공식화되지 않았으며 위험은 임시적이거나 종종 반응하는 방법으로 관리된다. 사이버보안 활동의 우선순위화는 기관적 위험 목표, 위협 환경 및 비즈니스/미션 요구사항이 직접적으로 반영이 되지 않을 수 있음
2) 통합 위험 관리 프로그램 – 기관의 수준에서 사이버보안 위험에 대해 제한적인 인식이 있으며 사이버보안 위험을 관리하는 것에 있어서 전사 차원의 접근법이 구축되지 않음. 기관은 외부 출처로부터 수집되는 다양한 경험 혹은 정보로 인하여 비정기적으로, 사례 기반 별로 사이버보안 위험 관리를 실행함. 기관은 기관 내에서 사이버보안 정보가 공유될 수 있도록 하는 프로세스를 보유하고 있지 않을 수 있음.

3) 외부 참여 - 기관은 의존 기관 혹은 의존하는 기관과 연관된 넓은 범위의 생태계 내 역할을 이해하지 않음. 기관은 협력하지 않으며 다른 기관(예: 구매업체, 공급업체, 용역업체, 정보 공유 및 분석 기관, 연구자, 정부)으로부터 정보(예: 위협 지식, 대표활동, 기술)를 받지 않으며 공유하지 않음. 기관은 일반적으로 제공하거나 사용하는 제품 및 서비스의 사이버 공급체인 위험에 대해 인식하지 않음.

2단계: 위험 정보 활용

1) 위험 관리 프로세스 - 위험 관리 활동은 관리에 의해 승인되었지만 전사 차원의 정책으로 수립되지 않을 수도 있음. 사이버보안 활동의 우선 순위화에 기관적 위험 목표, 위협 환경 혹은 비즈니스/미션 요구사항이 직접적으로 반영됨.
2) 통합 위험 관리 프로그램 - 기관 수준에서의 사이버보안 위험 인식은 있지만 사이버보안 위험을 관리하는 전사 차원의 접근법은 수립되지 않았다. 위험 정보를 활용하고 관리가 승인된 프로세스 및 절차는 정의되어 실행 중이며 운영자는 그들의 사이버보안 책무를 진행하는데 필요한 충분한 자원을 가지고 있음. 사이버보안 정보는 비공식적으로 기관 내에서 공유됨.
3) 외부 참여 - 일반적으로 기관은 관련기관과 업무 프로세스 역할에 대해 이해하고 있음. 기관은 다른 기관과 협력하고 정보를 받으며 고유의 정보를 생산하지만 다른 기관과 공유를 하지 않을 수 있음. 추가적으로, 기관은 제품 제공 및 서비스와 연관된 사이버 보안 위험에 대해 인식하고 있지만 일관성 있거나 공식적으로 위험에 대해 대응 하지 않음.

3단계: 반복적

1) 위험 관리 프로세스 - 기관의 위험 관리 활동은 공식적으로 승인되어 정책으로 표현됨. 기관의 사이버보안 활동은 정기적 경영관리에 따른 변경, 위협 및 기술에 따라 위험 관리 절차가 변경됨
2) 통합 위험 관리 프로그램 - 전사 차원의 사이버보안 위험을 관리하는 규정이 존재함. 위험에 관한 정책, 절차가 정의되어 있고 운영에 대한 검토가 진행되고 있음. 위험에 대해 효과적으로 응답하기 위한 방법이 존재함. 사이버보안 관리 인력은 부여된 역할 및 책임을 수행하기 위해 지식과 기술을 보유하고 있음.
3) 외부 참여 - 기관은 외부참여 기관에 대해 알고 있으며 기관의 넓은 범위의 생태계 내 역할과 의존성에 대해 이해하고 있어 기관의 위험 관리에 기여하고 있음. 기관은 다른 기관과 협력하여 정보를 주고 받으며 이것은 내부에서 생산된 정보를 보완하는 것이며 다른 기관과 정보를 공유함. 기관은 제공하거나 사용하는 제품 및 서비스와 연관된 사이버 공급체인 위험에 대해 인식하고 있음. 추가적으로, 기관은 기본적 요구사항, 거버넌스 구조(예: 위험 위원회)와 정책 구현 및 모니터링에 대한 의사소통을 하기 위한 서면 동의서와 같은 매커니즘을 포함하여 공식적으로 위험에 대해 대응함.

4단계: 적용적

1) 위험 관리 프로세스 – 기관은 사이버보안활동에 따라 얻은 교훈에 기반하여 이전과 현재의 사이버보안 활동에 의해 생성된 예측 지표를 적용함. 고도화된 사이버보안 기술 및 활동을 활용하여 복잡한 위협에 대해 진화되고 연속적인 절차를 통해 기관은 복잡한 사이버보안 상황에 적극적으로 대응함.
2) 통합 위험 관리 프로그램 – 잠재적인 사이버보안 위협을 다루기 위하여 위험 관련 정책, 절차 및 과정을 전사 차원의 접근법으로 관리하고 있음. 사이버보안 위험 관리는 기관 문화의 일부분이며 이전 활동에 대한 인지, 다른 자원으로부터 공유된 정보 및 기관의 시스템과 네트워크에서의 활동에 관한 지속적인 인지(지식)으로부터 진화됨.
3) 외부 참여 – 기관은 넓은 범위의 생태계 내 역할을 수행하며 생태계 내 외부참여의에 대해 이해함. 외부참여는 사이버보안 위협에 기여할 수 있음. 기관은 위협과 기술 상황이 진화함에 따라 위험에 대한 연속적인 분석내용을 알려주며 우선순위화된 정보를 받고, 생성하며 검토함. 기관은 다른 협력기관과 내외부적으로 정보를 공유함. 기관은 제공하거나 사용하는 제품 및 서비스와 연관된 온라인 공급 기관의 위험을 이해하고 일관성 있는 대응을 위해 실시간 혹은 일정시간 간격으로 사이버정보를 수집하여 사용함. 추가적으로, 기관은 외부 참여기관과의 관계를 구축하고 유지하기 위하여 공식(예: 계약서), 비공식적인 채널을 사용하여 적극적으로 의사소통을 함.

6.3 프레임워크 프로필

프레임워크 프로필(“프로필”)은 기관의 경영 요구사항, 위험 수용성 및 자원에 대하여 기능, 항목 및 하위항목들의 부합화 임. 프로필은 기관적, 분야적 목표를 잘 부합하며 법률적/규제적 요구사항 및 산업 대표 활동을 고려하고 위험 관리 우선순위를 반영하는 사이버보안 위험 감소를 위한 로드맵을 수립하는 것을 가능하게 함. 다수 기관의 복잡성을 고려하였을 때, 기관은 각 개인의 니즈를 인식하고 특정 구성요소와 부합하는 여러 개의 프로필을 선택할 수 있음.

프레임워크 프로필은 현재 상태 혹은 특정 사이버보안 활동의 목표 상태를 설명하는데 사용될 수 있음. 현재 프로필은 현재 달성하려고 하는 사이버보안 결과를 나타냄. 목표 프로필은 목표 사이버보안 위험 관리 목표를 달성하기 위해 필요한 결과를 나타냄. 프로필은 사업/미션 요구사항을 지원하며 기관 내외부적으로 위험에 대한 의사소통을 도모함. 본 프레임워크 문서는 구현에서 유연성을 인정하기에 프로필 양식에 대해 규정하지 않음.

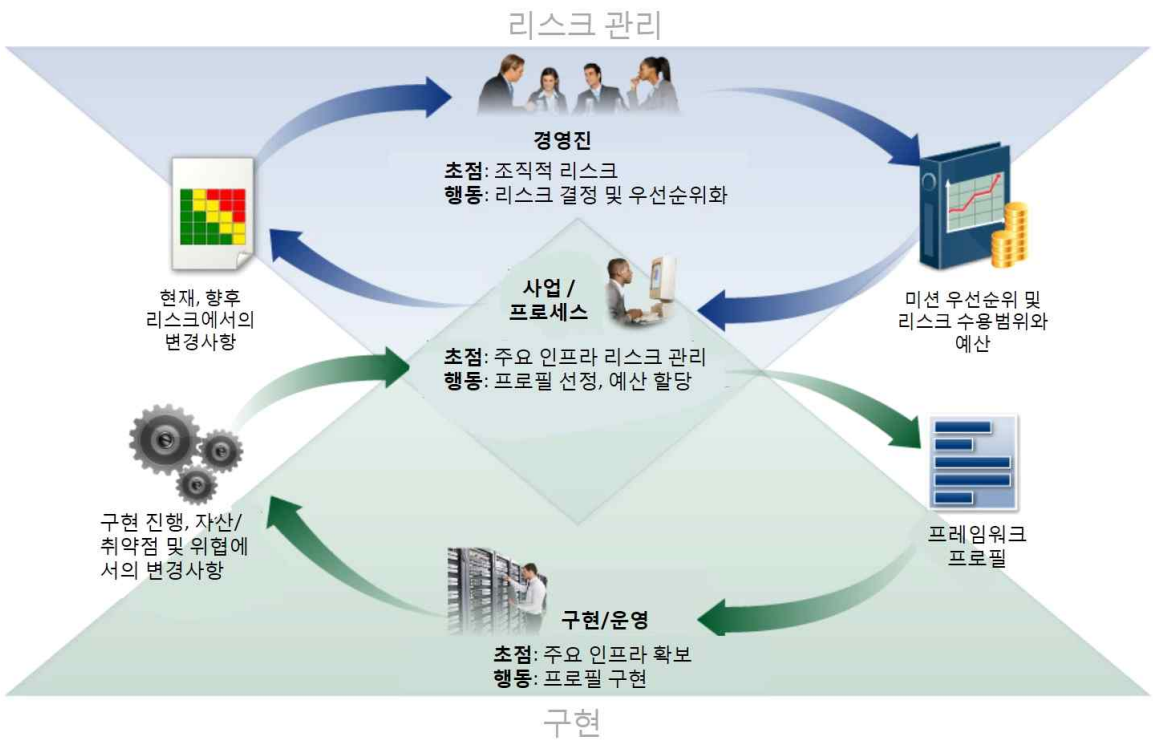
프로필의 비교(예: 현재 프로필 및 목표 프로필)는 사이버보안 위험 관리 목표를 충족하기 위해 다루어야 할 차이를 보여줌. 이러한 차이를 다루기 위한 활동 계획은 앞서 명시되었던 로드맵에 의함. 차이의 완화에 대한 우선 순위화는 기관의 비즈니스 니즈 및 위험 관리 프로세스에 기반하여 진행됨. 이러한 위험 기반 접근법은 기관으로 하여금 사이

버보안 목표를 비용 효과적이고 우선 순위화된 방법으로 달성하기 위해 필요한 자원에 대한 추정치(예: 스태프, 자금)를 판단할 수 있도록 함. 프레임워크는 특정 하위항목의 적용성 및 충족이 프로필 적용범위에 따라 상이한 위험 기반 접근법임.

그림 6-2는 기관 내 정보의 일반적인 흐름 및 각각의 수준에서 의사결정을 설명하고 있음:

1) 경영진
2) 사업/프로세스
3) 구현/운영

경영진은 사업/프로세스 차원에서 목표 우선순위, 사용자 참석 및 종합적인 위험 수용성에 대해 의사소통을 함. 사업/프로세스 차원은 위험 관리 프로세스에 정보를 입력으로 사용하며 비즈니스 니즈에 대한 의사소통 및 프로필을 생성하기 위해 구현/운영 차원과 협업함. 구현/운영 차원은 프로필 구현 진행사항에 관하여 사업/프로세스 차원과 의사소통을 함. 사업/프로세스 수준은 영향 평가를 실행하기 위하여 이러한 정보를 사용함. 사업/프로세스 차원에서의 관리는 기관의 종합적인 위험 관리 프로세스에 활용하기 위하여 영향 평가 결과를 경영진에 보고하며 사업 영향에 대한 인식을 위해서 구현/운영 차원에 보고함.



(그림 6-2) 기관 내 개념적 정보 및 결정 흐름도

7. 프레임워크 사용방법

7.1 사이버보안 활동에 대한 기본적 검토

프레임워크는 기관의 현재 사이버보안 활동과 프레임워크 코어에 정리되어 있는 활동을 비교하는데 사용될 수 있음. 현재 프로필 생성을 통해 기관은 5개 수준의 기능(식별, 보호, 탐지, 응답 및 회복)과 부합되어 코어 항목 및 하위항목에 명시된 결과를 달성한 수준을 검토할 수 있음. 기관은 목표 결과를 이미 달성하였다는 것을 발견할 수도 있으며 알려진 위험으로 완벽하게 사이버보안을 관리할 수 있음. 반대로, 기관은 향상 될(되어야 할) 기회가 있다는 것을 결정할 수 있음 기관은 기존 사이버보안 활동을 강화하기 위한 행동 계획 개발 및 사이버보안 위험 감소를 위해 프로필 정보를 사용할 수 있음. 또한, 기관은 특정 목표를 달성하는 것에 있어서 과다하게 투자하고 있다는 점을 발견할 수도 있음. 기관은 이러한 정보를 이용하여 우선순위를 재조정할 수 있음.

5개 수준의 기능이 위험 관리 프로세스를 대체하지는 않지만, 이러한 기능들은 고위 경영진 및 기타 이해관계자들에게 사이버보안 위험의 근본적인 개념을 이해시키기 위해 간결한 방법을 제공함. 제공되는 정보는 식별된 위험이 어떻게 관리되는지, 또 기관이 기존의 사이버보안 표준과 가이드라인 및 활동에 대하여 개념적 차원에서 어떻게 해석되는지 이해시켜 현재수준을 평가할 수 있도록 함. 또한, 프레임워크는 “우리가 어떻게 하고 있는가”를 포함하여 근본적인 질문에 대해 대답할 수 있도록 하며 이러한 질문들은 장소 및 시기적으로 적절하게 사이버보안 활동을 강화하는데 좀 더 정보를 활용한 방법으로 이동할 수 있게 함.

7.2 사이버보안 프로그램의 구축 혹은 개선

기관이 새로운 사이버보안 프로그램 구축 혹은 기존 프로그램을 개선하는데 프레임워크를 어떠한 방법으로 사용할 수 있는 지에 대해 설명함. 각 단계들은 지속적으로 사이버보안을 개선하기 위해 필요한 만큼 반복되어야 함.

1단계: 우선순위화 및 범위

사이버보안 목표 및 고 수준의 우선순위가 분류됨. 기관은 분류된 정보를 가지고 사이버보안 구현에 관한 전략적 결정을 하며 선정한 비즈니스 프로세스를 지원하는 시스템 및 자원의 범위를 결정함. 프레임워크는 다른 비즈니스 니즈 및 연관 위험 수용성을 가질 수 있는 기관 내 상이한 비즈니스 라인 혹은 프로세스를 지원할 수 있음.

2단계: 방향성 설정

사이버보안 프로그램의 범위가 비즈니스 라인 혹은 프로세스에 맞게 결정된 후, 기관은 관련 시스템 및 자원, 규제적 요구사항과 종합적인 위험 접근법을 식별한다. 기관은 이러

한 시스템 및 자원에 대한 위협 및 취약점들을 식별한다.

3단계: 현재 프로필 생성

기관은 프레임워크 코어 중 항목과 하위항목 결과가 현재 얼마만큼 달성되고 있는 지를 표시하고 현재 프로필을 생성함.

4단계: 위험 평가 실행

이 평가는 기관의 종합적인 위험 관리 프로세스 혹은 이전 위험 평가 활동으로 결정됨. 기관은 사이버보안 이벤트의 가능성 및 이벤트가 기관에게 미칠 영향을 판별하기 위해 보안 운영 환경을 분석함. 기관이 사이버보안 이벤트의 가능성 및 영향에 대해 인지하기 위해 발생하는 위험, 위협 및 취약점 데이터를 활용함.

5단계: 목표 프로필 수립

기관은 사이버보안 목표를 정량적으로 설명하기 위해 프레임워크 항목 및 하위항목에 의해 목표 프로필을 생성함. 기관은 고유한 기관의 위험을 설명하기 위해 추가적인 항목 및 하위항목을 개발할 수 있음. 기관은 목표 프로필 생성 시 관련 기관, 고객 및 비즈니스 파트너와 같이 외부 이해관계자들의 범위와 요구사항을 고려해야 할 수 있음.

6단계: 공백부분 결정, 분석 및 우선순위화 하기

기관은 현재와 목표의 간극을 확인하기 위하여 현재 프로필과 목표 프로필을 비교함. . 다음은 목표 프로필에서의 결과를 달성하기 위한 동인, 비용/효과 분석 및 위험에 대한 이해에 기반 한 간극부분을 다루는 우선 순위화된 활동계획을 수립함. 기관은 목표 프로필을 달성하기 위해 필수적인 자원을 결정함. 이러한 방법으로 프로필을 사용하는 것은 기관으로 하여금 사이버보안 활동에 대해 정보에 의한 결정이 가능하게 함. 그리고 효과적인 위험 관리와 비용 지원으로 목표까지 도달하는 것을 가능하게 함.

7단계: 활동 계획 실행하기

기관은 이전 단계에서 식별된 간극 부분에 대해 어떤 활동을 진행할지 결정함. 목표 프로필과 비교하여 현재 사이버보안 활동을 모니터링 함. 추가적인 가이드로써 프레임워크는 항목과 하위항목에 관한 참고적 정보 예제를 제공하며 기관은 특화된 영역을 포함한 표준, 가이드라인 등을 보고 기관의 니즈에 맞는 것을 선택함.

기관은 사이버보안을 연속적으로 평가하고 개선하기 위해 필요한 만큼 단계를 반복할 수 있음. 예를 들어, 기관은 목표하는 단계에서 빈번한 반복 수행이 위험 평가의 품질을 향상시킬 수 있음. 기관은 현재 프로필에 대한 반복적인 업데이트를 통하여 진행상황을 모니터링 할 수 있으며 목표 프로필과 현재 프로필을 비교할 수 있음. 기관은 그들의 사이버보안 프로그램을 목표 프레임워크 구현 단계와 부합하여 위험 평가 프로세스로 활용할 수 있음.

7.3 이해관계자들과의 사이버보안 요구사항에 대한 의사소통

프레임워크는 기본적으로 주요 인프라 서비스 제공을 담당하고 있는 이해관계자들 간의 의사소통을 위해 일반적인 언어로 프레임워크를 제안함. 예제는 다음을 포함함:

1) 기관은 외부 서비스 제공자 (예: 데이터를 내보내는 클라우드 제공자)에게 사이버 보안 위험 관리 요구사항을 표현하기 위하여 목표 프로필을 활용할 수 있음.
2) 기관은 결과를 보고하거나 수집된 요구사항을 비교하기 위하여 현재 프로필을 이용하여 사이버보안 상태를 표현할 수 있음.
3) 인프라에 기반을 두고 있는 외부 기관을 구분하고 주요 인프라 보유자/운영자에게 현재 보안 위험 상황을 전달하기 위해 현재 프로필을 사용할 수 있음.
4) 주요 인프라는 목표 프로필을 구축하기 위하여 구성원 간 현재 프로필을 사용하여 목표 프로필을 구축할 수 있음.
5) 기관은 구현 단계를 사용하여 주요 인프라와 보안 단계에 대한 평가를 통해 이해관계자 간 사이버보안 위험을 관리 할 수 있음.

의사소통은 공급 체인 내 이해관계자들 간 특히 중요함. 공급 체인은 기관 내 여러 수준의 복잡하고 광범위하게 연결되어 있는 자원 및 프로세스의 집합임. 공급 체인은 구성 및 기능 등 다양한 자원으로부터 시작되며 설계, 개발, 제조, 공정, 처리 및 최종 사용자에게 제품 및 서비스 제공으로 확장됨. 이러한 복잡한 연결 관계를 가정했을 때, 공급 체인 관리(SCRM)은 주요한 기관의 기능임.

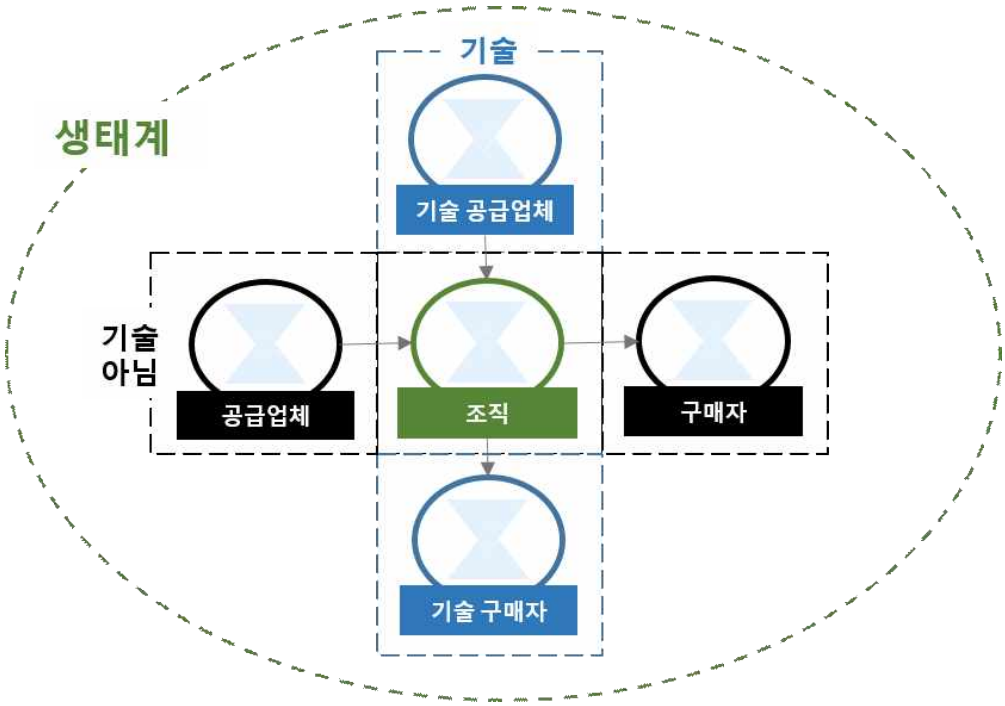
사이버 공급체인 위험 관리는 외부 관계자와 연결된 사이버보안 위험을 관리하기 위한 필수적인 활동 목록임. 구체적으로, 사이버 공급체인 위험 관리는 기관이 외부 관계자에 미치는 사이버보안 영향 및 외부 관계자가 기관에 미치는 사이버보안 영향 둘 다를 모두 포함함.

사이버 공급체인 위험 관리의 주요 목표는 잠재적인 악성 기능을 포함하는 “제품 및 서비스”, 사기 “제품 및 서비스” 및 사이버 공급 체인 내 낮은 수준의 제조 및 개발 활동로 인한 취약적인 “제품 및 서비스”를 식별, 평가 및 완화하기 위함에 있음. 사이버 공급체인 위험 관리 활동은 다음을 포함함:

1) 공급업체에 대한 사이버보안 요구사항 결정
2) 공식 합의를 통한 사이버보안 요구사항 실행(예: 계약)
3) 사이버보안 요구사항의 검증 및 유효성 확인 방법에 대해 공급업체를 대상으로 의사소통
4) 사이버보안 요구사항이 다양한 평가 방법에 의해 충족되었다는 검증
5) 위의 활동에 대한 감독 및 관리

그림 7-1에서 설명된 바와 같이, 사이버 공급체인 위험 관리는 기술 공급업체 및 구매자와 더불어 기술적인 공급업체와 구매자를 포함하며 기술은 정보기술(IT), 산업통제시스템

(ICS), 사이버물리적 시스템(CPS)와 일반적으로 사물인터넷(IoT)를 포함한 연결된 기기로 구성되어 있음. 그림 7-1은 한 시점에서의 기관을 나타냄. 하지만, 사업운영의 정상적인 과정 동안, 대다수의 기관은 다른 기관 혹은 최종 사용자와 대비하여 동시에 공급자 및 구매자가 될 수 있음.



(그림 7-1 사이버 공급체인 관계도)

그림 7-1에 묘사된 관계자들은 기관의 사이버보안 생태계를 구성함. 이러한 관계는 주요 인프라 및 폭넓은 사이버보안 위험을 다루는 것에 있어서 사이버 공급체인 관리의 주요한 역할을 강조함. 이러한 관계들 – 그들이 제공하는 제품 및 서비스 – 및 제시하는 위험은 기관의 보호적, 탐지적 기능과 더불어 기관의 응답 및 회복 프로토콜에서 식별되고 고려되어야 함.

위의 그림 7-1에서 “구매자”는 영리기업 및 비영리기업을 포함하며 기관으로부터의 제품 혹은 서비스를 소비하는 사람 혹은 기관을 지칭함. “공급업체”는 기관의 내부 목적(예: IT 인프라)로 사용되는 제품 및 서비스 제공자 또는 구매자에게 제공되는 제품 혹은 서비스로 통합되는 제품 및 서비스의 공급자를 포함함. 이러한 용어는 기술 기반 및 비기술 기반의 제품 및 서비스 모두에 적용됨.

코어의 하위 단계 또는 프로필의 종합적인 고려사항의 경우, 프레임워크는 기관 및 파트너들에게 새로운 제품 및 서비스가 주요 보안 결과를 충족하도록 지원함. 상황(예: 개인 식별정보의 전송, 미션 주요 서비스 제공, 데이터 검증 서비스, 제품 혹은 서비스 무결

성)에 적절한 결과를 먼저 선정함으로써 기관은 이러한 평가기준에 따라 파트너에 대해 평가할 수 있음. 예를 들어, 네트워크의 비정상적인 운영(OT)을 모니터링하는 시스템을 구매할 경우, 특히 가용성은 달성해야 할 중요한 사이버보안 목표이며 적용 가능한 하위 항목(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)에 대하여 기술 공급업체 평가를 진행해야 함.

7.4 구매결정

프레임워크 대상 프로필은 기관적 사이버보안 요구사항에서의 우선순위화된 목록으로, 대상 프로필은 구매 제품 및 서비스에 대한 결정을 하기 위하여 사용될 수 있음. 이러한 계약은 공급업체에 대한 사이버보안 요구사항 목록에 대해 이해관계자들 사이의 의사소통을 지원할 수 있음. 목적은 사이버보안 요구사항에 관하여 신중하게 결정된 목록을 가정할 시 여러 개의 공급업체 중 가장 좋은 구매결정을 지원함. 이는 현재와 목표 프로필에 통해 달성하고자 하는 알려진 간극을 지원하기 위한 여러 개의 제품 혹은 서비스를 비교할 수 있음.

제품 혹은 서비스를 구매한 후, 프로필은 잔여 사이버보안 위험을 추적하고 다루는 것에 사용될 수 있다. 예를 들어, 구매한 서비스 혹은 제품이 대상 프로필에서 명시된 모든 목표를 충족시키지 못했을 시, 기관은 다른 관리 조치를 통하여 잔여 위험을 다룰 수 있음. 또한 프로필은 주기적인 검토 및 시험을 통해 제품이 사이버보안 결과를 충족하는 지에 대해 평가 할 수 있음

프레임워크는 추가적인 참고적 정보가 기관에서 발생하는 니즈를 지원할 경우, 신규 혹은 개정된 표준, 가이드라인 및 활동을 구분하는데 사용될 수 있음. 주어진 항목을 구현하는 기관 혹은 새로운 항목을 개발하는 기관은 관련된 활동에 대해 참고적 정보가 있다는 것을 인지할 수 있음. 이러한 수요를 다루기 위해 기관은 표준, 가이드라인 혹은 활동을 작성하고 개발과 이해관계자(기술적 리더 및/또는 표준기구)와 협업할 수 있음.

7.5 새로운 혹은 개정된 참고적 정보에서의 활동 식별

프레임워크는 추가적인 참고 정보가 기관으로 하여금 발생하는 니즈를 다루는 것을 지원할 경우, 신규 혹은 개정된 표준, 가이드라인 또는 활동에 대한 기회를 식별하는데 사용될 수 있다. 주어진 항목을 구현하는 기관 혹은 새로운 항목을 개발하는 기관은 해당 될 시, 관련된 활동에 관하여 오로지 소수의 참고적 정보가 있다는 것을 발견할 수 있다. 이러한 수요를 다루기 위해 기관은 표준, 가이드라인 혹은 활동을 작성, 개발 및 조정하기 위해 기술적 리더 및/또는 표준기구와 협업할 수 있음.

7.6 개인정보 보호 및 보안을 위한 방법

본 항목은 사이버보안으로부터 발생할 수 있는 개인 정보보호 및 보안을 수행하기 위한 방법임. 개인정보보호 및 보안은 산업분야마다 상이할 수 있기 때문에 기관은 기술적 구현 범위에서 개인정보에 대한 고려사항 및 비즈니스 프로세스를 고려해야 함. 그러나 기존 사이버보안 프로그램의 모든 활동은 개인정보 보호 및 보안을 고려하고 있음. 기술적인 개인정보 보호 및 보안 표준, 가이드라인 및 추가적인 대표사례는 개선된 기술의 구현을 지원하기 위해 개발해야 함.

개인정보 보호 및 사이버보안은 강한 연결성을 가지고 있음. 기관은 사이버보안 활동 중 개인 정보의 수집, 처리, 사용 및 저장을 하므로 각 프로세스 따라 위협이 발생할 수 있음. 다음은 위협 발생의 예제임 : 개인정보의 과다수집 혹은 과다보유에 의한 위협; 사이버보안 활동과 관련없는 개인정보의 공개 혹은 사용; 서비스 거절 또는 유사한 사례시 위협을 발생시킬 수 있는 사이버보안 완화 활동; 사이버보안 활동을 방해하는 몇몇 유형의 사건 탐지 또는 모니터링.

정부 및 관련 기관은 사이버보안 활동으로 발생할 수 있는 개인정보 보호 및 보안에 관한 책임을 가지고 있음. 아래의 방법론에 참고되었듯이, 주요 인프라를 보유하거나 운영하는 정부 혹은 관련 기관에 적용 가능함.

사이버보안 위험의 거버넌스

1) 기관의 잠재적인 위험을 포함한 위험 대응 사이버보안의 평가는 개인정보 보호 및 보안을 고려함
2) 사이버보안의 개인 정보보호 및 보안 책임을 갖는 개개인은 관리부서에 보고하며 보안에 대해 훈련되어 있음
3) 프로세스는 적용되는 개인 정보보호 및 보안 법률 및 규정에 의한 요구사항에 맞춰 사이버보안 활동을 지원함
4) 프로세스는 이전에 언급되었던 기관적 조치 및 통제의 구현을 평가하도록 실행되고 있음

기관의 자원 및 시스템 접속을 위한 개인 식별 및 승인 방법

1) 이 단계는 개인 정보의 수집과 공개 또는 사용에 관한 것으로 접근 통제 시 개인정보보호 및 보안에 관한 영향을 고려한 활동임

보호 및 보안 인식 및 활동(교육) 방안

1) 기관의 개인정보 보호 및 보안 규정에 따라 이용 가능한 정보는 사이버보안 인력 훈련 및 인식 활동도 포함되어 있음
2) 기관에 사이버보안 서비스를 제공하는 기관은 기관에 적용되는 개인정보 보호 및

보안 규정에 대한 공지를 전달 받고 있음

비정상 활동 탐지와 시스템과 자원 모니터링

1) 프로세스는 기관의 비정상 활동 탐지 및 사이버보안 모니터링에 대해 개인정보 보호 및 보안을 절차에 따라 실행함

정보 공유 또는 다른 완화 노력을 포함한 응답 활동

1) 프로세스는 사이버보안 정보 공유 활동의 일부분으로써 개인 정보가 기관 외부로 공유되는 이유, 시점, 방법 및 수준에 대한 평가에 의해 실행중임
2) 프로세스는 기관의 사이버보안 활동 완화에 대해 개인정보 보호 및 보안 검토 실행 중임

8. 프레임워크를 활용한 사이버보안 위험 자가 평가

사이버보안 프레임워크는 기관의 사이버보안 위험관리 활동을 수행하여 위험이 감소하도록 설계됨. 이상적으로, 프레임워크를 사용하는 기관은 수용 가능한 수준으로 위험을 감소시키기 위해 수행된 비용과 위험으로부터 벗어난 이익에 대해 측정할 수 있음. 기관이 사이버보안 전략 및 단계에 대한 위험, 비용 및 이익을 정량적으로 측정할수록, 사이버보안 방법 및 투자가 합리적이고 효과적으로 운용됨

사이버보안 운영이 지속되면 자가평가 및 정량적 측정으로 투자를 위한 우선순위 결정을 용이하게 함. 예를 들어, 특정 시간에 대한 측정은 기관의 사이버보안 운용 상태를 확인하여 협력업체, 공급업체, 구매자 및 다른 이해관계자들에게 의미 있는 위험 정보를 전달할 수 있음. 기관은 이러한 활동을 내부적으로 달성할 수 있거나 제 3 자에게 평가를 받을 수 있음. 사이버보안 활동이 적절하게 수행되고 한계점에 대한 인식을 갖는다면, 이러한 정량적 측정들은 기관 내외부적으로 신뢰할 수 있는 지표를 제공할 수 있음. .

투자의 효과성을 살펴보기 위해, 기관은 먼저 사이버보안의 목적, 구현 및 운용방법, 결과에 관한 명확한 이해를 가지고 있어야 함. 이러한 중요 요소는 본 프레임워크의 범위 밖이긴 하지만, 프레임워크 코어의 사이버보안 결과는 다음과 같은 방법으로 투자 대비 효과성, 사이버보안 활동에 대한 자가평가를 지원함:

1) 사이버보안 운영에서 해당 단계와 상이한 부분은 구현 대상에 영향을 미침
2) 현재 구현 단계를 결정함에 따라 사이버보안 위험관리 기관의 운영방법을 평가함
3) 대상 프로필을 개발함으로써 사이버보안 결과를 우선 순위화 함.
4) 현재 프로필에 대한 평가를 통해 이상적인 사이버보안의 결과 달성을 위해 구체적인 사이버보안 단계의 수준을 결정함
5) 정보적 참고사항에 명시된 통제 카탈로그 혹은 기술적 가이드라인에 대한 구현 수준을 측정함

사이버보안 성과 측정지표의 개발은 개선중임. 기관은 사이버보안 운영의 확산을 위해 측정 지표의 사용방법은 신중해야 하며, 사이버보안 위험 관리를 개선하기 위해 현재 상태 및 진행상황에 대한 것은 측정 지표에 의해 한정하지 않아야 함. 사이버 보안 위험을 판단하는 것은 규정에 따르며 규정은 정기적으로 업데이트되어야 함. 프레임워크 프로세스의 일부로 측정지표가 사용될 때마다, 기관은 이러한 측정이 왜 중요한지와 사이버보안 위험의 전체적인 관리에 기여하는 방안에 대해 명백하게 구분하는 것을 권장함. 또한, 기관은 사용된 측정에 한계점에 대해 인지해야 함.

예를 들어, 사이버 보안 방법과 경영결과를 추적하는 것은 세분화된 보안 통제에서의 변경사항이 기관의 목표 완성에 어떠한 영향을 미치는 지에 대해 의미 있는 결과를 제공할 수 있음. 몇몇 기관의 목표 달성을 검증하는 것은 목표가 달성된 이후데이터 분석에 의함. 이러한 후향적 방법이 주로 사용되나, 예측연구인 사이버보안 위험 발생여부 및 미치는 영향이 더 중요할 수 있음.

기관은 프레임워크의 활용에 따라 전 후의 측정방법이 권장되며 프레임워크의 활용성을 높이며 또한 제한점을 인지하여야 함.

부 록 I

프레임워크 코어

본 부록은 프레임워크 코어를 제시함: 기능, 항목, 하위항목 및 참고적 정보 목록으로 모든 주요 인프라 분야에 걸쳐 공통적인 특정 사이버보안 활동을 설명함. 프레임워크 코어를 설명하는 형식은 특정 구현 순서를 제안한다거나 항목, 하위항목 및 참고적 정보에 대한 중요성 수준을 암시하지 않음
본 부록에 제시된 프레임워크 코어는 사이버보안 위험을 관리하는 것에 있어서의 일반적인 활동 집합을 대변함
프레임워크가 포괄적이지는 않지만, 확장가능하여 기관, 분야 및 다른 기관들이 비용 효과적, 비용 효율적인 하위항목 및 참고적 정보 목록을 사용하는 것이 가능하며 사이버보안 위험 관리를 가능케 함.
활동은 프로필 생성 프로세스 동안 프레임워크 코어에서 선정될 수 있으며, 추가적 항목, 하위항목 및 참고 정보는 프로필에 추가될 수 있음. 기관의 위험관리 프로세스, 법률/규정 요구사항, 경영/미션 목표 및 기관의 제한점은 프로필이 생성되는 동안 활동을 선정함. 개인정보는 보안 위험 및 보호를 평가할 시 항목 내 인용된 데이터 혹은 자원의 구성요소로 고려됨

기능, 항목 및 하위항목에 식별된 의도하는 결과는 IT와 ICS에서 동일하지만, IT와 ICS에서의 운영환경과 고려사항은 상이함. ICS는 개인의 건강 및 안전에 대한 잠재적인 위험과 환경에 대한 영향을 포함하여 물리적 환경에 직접적인 영향을 끼침. 추가적으로, ICS는 IT와 비교하여 고유한 성능 및 신뢰성 요구사항을 가지고 있으며 안전성과 효율성 목표는 사이버보안 방안을 구현할 시 고려되어야 함.

사용의 용이성을 위하여, 프레임워크 코어의 각 구성요소는 고유식별자가 부여됨. 기능과 항목은 표 1에서와 같이 고유한 알파벳 식별자를 가지고 있음. 각 항목 내 하위항목은 숫자로 인용되며 각 하위항목에 대한 고유식별자는 표 2에 포함되어 있음.

참고 정보를 포함하여 프레임워크와 관련된 추가적인 자료는 NIST 웹사이트를 참고함. http://www.nist.gov/cyberframework/.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Enviroment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvement
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	식별	ID.AM	자산 관리
		ID.BE	사업 환경
		ID.GV	통치
		ID.RA	리스크 평가
		ID.RM	리스크 관리 전략
		ID.SC	공급체인 리스크 관리
PR	보호	PR.AC	ID관리 및 액세스 제어
		PR.AT	인식과 훈련
		PR.DS	데이터 보안
		PR.IP	정보보호 프로세스 및 절차
		PR.MA	유지보수
		PR.PT	보호적 기술
DE	탐지	DE.AE	이상 및 이벤트
		DE.CM	보안 연속 모니터링
		DE.DP	탐지 프로세스
RS	대응	RS.RP	대응 계획
		RS.CO	의사소통
		RS.AN	분석
		RS.MI	완화
		RS.IM	개선
RC	복구	RC.RP	복구 계획
		RC.IM	개량
		RC.CO	의사소통

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**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: Software platforms and applications within the organization are inventoried	**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: Organizational communication and data flows are mapped	**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: External information systems are catalogued	**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: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01 **ISA 62443-2-1:2009** 4.2.3.6 **ISA 62443-3-3:2013** A.8.2.1 **NIST SP 800-53 Rev.4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders(e.g., suppliers, customers, partners) are established	**CIS CSC** 17,19 **COBIT 5** APO01.02, APO07.06,APO13.01,DSS06.03 **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

기능	항목	하위항목	참조 정보
식별 (ID)	**자산 관리(ID.AM):** 조직이 사업 목적을 달성 할 수 있도록 하는 데이터, 인력, 장치, 시스템 및 시설은 조직 목표 및 조직의 위험 전략에 대한 상대적 중요성에 따라 식별되고 관리된다.	**ID.AM-1:** 조직 내 물리적 장치 및 시스템은 재고되어있다	**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 내 소프트웨어 플랫폼 및 어플리케이션은 재고되어있다	**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: 조직적 의사소통과 데이터 흐름은 매핑되어 있다	**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 목록에 있다	**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, 장비, 데이터 및 소프트웨어)은 그들의 분류, 심각성 및 사업 가치에 기반하여 우선순위화 되어 있다	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01 **ISA 62443-2-1:2009** 4.2.3.6 **ISA 62443-3-3:2013** A.8.2.1 **NIST SP 800-53 Rev.4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: 전체 인력 및 제3자 이해관계자 (예: 공급업체,고객,파트너) 내 사이버 보안 역할 및 책무가 구축되어 있다	**CIS CSC** 17,19 **COBIT 5** APO01.02, APO07.06,APO13.01,DSS06.03 **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

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**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.15.2.1, A.15.2.2 **NIST SP 800-53 Rev.4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev.4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**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.BE-4: Dependencies and critical functions for delivery of critical services are established	**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.BE-5: Resilience requirements to support delivery of critical services are established for all operating states(e.g. under duress/attack, during recovery, normal operations)	**CIS CSC 13, 14** **COBIT 5** APO03.03, APO03.04, APO12.01 **ISA 62443-2-1:2009** 4.2.3.6 **ISA 62443-3-3:2013** A.8.2.1 **NIST SP 800-53 Rev.4** CP-2, RA-2, SA-14, SC-6

기능	항목	하위항목	참조 정보
식별 (ID)	**사업환경(ID.BE):** 조직의 미션, 목적, 이해관계자 및 활동은 이해되고 우선순위화 되어 있다. 이 정보는 사이버보안 역할, 책무 및 리스크관리 결정을 공지하기 위해 사용된다.	**ID.BE-1:** 공급 체인에서의 조직의 역할은 식별되고 의사소통 되고 있다.	**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.15.2.1, A.15.2.2 **NIST SP 800-53 Rev.4** CP-2, SA-12
		ID.BE-2: 주요 인프라 및 산업분야에서의 조직의 위치는 식별되고 의사소통 되고 있다.	**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 미션, 목적 및 활동에서의 우선순위는 식별되고 의사소통 되고 있다.	**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.BE-4: 주요 서비스 제공에서의 의존성 및 주요 기능은 구축되어 있다.	**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.BE-5: 주요 서비스 제공을 지원하기 위한 탄력성에 관한 요구사항이 구축되어 있다.	**CIS CSC 13, 14** **COBIT 5** APO03.03, APO03.04, APO12.01 **ISA 62443-2-1:2009** 4.2.3.6 **ISA 62443-3-3:2013** A.8.2.1 **NIST SP 800-53 Rev.4** CP-2, RA-2, SA-14, SC-6

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, enviromental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, 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
		ID.GV-2: Cybersecurity roles and responsibilities are coordinatted and aligned with internal roles and external partners	**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: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**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: Governance and risk management processes address cybersecurity risks	**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

기능	항목	하위항목	참조 정보
식별 (ID)	**통치 (ID.GV):** 조직의 규제적, 법률적, 리스크, 환경적 및 운영적 요구사항을 관리하고 모니터링 하기 위한 정책. 절차 및 프로세스는 이해되며 사이버보안 리스크 관리에 대해 공지하고 있다.	**ID.GV-1:** 조직적 정보 보안 정책이 구축되어 있다.	**CIS CSC** 19 **COBIT 5** APO01.03, 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
		ID.GV-2: 정보보안 역할&책무는 내부 역할 및 외부 파트너와 조정되어 있으며 부합화되어 있다.	**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: 프라이버시 및 인권 옹호 책임을 포함한 사이버보안 관련 법률적, 규제적 요구사항은 이해되며 관리되고 있다	**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: 통치 및 리스크 관리 프로세스는 사이버보안 리스크를 다루고 있다.	**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

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Risk Assessment (ID.RA): The oraganization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	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, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	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
		ID.RA-3: Threats, both internal and external, are identified and documented	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: Potential business impacts and likelihoods are identified	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: Threats, vulnerabilities, likehoods, and impacts are used to determine risk	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: Risk responses are identified and prioritized	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

기능	항목	하위항목	참조 정보
식별 (ID)	**리스크 평가 (ID.RA):** 조직은 조직적 운영(미션,기능,이미지 혹은 명성), 조직 자산 및 개개인에 대한 사이버보안 리스크에 대해 이해하고 있다.	**ID.RA-1:** 자산 취약점은 식별되고 문서화되어 있다.	**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, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: 위협 및 취약점 정보는 정보 공유 포럼 및 소스로부터 수신되고 있다.	**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
		ID.RA-3: 내외부 위협은 식별되고 문서화되어 있다.	**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 사업 영향 및 가능성은 식별되고 있다.	**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 리스크를 결정하는데 사용되고 있다.	**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: 리스크 응답은 식별되고 우선순위화 되어 있다.	**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

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**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: Organizational risk tolerance is determined and clearly expressed	**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
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**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

기능	항목	하위항목	참조 정보
식별 (ID)	**리스크 관리 전략 (ID.RM):** 조직의 우선 순위, 제약 조건, 리스크 허용오차 및 가정이 설정되어 운영 위험 결정을 지원합니다.	**ID.RM-1:** 리스크 관리 프로세스는 조직적 이해관계자들에 의해 구축, 관리, 동의되고 있다.	**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: 조직적 리스크 수용성은 결정되어 있고 명백하게 표현되어 있다.	**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
		ID.RM-3: 조직의 리스크 수용성 결정은 주요 인프라 및 분야 특화 리스크 분석에 뚜라 공지되어 있다.	**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

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**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: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**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: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**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: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**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
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**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

기능	항목	하위항목	참조 정보
식별 (ID)	**공급망 리스크 관리 (ID.SC):** 조직의 우선순위, 제한점, 리스크 수용성 및 가정은 구축되어 공급망 리스크 관리와 연관된 리스크 결정을 지원하는데 사용된다. 조직은 공급망 리스크를 식별, 평가 및 관리하기 위한 프로세스를 구축하여 구현하고 있다.	**ID.SC-1:** 사이버 공급망 리스크 관리 프로세스는 조직 이해관계자로부터 식별되고 구축되어, 평가되고, 관리되며 동의되어 있다.	**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, 구성요소 및 서비스의 공급업체 및 제3자 파트너는 사이버 공급망 리스크 평가 프로세스를 사용하여 식별되고, 우선순위화 되어 평가된다.	**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 제3자 파트너와의 계약은 조직의 사이버보안 프로그램 및 사이버 공급망 리스크 관리 계획의 목적을 충족하도록 설계된 적절한 방안을 구현하는데 사용된다.	**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 제3자 파트너는 내부 검사, 시험 결과 혹은 다른 형식의 평가를 사용하여 이들의 계약적 책임을 충족하고 있는 지 확인하기 위하여 정기적으로 평가된다.	**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
		ID.SC-5: 응답,회복 계획 및 시험은 공급업체 및 제3자 제공자와 수행된다.	**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

Function	Category	Subcategory	Informative References
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Acess to physical and logical assets and associated facilities is limitied to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	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: Physical access to assets is managed and protected	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: Remote access is managed	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 NIST SP 800-53 Rev.4 AC-1, AC-17, AC-19, AC-20 SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	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: Network integrity is protected (e.g., network segregation, network segmentation)	**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: Identities are proofed and bound to credentials and asserted in interactions	**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, PE-3
		PR.AC-7: Users, devices, and other assets are authenticated(e.g., single-factor, multi-factor) commensurate with the risk of the transaction(e.g., individuals' security and privacy risks and other organizational risks)	**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 **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.9.4.2, 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

기능	항목	하위항목	참고적 정보
보호(PR)	**접근 통제(PR.AC):** 자산 및 관련 시설물에 대한 접근은 승인 받은 사용자, 프로세스 혹은 기기 및 승인	**PR.AC-1:** 승인받은 기기 및 사용자들을 대상으로 신원 및 증명은 관리되고 있다.	**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,

	받은 활동 및 결제로 제한되고 있다.		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 보호되어 있다	**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 관리되고 있다	**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 **NIST SP 800-53 Rev.4** AC-1, AC-17, AC-19, AC-20 SC-15
		PR.AC-4: 접근 허가는 최소 권한 및 업무 분할 원칙을 활용하여 관리되고 있다.	**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 무결성은 해당 될 시 네트워크 분리를 활용하여 보호되고 있다.	**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: 신분증명 및 자격증명을 얻게 되며 상호작용에서 삽입된다.	**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, PE-3
		PR.AC-7: 사용자, 장치 및 다른 자산은 거래의 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타)에 상응하여 인가된다. (예: 단일 요인, 다요인)	**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 **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.9.4.2, 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

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and aggreements.	**PR.AT-1:** All users are informed and trained	**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: Privileged users understand their roles and responsibilities	**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: Third-party stakeholders (e.g., suppliers, customers, patners)understand their roles and responsibilities	**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: Senior executives understand their roles and responsibilities	**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: Physical and cybersecurity personnel understand their roles and responsibilities	**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 **NIST SP 800-53 Rev.4** AT-3, IR-2, PM-13

기능	항목	하위항목	참고적 정보
보호(PR)	**인식 및 훈련 (PR.AT):** 조직의 인력과 파트너는 사이버 보안 인식 교육을 실시하고 관련 정책, 절차, 학위 등에 부합하는 사이버보안 관련 업무 및 책임을 수행하도록 교육을 받는다.	**PR.AT-1:** 모든 사용자는 공지를 받으며 훈련을 받고 있다.	**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: 특혜 받은 사용자는 역할과 책임을 이해하고 있다.	**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: 제3의 이해관계자(예:공급업체, 고객, 파트너)는 역할과 책임을 이해하고 있다.	**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 경영진들은 역할과 책임을 이해하고 있다.	**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 정보보안 인력은 역할과 책임을 이해하고 있다.	**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 **NIST SP 800-53 Rev.4** AT-3, IR-2, PM-13

Function	Category	Subcategory	Informative References
PROTECT (PR)	Data Security (PR.DS): Information and record (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	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-2, SC-28
		PR.DS-2: Data-in-transit is protected	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: Assets are formally managed throughout removal, transfers, and disposition.	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.2.4.2 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: Adequate capacity to ensure availability is maintained.	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: Protections against data leaks are implemented.	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, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.1, 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: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**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: The development and testing enviroment(s) are separate from the production enviroment	**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: Integrity checking mechanisms are used to verify hardware integrity	**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

기능	항목	하위항목	참고적 정보
보호(PR)	**데이터 보안 (PR.DS):** 정보 및 기록(데이터)은 정보의 기밀성, 무결성 및 가용성을 보호하기 위해 조직의 리스크 전략과 일관적으로 관리되고 있다.	**PR.DS-1:** 유휴 상태의 데이터는 보호되고 있다.	**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-2, SC-28
		PR.DS-2: 전송 중인 데이터는 보호되고 있다.	**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 관리된다.	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.2.4.2 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 적절한 기능은 유지되고 있다.	**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 보호가 구현되고 있다.	**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, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.1, 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: 무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 검증하는데 사용되고 있다.	**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 독립적이다.	**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: 무결성 확인 메커니즘은 하드웨어 무결성을 검증하기 위해 사용된다.	**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

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control system is created and maintained incorporating security principles(e.g. concept of least functionality)	**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: A System Development Life Cycle to manage systems is implemented	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01 BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **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: Configuration change control processes are in place	**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: Backups of information are conducted, maintained, and tested	**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: Policy and regulations regarding the physical operating environment for organizational assets are met	**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: Data is destroyed according to policy	**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
		PR.IP-7: Protection processes are improved	**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: Effectiveness of protection technologies is shared	**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: Response plans(Incident Response and Business Continuity) and recovery plans(Incident Recovery and Disaster Recovery) are in place and managed.	**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: Response and recovery plans are tested	**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: Cybersecurity is included in human resources practices(e.g., deprovisioning, personnel screening)	**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

		PR.IP-12: A vulnerability management plan is developed and implemented	**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

기능	항목	하위항목	참고적 정보
보호(PR)	**정보 보호 프로세스 및 절차 (PR.IP):** 정보 시스템 및 자산 보호를 관리하기 위해 보안정책(목적, 범위, 역할, 책임, 경영 위탁 및 조직 개체 간의 조정), 프로세스 및 절차가 유지 관리 및 사용되고 있다.	**PR.IP-1:** 보안원칙(예:최소 기능 개념)을 통합하여 정보기술/산업 제어 시스템의 기본 구성을 생성하고 유지하고 있다.	**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 관리하는 시스템 개발 수명 주기가 구현 되고 있다.	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01 BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **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: 형상 변경 제어 프로세스가 실행 되고 있다.	**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: 정보 백업은 정기적으로 실행되고, 유지되며 테스트되고 있다.	**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 자산에 대한 물리적 운영 환경에 관한 정책 및 규정이 충족되고 있다.	**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: 정책에 따라 데이터가 삭제됩니다.	**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
		PR.IP-7: 보호 프로세스가 향상되고 있다.	**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 효율성이 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: 대응계획(사고 대응 및 비즈니스 연속성) 및 복구 계획(사고 복구 및 재해 복구)이 마련되어 관리 됩니다.	**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 계획 테스트	**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: 사이버보안은 인적 자원 실행에 포함됩니다.(예:프로비저닝 해제, 인사 심사)	**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
		PR.IP-12: 취약성 관리 계획을 개발하고 구현합니다.	**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

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	**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: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**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
	Protective Technology (PR.PT): Technical security solutions are	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**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,

	managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.		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: Removable media is protected and its use restricted according to policy	**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 **NIST SP 800-53 Rev.4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**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: Communications and control networks are protected	**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 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: Mechanisms(e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	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

기능	항목	하위항목	참고적 정보
보호(PR)	유지보수(PR.MA): 산업 제어 및 정보 시스템 구성 요소의 유지 보수 및 수리는 정책 및 절차에 따라 수행됩니다.	PR.MA-1: 조직 자산의 유지 보수는 승인되고 통제되는 도구를 사용하여 수행되고 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 유지 관리는 승인되지 않은 액세스를 방지하는 방식으로 승인, 기록 및 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
	보호적 기술(PR.PT): 기술 보안 솔루션은 관련 정책, 절차 및 계약에 따라 시스템 및 자산의 보안과 복원력을 보장하도록 관리됩니다.	PR.PT-1: 감사 / 로그 기록은 정책에 따라 결정, 문서화, 구현 및 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 정책에 뚜라 보호되고 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 NIST SP 800-53 Rev.4 MP-2, MP-3, MP-4, MP-5,

			MP-7, MP-8
		PR.PT-3: 최소 기능의 원칙은 필수 기능만 제공하도록 시스템을 구성하여 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 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: 매커니즘(예: 페일 세이프, 로드 밸런싱, 핵 스왑)은 정상 및 불리한 상황에서 복원력 요구사항을 달성하기 위해 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

Function	Category	Subcategory	Informative References
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**CIS CSC** 1,4,6,12,13,15,16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **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: Detected events are analyzed to understand attack targets and methods	**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 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: Event data are collected and correlated from multiple sources and sensors	**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-8, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**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: Incident alert thresholds are established	**CIS CSC** 6, 19 **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	항목	하위항목	참고적 정보
탐지(DE)	이상 및 이벤트 (DE.AE): 비정상적인 활동이 감지되고 사건의 잠재적 영향을 이해합니다.	DE.AE-1: 사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준이 설정되고 관리됩니다.	CIS CSC 1,4,6,12,13,15,16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 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 이벤트는 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 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: 이벤트 데이터는 여러 소스 및 센서에서 수집 및 상관 관계가 있습니다.	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-8, SI-4
		DE.AE-4: 이벤트의 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 경고 임계값이 설정됩니다.	CIS CSC 6, 19 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

Function	Category	Subcategory	Informative References
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**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
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**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: Personnel activity is monitored to detect potential cybersecurity events	**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: Malicious code id detected	**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: Unauthorized mobile code is detected	**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: External service provider activity is monitored to detect potential cybersecurity events	**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: Monitoring for unauthorized personnel, connections, devices, and software is performed	**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: Vulnerability scans are performed	**CIS CSC** 4. 20 **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

기능	항목	하위항목	참고적 정보
탐지(DE)	**보안 연속 모니터링 (DE.CM):** 정보 시스템과 자산을 모니터링하여 사이버 보안 이벤트를 식별하고 보호 조치의 효과를 확인합니다.	**DE.CM-1:** 네트워크가 모니터링되어 잠재적인 사이버 보안 이벤트를 탐지합니다.	**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
		DE.CM-2: 잠재적인 사이버 보안 이벤트를 탐지하기 위해서 물리적 환경은 모니터링이 됩니다.	**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: 잠재적인 사이버보안 이벤트를 탐지하기 위해 인적 활동은 모니터링이 됩니다.	**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: 비인가된 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: 잠재적인 사이버 보안 이벤트를 탐지하기 위해 외부 서비스 공급자 활동을 모니터링합니다.	**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: 무단 직원, 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: 취약성 검사가 수행됩니다.	**CIS CSC** 4. 20 **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

Function	Category	Subcategory	Informative References
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.14 **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: Detection activities comply with all applicable requirements	**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: Detection processes are tested	**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: Event detection information is communicated	**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: Detection processes are continuously improved	**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	항목	하위항목	참고적 정보
탐지(DE)	**탐지 프로세스 (DE.DP):** 비정상적인 이벤트에 대한 인식을 보장하기 위해 감지 프로세스 및 절차를 유지하고 테스트합니다.	**DE.DP-1:** 탐지 역할과 책임은 책임성을 보장하기 위해 잘 정의되어 있습니다.	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.14 **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: 감지 활동은 모든 해당 요구 사항을 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: 감지 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: 이벤트 감지 정보가 전달됩니다.	**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: 감지 프로세스가 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

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**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
	Communication (RS.CO): response activities are coordinated with internal and external stake holders(e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**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: Incidents are reported consistent with established criteria	**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: Information is shared consistent with response plans	**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: Coordination with stakeholders occurs consistent with response plans	**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: Voluntary information sharing occurs with external stakeholders to achieve boarder cybersecurity situational awareness	**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	항목	하위항목	참고적 정보
대응(RS)	**대응 계획 (RS.RP):** 감지된 사이버 보안 사고에 대한 대응을 보장하기 위해 대응 프로세스 및 절차를 실행하고 유지합니다.	**RS.RP-1:** 대응 계획은 사건 발생 또는 발생 후에 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
	의사소통 (RS.CO): 대응 활동은 내부 및 외부 이해관계자와 조정됩니다. (예: 법 집행 기관의 외부 지원)	**RS.CO-1:** 직원은 대응이 필요할 때 자신의 역할과 작업 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: 사고는 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 계획과 일관되게 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: 이해당사자와의 조정은 대응 계획에 따라 이루어집니다.	**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: 외부 이해관계자와 자발적 정보 공유는 이사회 사이버 보안 상황 인식을 실현하기 위해 이루어 집니다.	**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

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and supoprt recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**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: The impact of the incident is understood	**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: Forensics are performed	**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: Incidents are categorized consistent with response plans	**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** CA-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources(e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev.4** SI-5, PM-15

기능	항목	하위항목	참고적 정보
대응(RS)	**분석 (RS.AN):** 효과적인 대응 및 서포트 복구 활동을 보장하기 위해 분석이 수행됩니다.	**RS.AN-1:** 탐지 시스템의 통지를 조사합니다.	**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: 법의학이 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: 사고는 대응 계획에 따라 분류됩니다.	**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** CA-2, IR-4, IR-5, IR-8
		RS.AN-5: 내부 및 외부소스(예: 내부 테스트, 보안 게시판 또는 보안 연구원)에서 조직에 공개된 취약점을 수신, 분석 및 대응하기 위한 프로세스를 정의합니다.	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev.4** SI-5, PM-15

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**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 **NIST SP 800-53 Rev.4** IR-4
		RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO02.02 **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: Newly identified vulnerabilities are mitigated or documented as accepted risks	**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
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**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: Response stategies are updated	**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

기능	항목	하위항목	참고적 정보
대응(RS)	**완화 (RS.MI):** 이벤트의 확장을 방지하고, 그 영향을 완화하며, 사건을 해결하기 위한 활동을 수행합니다.	**RS.MI-1:** 사건이 포함되어 있습니다.	**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 **NIST SP 800-53 Rev.4** IR-4
		RS.MI-2: 사건이 완화됩니다.	**CIS CSC** 4, 19 **COBIT 5** APO02.02 **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: 새롭게 식별된 취약성은 허용된 위험으로 완화되거나 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 (RS.IM): 조직 대응 활동은 현재 및 이전 탐지/대응 활동에서 얻은 교훈을 통합하여 개선됩니다.	**RS.IM-1:** 대응 계획에는 학습된 교육이 통합되어 있습니다.	**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: 응답 상태가 업데이트 되었습니다.	**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

Function	Category	Subcategory	Informative References
RECOVER(RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed andn maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**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
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**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: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.12.6.1, Clause 10 **NIST SP 800-53 Rev.4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties(e.g. coorinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputations is repaired after an incident	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev.4** CP-2, IR-4

기능	항목	하위항목	참고적 정보
복구(RC)	**복구 계획 (RC.RP):** 복구 프로세스 및 절차를 실행하고 유지 관리하여 사이버 보안 사고의 영향을 받는 시스템 또는 자산을 복원합니다.	**RC.RP-1:** 복구 계획은 사이버 보안 문제 발생 시 또는 이후에 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 (RC.IM): 조직 대응 활동은 현재 및 이전 탐지/대응 활동에서 얻은 교훈을 통하여 개선됩니다.	**RC.IM-1:** 복구 계획에는 학습된 교육이 통합되어 있습니다.	**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 업데이트 되었습니다.	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.12.6.1, Clause 10 **NIST SP 800-53 Rev.4** CP-2, IR-4, IR-8
	의사소통 (RC.CO): 복원 활동은 내부 및 외부 당사자(예: 조정 센터, 인터넷 서비스 공급자, 공격 시스템 소유자, 피해자, 기타 CSIRT 및 공급업체)와 조정됩니다.	**RC.CO-1:** 홍보 활동이 관리됩니다.	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: 교체는 문제 발생 후 복구됩니다.	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: 복구 활동은 경영진 및 관리 팀뿐만 아니라 내부 및 외부 관계자에게도 전달됩니다.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev.4** CP-2, IR-4

부 록 II-1 *(스타일 적용-본문상단제목)*

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 II-2 *(스타일 적용-본문상단제목)*

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 II-3 *(스타일 적용-본문상단제목)*

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] COBIT: http://www.isaca.org/COBIT/Pages/default.aspx
[2] CIS Controls: https://www.cisecurity.org
[3]ANSI/ISA 62443-2-1:
https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
[4]ANSI/ISA 62443-3-3:
https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
[5] ISO/IEC 27001: https://www.iso.org/standard/54534.html
[6] NIST SP 800-53: https://doi.org/10.6028/NIST.SP.800-53r4

부 록 II-5 *(스타일 적용-본문상단제목)*

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2019.10.xx	TTAX.xx-xx.xxxx	의료기관 정보 인프라의 사이버보안 참조 모델	바이오인식 프로젝트그룹 (PG505)