2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 5-3

공급망 보안

한근희 교수 (고려대학교)

[요약문]

- 기업에서 사용하는 ICT 시스템과 연관된 하드웨어, 소프트웨어, 공급사, 유지보수업체, 외주업체 등 전체 공급망은 이루 헤아릴 수 없을 정도로 규모가 거대함.
- 대기업이나 대형 병원의 경우 24시간 365일 물류 및 관련 제품 등이 중단없이 공급되어야 함
- 다양한 ICT 제품이 공급되는 과정에서 공급망에 대한 사이버 보안 위협·공격으로 기업의 중요한 자산과 민감한 개인정보의 유·노출 등 사이버 위협이나 침해사고가 발생할 수 있음
- 기업의 공급망 사슬에 대한 사이버 보안 취약성을 살펴 보고 보안 대책을 강구할 수 있는 방안을 소개함

[발표자 약력]

- 고려대학교 정보보호대학원 연구교수
- 한국정보보호학회, 한국정보처리학회, 한국사물인터넷학회 부회장
- 스마트의료보안포럼 의장,
- ISO TC 215 Health Informatics WG 4 Security, Safety and Privacy 전문위원
- IEC TC 65 WG 10 Security for industrial process measurement and control - Network and system security 전문위원

관심분야 : 소프트웨어 보안, 공급망 보안, 융합보안(의료보안, 제조보안), 위험관리, ISMS, 개인정보보호 등

고려대학교
KOREA UNIVERSITY

공급망 보안
Supply Chain Security

2020. 9. 25.

韓 根熙
고려대학교
khhan1@korea.ac.kr

고려대학교
KOREA UNIVERSITY

고려대학교 KOREA UNIVERSITY

목차

I 공급망 위협 및 공격 사례

II 미국 공급망 보안 기준

III 공급망 보안 국제표준

IV 공급망 보안 대책

V 마무리

고려대학교 KOREA UNIVERSITY

Quality Model

- IT 시스템의 품질 특성은 기능, 성능, 신뢰성, 가용성, 보안 및 휴대성의 상호작용을 정의할 수 있다.
- 품질 특성은 제품 표준을 사용하여 정의
- 제품 및 공정의 관리 및 기술 프로세스를 따르고 제품 및 공정의 검사/검토/시험 등 다른 기법에 의해 확인 및 검증된다.

Quality Characteristics	Defined	Achieved by following	
		Software Process	System Process
Functionality	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 15288
Performance	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 20000-1
Reliability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207 IEEE 982.1	ISO/IEC 20000-1
Usability	ISO 9241	ISO/IEC 13407	ISO 9241
Security	ISO 9126 / ISO/IEC 25010:2011 ISO/IEC 27034 ISO/IEC 27033	ISO/IEC 21827	ISO/IEC 27001
Portability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 12207	ISO/IEC 15288
Maintainability	ISO 9126 / ISO/IEC 25010:2011	ISO/IEC 14764	ISO/IEC 15288

나비 효과?

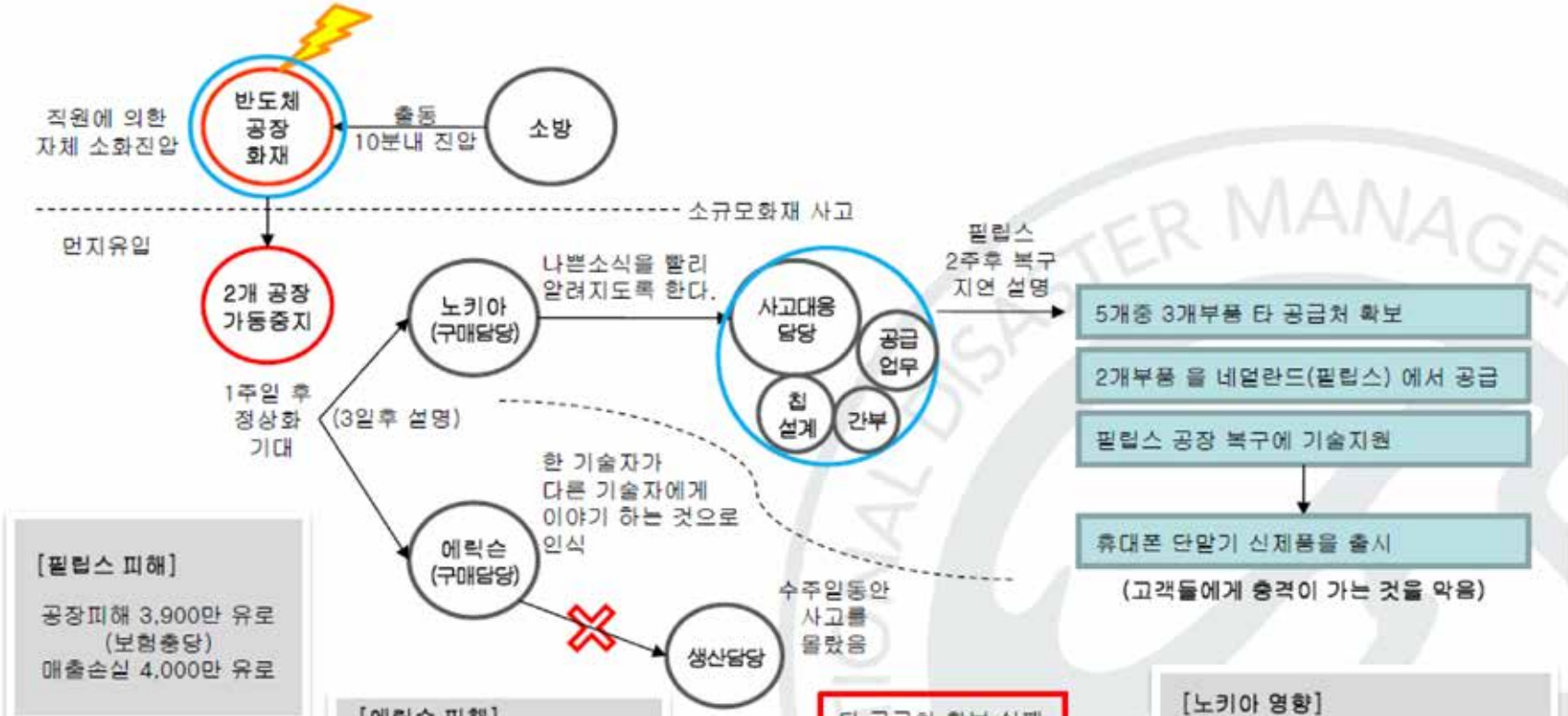
- 1999.9.21 대만 지진으로 야기된 반도체 공급 차질에 대한 델과 애플의 대응
  - 규모 7.6의 강진으로 전기 공급이 중단되면서 컴퓨터 칩으로 쓰일 반도체 웨이퍼 모두 폐기.
- Dell
  - 소수의 공급업체에 대한 의존도가 높은 글로벌 공급망의 취약점을 미리 간파
  - 이미 오래전부터 물류부문 혁신에 주력해 단기간의 주문-생산-출하 사이클을 운영
  - 특정 모델이나 가격에 얽매이지 않는 유연성 사전 확보.
- Apple
  - 신제품 개발에만 몰두
  - 소수 부품공급업체와의 장기공급계약
  - 부품조달 차질을 메울 만한 대체 공급원 준비하지 않았음
  - 결국 회사의 사활을 걸고 야심차게 준비해 온 노트북인 아이북(iBook) 생산 차질
- 그 결과 애플이 시장을 잃은 반면 델은 그해 3분기 순익을 전년 대비 41%나 높이는 성과를 나타냄

韓 根熙

나비 효과?

- 2000.3.17 Nokia 와 Ericsson 두 회사에 휴대폰 용 반도체 칩을 공급하던 New Mexico Philips의 반도체 공장에 낙뢰로 인한 화재 발생. → 화재는 10분만에 진압했으나 연기와 그을음으로 인해 반도체 생산을 위한 클린룸이 오염되어 생산라인 4개 중 2개 공정 중단
  - 예상복구 기간은 1주일로 결정되었지만, 실제 공정을 복구 하기 까지는 4주정도 기간이 소요
  - 화재 직후 필립스는 이 공장의 반도체 생산물량의 40%를 공급받는 노키아와 에릭슨에 1주일의 조업 중단이 예상된다고 통보
- Nokia는 사태를 예의 주시할 필요가 있다고 판단해 계획된 BCP에 따라 문제의 부품을 즉시 특별관리 품목에 올리고 전 부서에 이 사실을 알렸다. 또 필립스와 긴밀한 연락을 취하면서 상황을 점검했다. 노키아는 즉시 전 세계 필립스 공장의 생산 여력을 모두 노키아에 배정해 달라고 강력히 요구했다.
- Ericsson도 사고 발생 직후 필립스로부터 연락을 받았다. 그러나 에릭슨의 담당자는 1주일만 지나면 사태가 해결될 거라고 보고, 별다른 조치를 취하지 않고, 경영진에게 보고조차 하지 않았다. 수 일 후 사태가 심각한 지경에 이르렀다는 사실을 파악한 에릭슨의 경영진은 필립스로 달려갔지만 이미 때는 늦었다. 필립스의 모든 생산 여력이 노키아로 옮겨졌기 때문이다. 다른 반도체 공급처 역시 노키아가 이미 동원 가능한 설비를 모두 장악한 상태였다.
- R&CM의 부재로 인해 Ericsson은 2000년 휴대전화 부문에서 25억 달러의 적자를 기록
- 화재 여파가 겹친 2001년에는 세계시장 점유율이 2000년의 10%보다 낮은 6.7%로 하락했다.
- 결국 Ericsson 은 Sony 와 함께 Sony-Ericsson 이란 새로운 회사를 만들어야만 했다.

나비 효과?



(출처) 업무연속성 기반의 재난안전관리(오금호, 14.6.26)

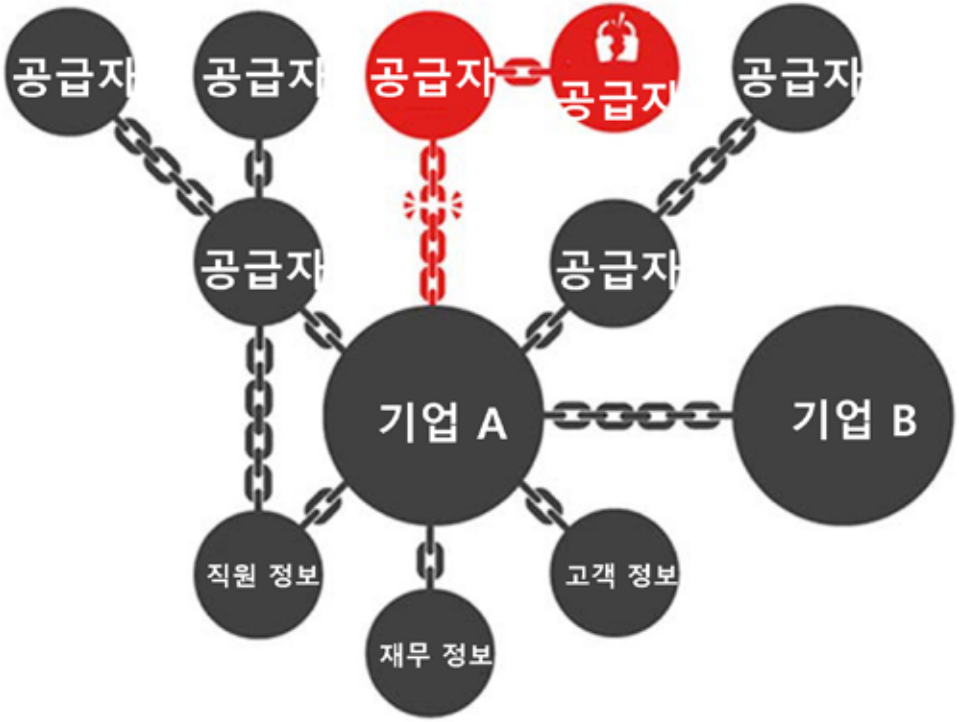
韓 根熙

Supply Chain

전체 보안 수준 = 많은 연결고리 중 가장 약한 부분의 보안 수준

Supply Chain Impact Analysis

- 공급망 영향평가는 특정 공급자가 획득자에 영향을 미치게 될 각종 요인들에 대해 그 부정적 영향을 제거하거나 최소화하기 위해 사전에 영향을 분석하여 검토하는 작업.
- 공격자가 보안 시스템이 준비된 표적 시스템을 직접 공격하지 않고 공급망에서 가장 허술한 말단 공급자를 침투하여 공급망 중단을 유발시킴



오래된 소프트웨어 Upgrade,보안 Patch

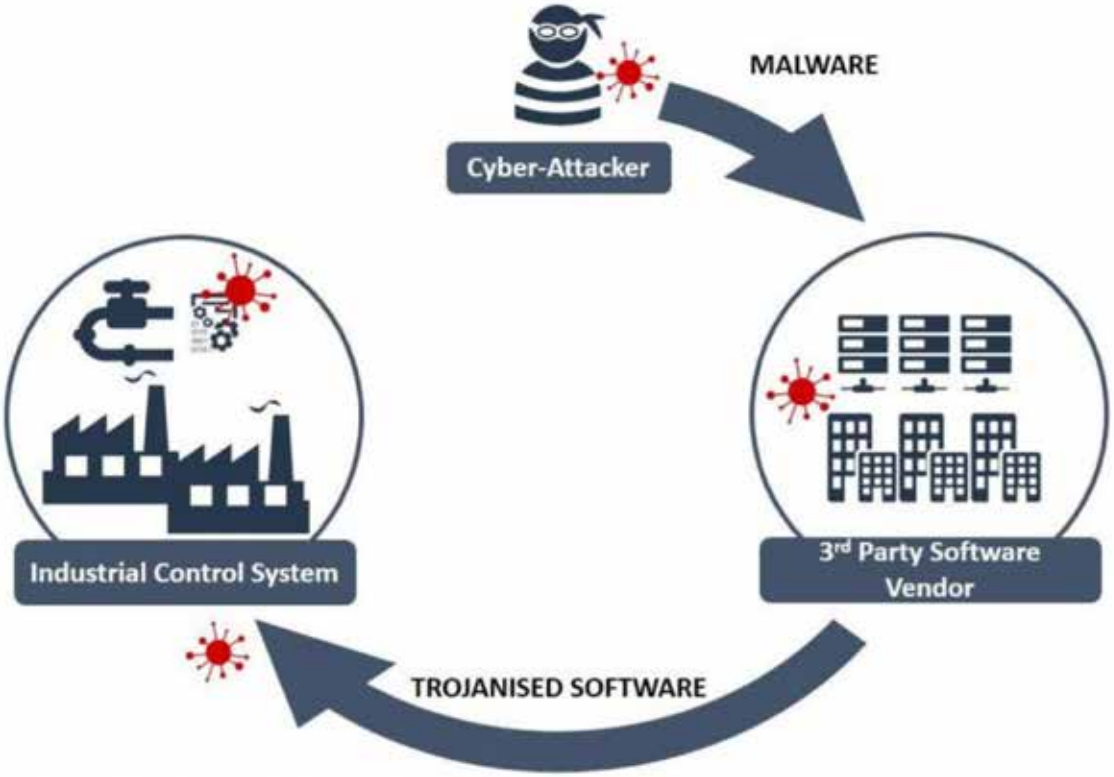
- 잘 동작하고 있는 시스템이나 기기에 손대지 마라.
  - 보안 패치나 업그레이드 진행하지 않음
- ICT 시스템과 설비 대다수가 오래된 운영체제인 Window XP, 7 등 사용
- '19.5월 KISA에서 마이크로소프트 윈도 제품의 원격 접속·관리 기능(원격 데스크톱 프로토콜·RDP)을 통해 악성코드를 설치·실행 할 수 있는 취약점을 발견했다며 모든 이용자는 보안 업데이트를 실행하라고 발표
  - 사용자 조작 없이도 자가 전파해 감염을 유발시키는 웜 형태의 악성코드와 통합
  - 2017년 세계적으로 큰 피해가 발생했던 워너크라이(WannaCry) 랜섬웨어와 유사한 방식으로 취약한 PC에 악성코드 전파가 가능
  - 영향을 받는 제품은 윈도우XP, 윈도7와 윈도우 서버 2003, 2008 등
  - MS는 취약점을 개선한 보안 업데이트를 배포 중
  - 해당 윈도우 제품 사용자들은 MS 홈페이지 또는 윈도우 업데이트 기능을 통해 보안 업데이트를 진행해야 함.
  - MS는 이번 **취약점의 위험성과 파급력을 감안**하여 기술지원이 종료된 윈도우 XP, 윈도우 서버 2003까지 별도의 보안 업데이트 제공

Do you know the real source of your components?

韓 根熙

Supply Chain Attack

❖ 공급망 공격(Supply Chain Attack)이란?



Example 1: Third Party Software Providers

Supply Chain Attack

❖ 공급망 공격(Supply Chain Attack)이란?

- 기관이나 기업의 **공급망에 침투**하여 사용자에게 전달되는 **S/W나 H/W를 변조**하는 형태의 공격

- **공급망** : 제품이나 서비스가 **공급자로부터 소비자에게 전달**되기까지의 **조직, 사람, 정보, 자원** 등에 대한 시스템을 총칭

Ex) 소프트웨어 **개발사의 네트워크에 침투**하여 소스 코드를 수정하여 **악의적인 목적의 코드(백도어 등)를 삽입**한다거나, **배포를 위한 서버**에 접근하여 **파일을 변경**하는 방식의 공격

Supply Chain Attack

❖ 공급망 공격(Supply Chain Attack)이 증가하게 된 배경

- 사이버 공격 이슈가 계속 됨에 따라 **큰 기관이나 기업은 정보보안에 지속적인 투자**를 하여 그 수준이 점점 높아지고 있음

- **중요 인프라가 설치된 망의 경우 망분리**를 통해 인터넷을 통한 접근을 차단

- 그럼에도 불구하고, 최종 서비스를 제공하는데 있어 **S/W 및 H/W의 Third Party 제조사들에 대한 의존도는** 줄일 수 없는 부분으로 남아있음(**인소싱의 한계**)

- **S/W, H/W 제조사**는 최종 서비스를 제공하는 기관이나 기업에 비해 **규모가 작고,**
  상대적으로 보안에 많은 투자를 하지 못함

- 따라서, **공격자가 더 쉽게 공략**을 할 수 있으며 **개발 서버나 배포 서버 장악에 성공하였을 경우 기대되는 파급효과도 매우 큰 특징**이 있음

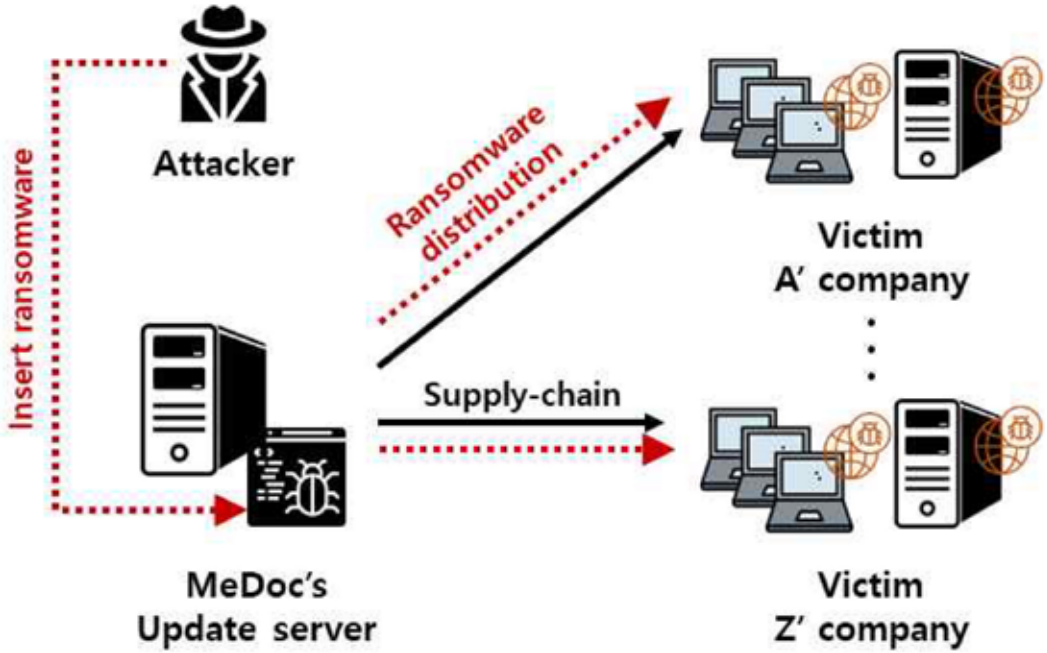
공급망 위협: 정품 하드웨어/소프트웨어 '19.9.28

- 중국산 저가 안드로이드 폰Mobile Malware 'Triada' 탑재
  - Mobile Malware 중 가장 발전된 형태로 추가 멀웨어를 다운로드 받아 설치
  - 광고를 억지로 보게하거나, 문자메시지를 가로채 인앱 구매대금을 빼돌리는 등의 다양한 피해 가능
  - 보안업체 비트사이트는 전세계 통신사 네트워크의 15%에서 트리아다가 감염된 장비들이 발견된다고 경고
- 구글 플레이스토어에서 1억번 이상 다운로드된 애플리케이션 '캠스캐너'에서 최근 악성 소프트웨어를 내려받는 기능의 트로이목마 발견(카스퍼스키랩)

韓 根熙

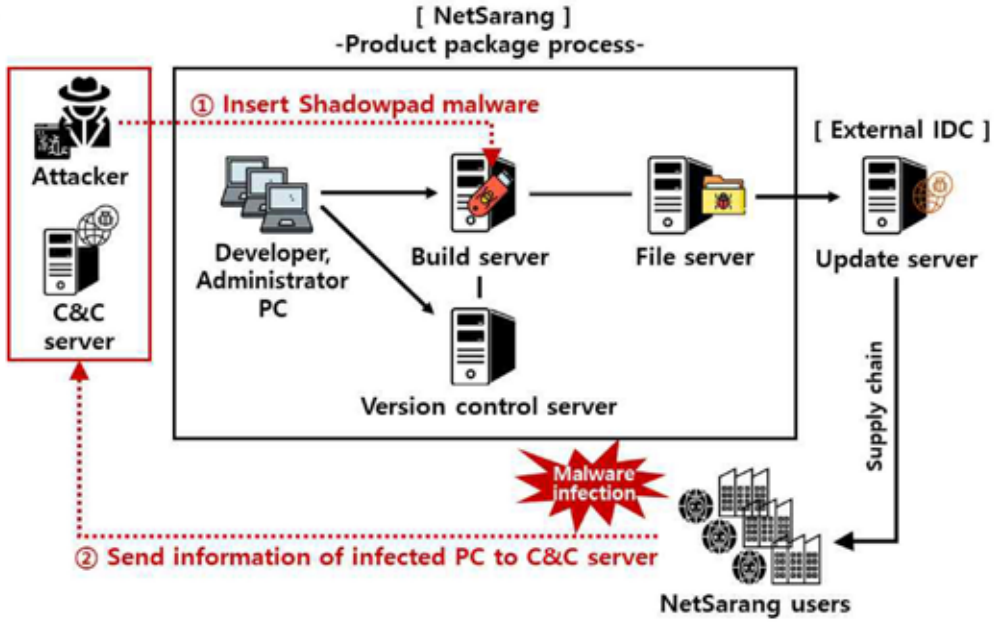
MeDoc Supply-chain Attack Process

- MeDoc – 우크라이나에서 세무회계 관리 소프트웨어를 개발하는 회사로서, 우크라이나는 모든 정부 기관에 대해 이 소프트웨어의 사용을 의무화하여 90%의 기업에서 사용.
- 소프트웨어 공급망 과정 중 배포 단계를 침투한 공급망 공격
- 2017년 6월 공격자는 MeDoc의 업데이트 서버를 해킹하여, 업데이트 요청 시 정상 업데이트가 아닌 Petya 랜섬웨어를 배포하도록 변조.
- FedEx 등 국제적 기업에도 피해를 입혀 **총 10조원의 손실 발생**

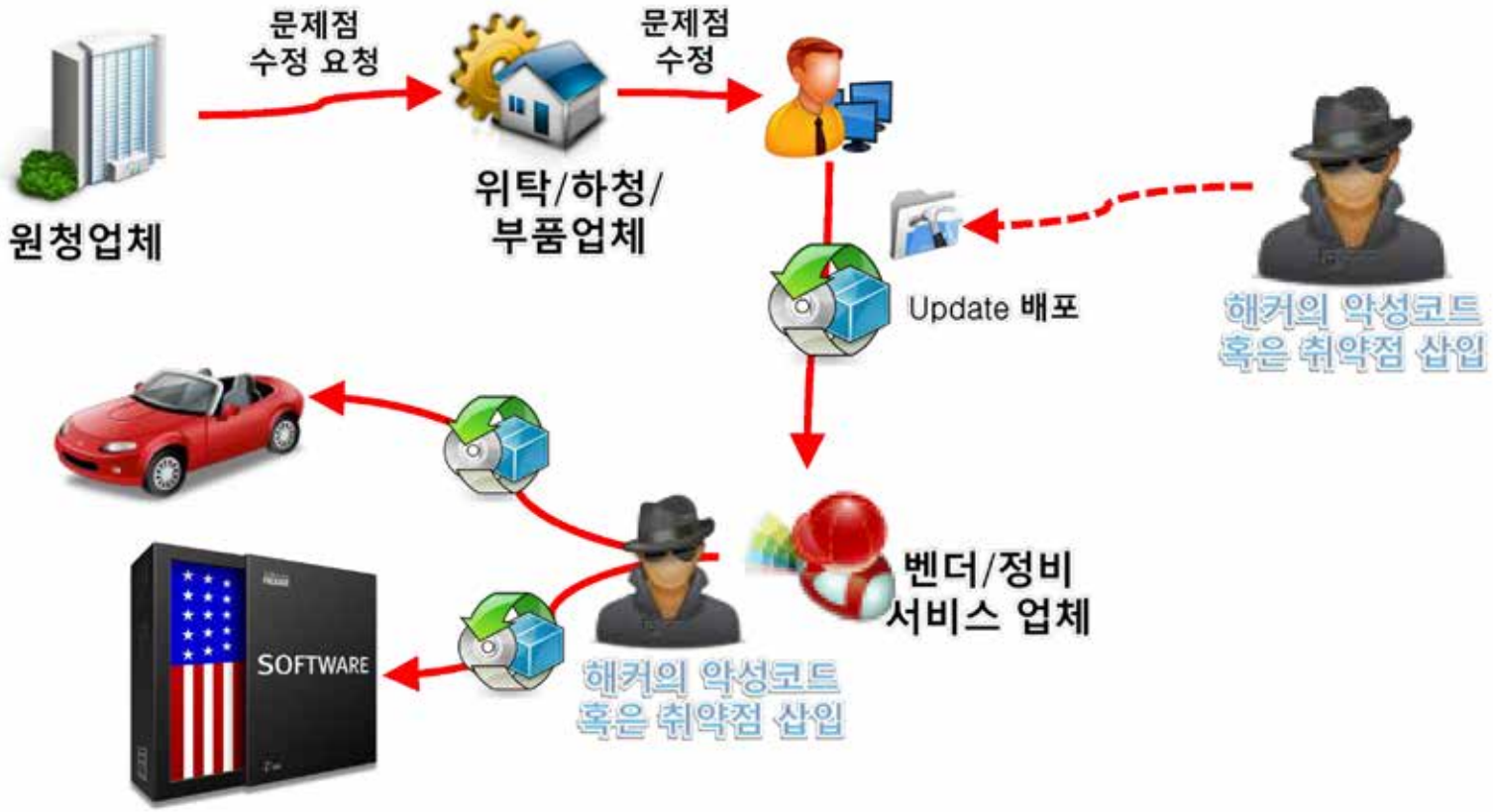


NetSarang Supply-chain Attack Process

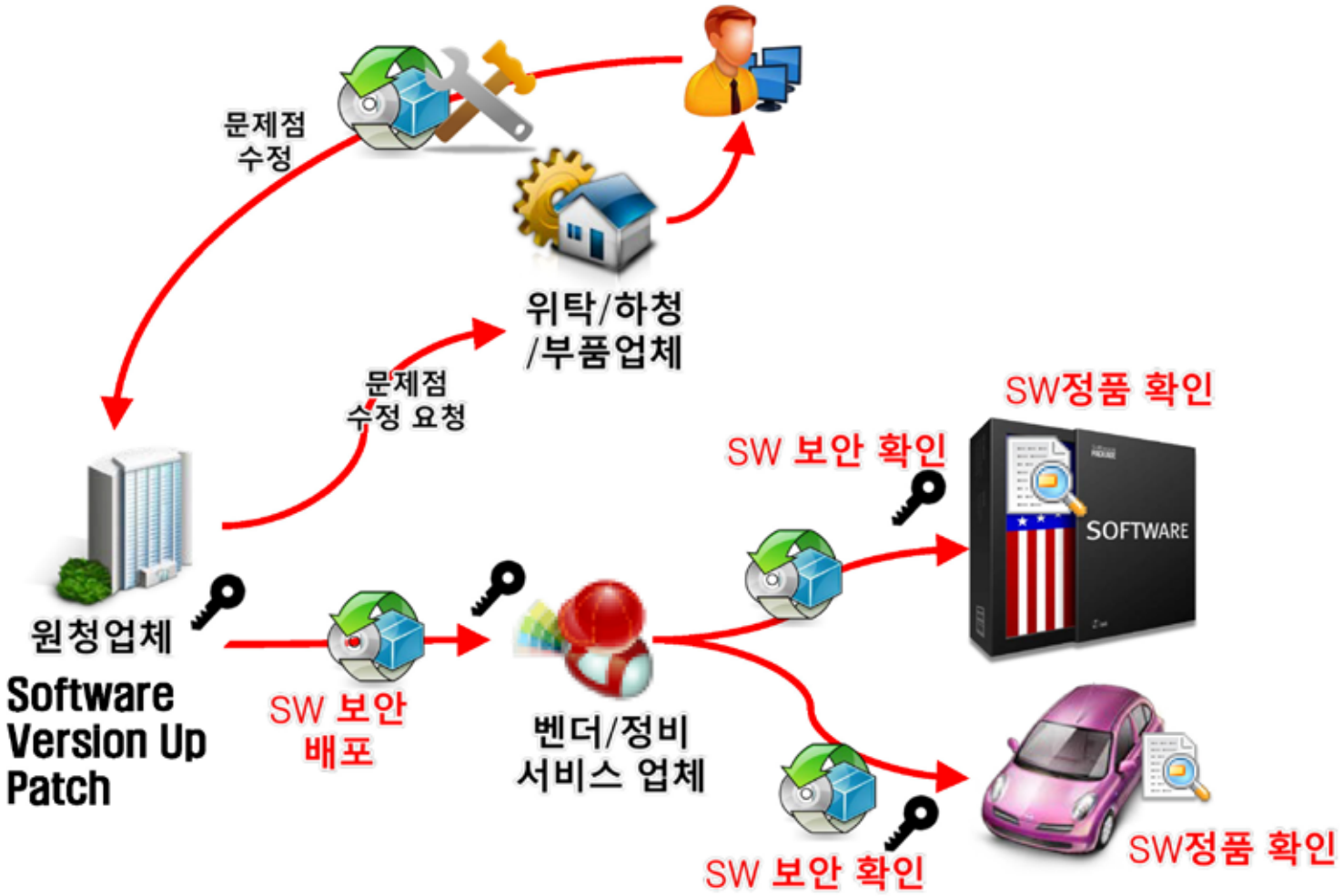
- 넷사랑컴퓨터 – 서버와 어플리케이션을 원격에서 관리하는 프로그램 공급
- 2017년 8월 공격자는 빌드 서버에 침입하여, 배포 패키지 빌드에 사용되는 정상 파일 대신에 Shadowpad 악성코드가 삽입된 파일로 교체
- 감염된 사용자들의 PC는 프로그램을 업데이트 함과 동시에 설치된 Shadowpad 악성코드를 통하여 PC에 저장되어 있는 사용자 정보를 C&C 서버로 전송
- 소프트웨어 [illegible]



Supply Chain Threats

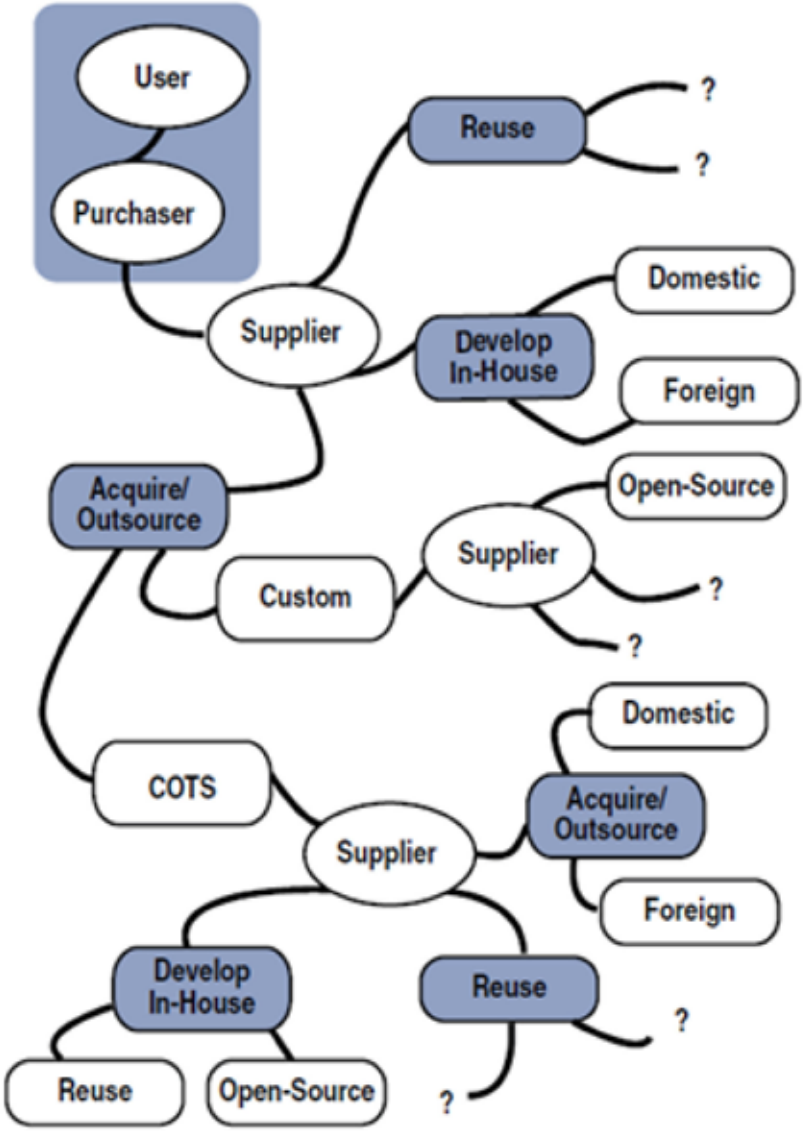


Supply Chain Threats Countermeasure



Supply Chain

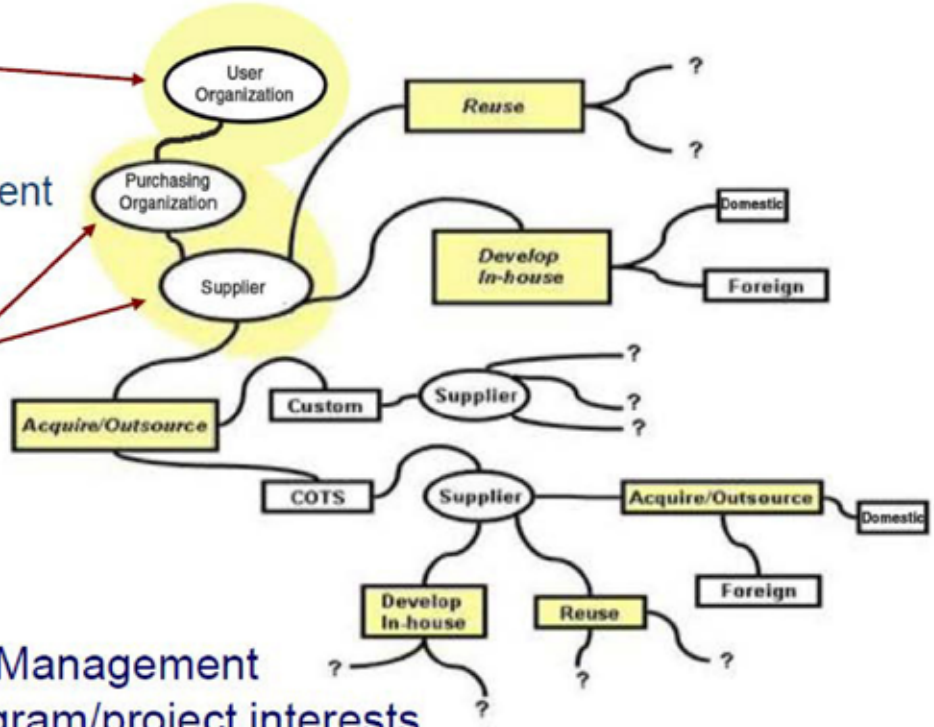
- ICT 제품은 전 세계 여러 벤더에 의해 조립, 구축 및 운송.
- 소프트웨어에는 자체개발, 외주개발, 재사용 가능한 라이브러리, 사용자 정의 코드, 상용 제품, 오픈 소스 등 일부 혹은 모두가 포함됨.
- 공급망 보안
  - 스토리지 및 처리량 노드
  - 운송라인 (& 커뮤니케이션)
- 공급망 복원력
  - 다중 자원
  - 멀티노드
  - 멀티 루트
- 제품 무결성
  - 글로벌 공급망에서 제공하는 HW, SW & Services에 대한 신뢰와 신뢰도를 어떻게 향상시키고 있는가?



韓 根熙

SCRM

- Enterprise-Level:
  - Regulatory compliance
  - Changing threat environment
  - Business Case
- Program/Project-Level:
  - Cost
  - Schedule
  - Performance



Software Supply Chain Risk Management traverses enterprise and program/project interests

1. 계약서에 소프트웨어 보증 요구사항을 삽입하고 시행.
2. IT 보안 정책을 검토하여 기업 네트워크 및 데이터의 모든 사용자가 미션과 관련하여 가능한 가장 엄격한 보안 정책을 준수하는지 확인.
3. 조직이 어느 정도의 리스크를 감당할 수 있는지, 그 리스크에 대한 책임은 누구에게 있는지 판단

SCRM Approach

- Ensure SCRM is a part of RFP/Contract document
- Use essential security and foundation practices
- Use ISO 27001 (ISMS) Framework (focus on ISO 27002)
- Leverage Support Standard (ISO/IEC 27036)
- Use Guidance from NIST 800-161

- Practices
  - Management Systems: ISO 9001 -Quality, ISO 27001 -Information Security, ISO 20000 -IT Service Management, ISO 28000 -Supply Chain Resiliency
  - Security Controls: ISO/IEC 27002, NIST 800-53, NIST 800-161
  - Lifecycle Processes: ISO/IEEE 15288 -Systems, ISO/IEEE 12207 -Software
  - Risk Management: ISO 31000 -overall, ISO/IEC 27005 -security, and ISO/IEC 16085 -systems
  - Industry Best Practices: CMMI, Assurance Process Reference Model, COBIT, ITIL, PMBOK, eSCM

US EO 13873

2019.5.15 US President's EO 13873

- 1977년 제정된 International Emergency Economic Powers Act(국제긴급경제권한법)에 기초
- "정보통신 기술 및 서비스 공급망 확보에 관한 행정명령"(Executive Order on Securing the Information and Communications Technology and Services Supply Chain)
- 미국의 국가 안보를 침해하고 미국 기업들의 기술 유출을 시도하는 타국의 ICT (하드웨어, 소프트웨어, 서비스 등) 분야 기업들에 대한 미국 기업들의 거래를 전면적으로 금지
  - 기존의 거래를 유지하거나 새로운 거래를 시도할 때에는 미합중국 상무부에 허가 신청
  - 상무부와 미국 재무부 등 관련 부처에서 최장 180일 간 심의를 거친 후 허가 여부 결정
  - 2019년 기준 이란, 러시아, 중국, 예멘, 리비아, 시리아, 베네수엘라, 북한, 레바논, 남수단, 수단, 짐바브웨, 콜롬비아 등에 적용

CISA ICT SUpply Chain Methodology – 200115 .pdf

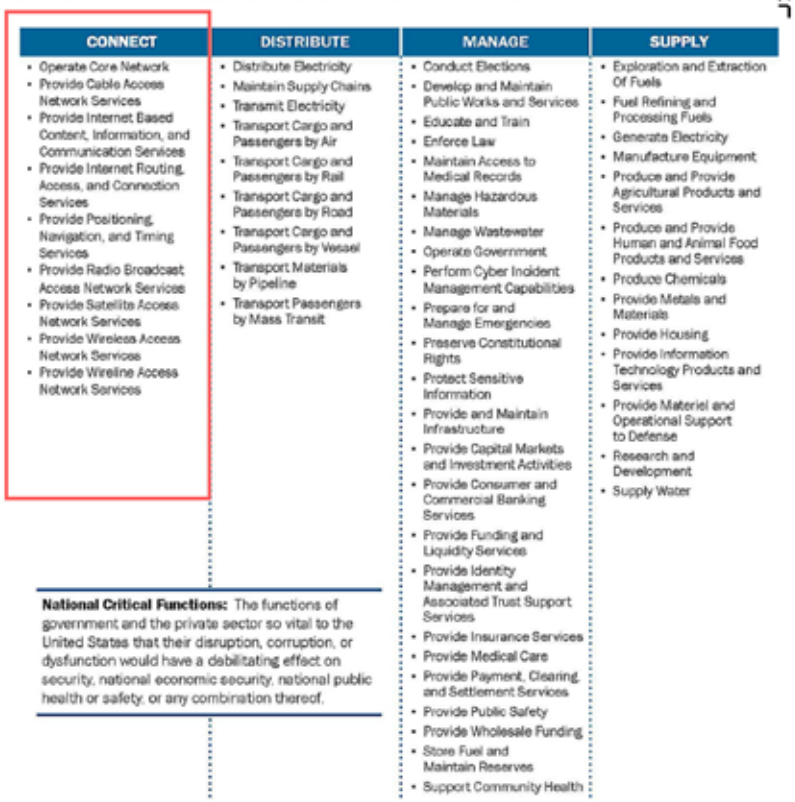
Supply Chain Methodology (SCM)

- EO 13738에 의해 SCM을 개발: DHS CISA 주관으로 ICT 공급망에 대한 취약성을 2단계로 평가
  - 1. ICT Framework 내에 ICT 요소 등급 식별
  - 2. ICT 요소 등급에 대한 평가
- Phase 1 preparation – Decomposition를 해서 NCFs(국가중요기능) 식별

The CISA initial assessment focused on the following National Critical Functions (NCFs) within the "Connect" theme:

- **Operate Core Network**
- **Provide Cable Access Network Services**
- **Provide Internet Routing, Access, and Connection Services**
- **Provide Radio Broadcast Access Network Services**
- **Provide Satellite Access Network Services**
- **Provide Wireless Access Network Services**
- **Provide Wireline Access Network Services**

While not all "Connect" NCFs were addressed, due to the cross-cutting nature of ICT, some NCFs are indirectly addressed due to ICT dependencies.



Phase 1 Identify classes of ICT Elements

❑ 일반화된 ICT 프레임워크 내에서 ICT 요소의 분류 식별 : CISA는 산업계 및 정부 기관과 협력하여 선택된 "연결" 테마 NCFs를 ICT 요소와 그 요소가 가능하게 하는 기능적 역할 및 하위 역할로 분해(Decomposition)

Local User Access	Transmission	Storage	Processing	System Management
Broadcast Networks	Core Networking Systems	Storage & Cloud Based Services	End User & Edge Networking Equipment	Security & Operations
Wireless Local Area Networks	Long and Short Haul Networks			
Mobile Networks				
Satellite Access Points				
Cable Access Points				
Wireline Access Points				

- Draws upon existing ICT industry and DHS architecture concepts (e.g., Sector Specific Plans, Risk Assessments, etc.)
- Can be progressively elaborated to include sufficient detail based on specific analytical objectives
- Organizing ICT elements by roles and sub-roles helps bin elements in a way that enables determination of basic judgements about criticality

Phase 2: Assess ICT Element Classes

Determine Criticality. Criticality is determined by analyzing each element based on the sub-role it supports and core factors exhibited. DHS assessed the criticality of each ICT element in the context of the function it supports.

Criticality Criteria:

- Does the element perform a security function?
- If the element fails, can operations continue?
- Does the element transmit, store, or receive critical data?
- Does the element have security features?
- Mitigation
  - If a device has known vulnerabilities, is it possible to manage risk through known, reliable mitigation measures?
  - If compromised, can its compromise be readily identified and mitigated?

Criticality Determinations

The National Risk Management Center (NRMC) makes final ICT element criticality determinations. ICT elements will receive one of the following determinations:

- **Critical:** Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.
- **Manageably Critical:** Compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.
- **Not Critical:** Compromise of the element is unlikely to have significant regional or national impacts.

Roadmap for Selecting Applicable Standards

	USING NIST	NO CURRENT FRAMEWORK	USING ISO/IEC	USING Sector-specific or Organization-specific
Security Framework	NIST RMF SP 800-53	NIST CSF	ISO/IEC 27001 ISO/IEC 27002	Sector-specific or Organization-specific
Cyber Supply Chain	NIST SP 800-161 NIST IR 7622**		ISO/IEC 27036 ISO/IEC 20243	FFIEC and OCC Guidelines IEC/ISA 62443-2-4 FS ISAC Third Party Software Security Control Types Cybersecurity Procurement Language for Energy Delivery Systems
Sector-Specific	NIST SP 800-82 NIST IR 7628	Energy Sector Cybersecurity Framework Implementation Guidance Cybersecurity and Risk Management Best Practices: CSRIC WG4	ISO/IEC 27011 ISO/IEC 27015 ISO/IEC 27019	NERC CIP; C2M2 CSRIC
Software Integrity	SAFECode Software Integrity Documents			
Delivery Security	ANSI/ESD S20.20-2007; C-TPAT; AEO; TAPA; Electronics Industry Citizenship Coalition (EICC); Dodd-Frank Conflict Mineral Requirements			
Counterfeits	SAE Standards			
Conformity Assessment	Common Criteria; The Open Group Trusted Supplier Program; A2LA Accreditation; ISO 9001 Certification			

NIST CSF v1.1

CyberSecurity Framework V.1.1 (2018. 4. 16)

- EO 13636 Improving Critical Infrastructure Cybersecurity – 2013. 2. 19
- Cybersecurity Framework v.1.0 – 2014. 2

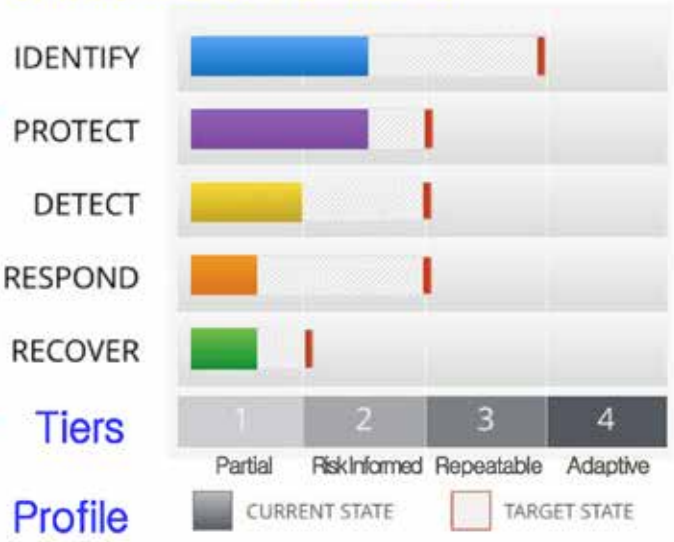
Core

The Core consists of three parts: Functions(5), Categories(23), and Subcategories(108).

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

Subcategory	Informative References
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.15.1.3, 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** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Functions



韓 根熙

NIST CSF v1.1 : SCRM 도입

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		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	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

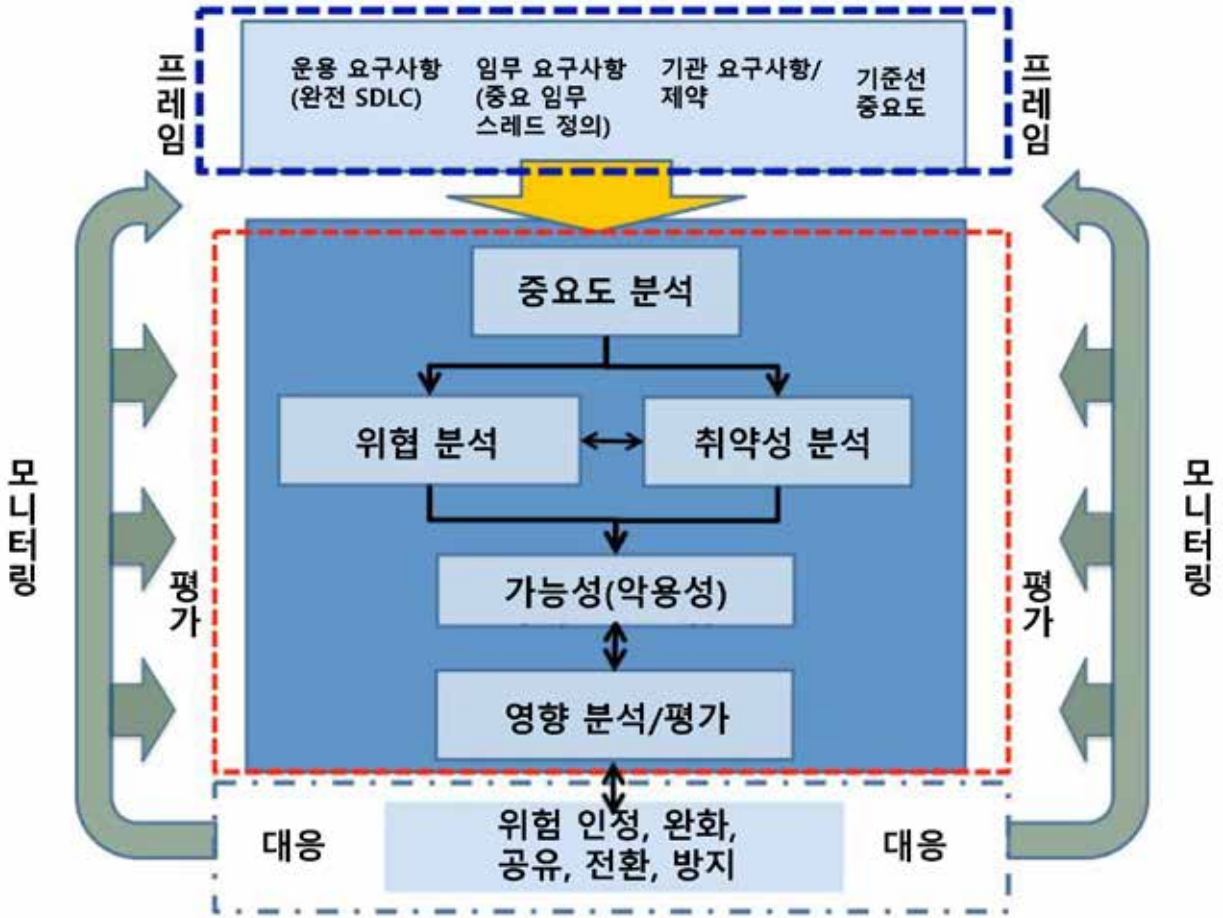
NIST IR 7622

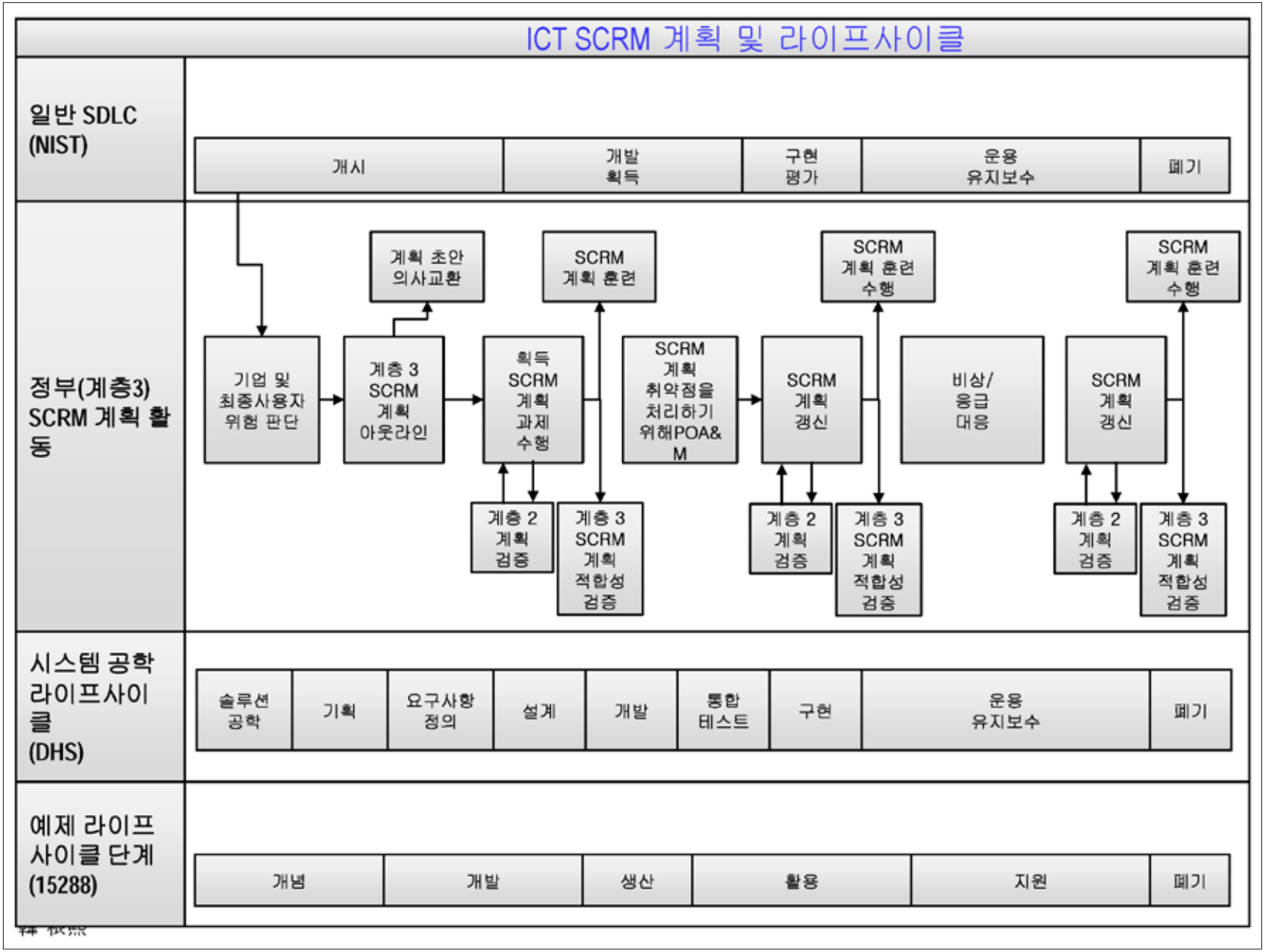
- 법규 FISMA(Federal Information Security Modernization Act, 2012.12), PL(Public Law) 107-347 적용
- 연방 기관이 ICT 공급망 위험 관리를 위하여 ICT 제품 및 서비스를 도입할 경우 고려해야 할 사항들을 명시
- 공급망 위험 관리에 대한 전체적인 배경 지식을 제공
- 시스템 및 소프트웨어 공학, 정보보호, 소프트웨어 보증, 공급망 및 물류, 취득 등에서의 공급망 관리 사례를 포함

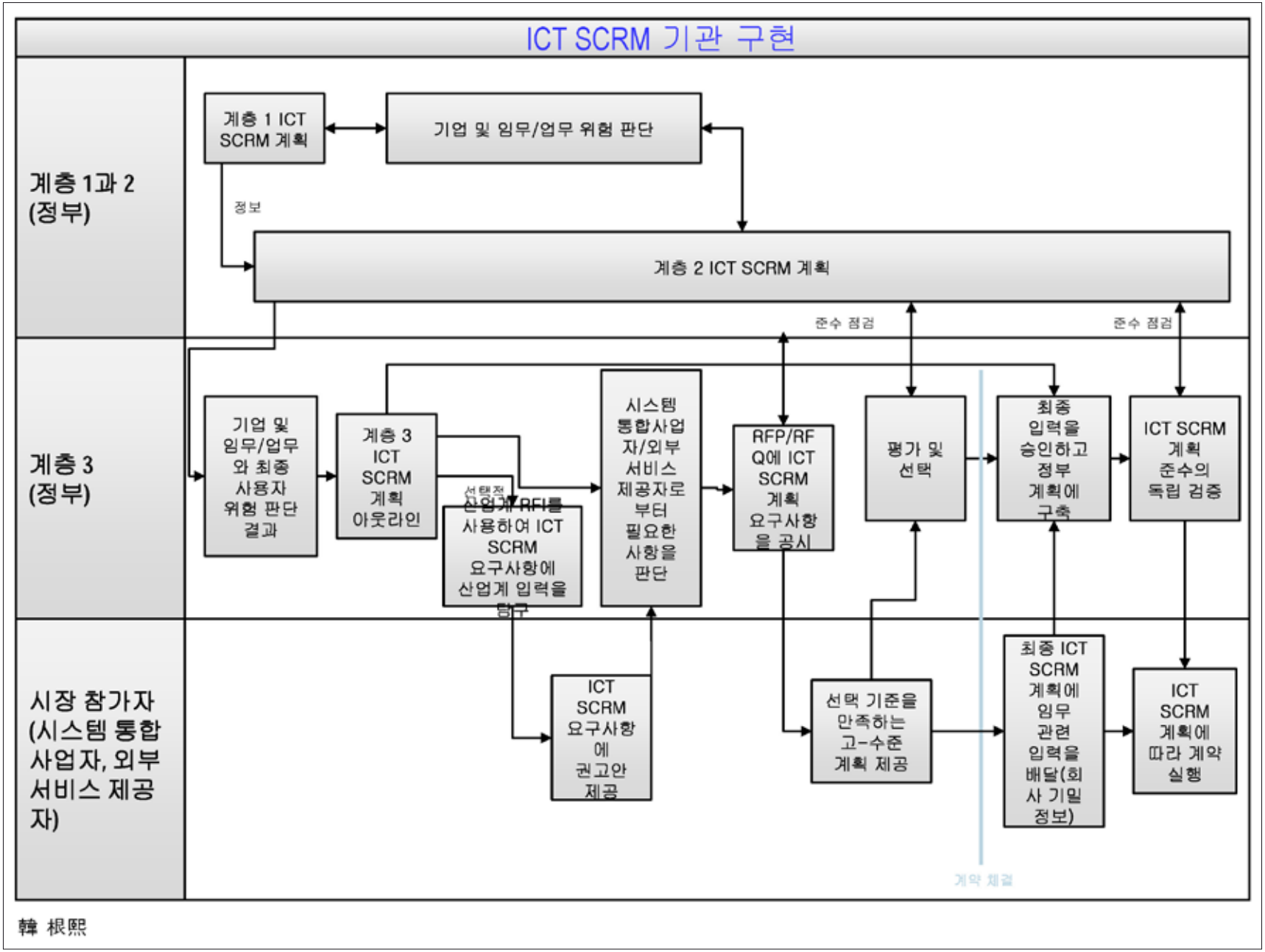
NIST SP 800-161 SCRM

- FISMA(Federal Information Security Modernization Act, 2012.12), PL(Public Law) 107-347 법규 적용
- FIPS 199, NIST SP 800-30 Rev.1, NIST SP 800-37 Rev.2, NIST SP 800-39, NIST SP 800-53 Rev.5 문서들을 기반으로 작성
- ICT 공급망 위험 관리는 기관에서 관리하는 하드웨어 및 소프트웨어를 포함한 모든 ICT 제품과 서비스의 생명주기 전반을 대상
  - 연구개발, 설계, 제조 및 운영 단계부터 처분, 폐기까지의 모든 활동을 포함
- 공급망 과정 내 제품 무단 생산, 변조, 도난, 악성 소프트웨어 및 하드웨어 삽입, ICT 공급망의 제조 및 개발 관행 부실 등 을 공급망 위험 요소로 지정
- 연방 기관이 ICT 공급망 위험 관리를 위하여 ICT 제품 및 서비스를 도입할 경우 고려해야 할 사항들을 명시
- 공급망 위험 관리에 대한 전체적인 배경 지식을 제공
- 시스템 및 소프트웨어 공학, 정보보호, 소프트웨어 보증, 공급망 및 물류, 취득 등에서의 공급망 관리 사례를 포함

NIST SP 800-161 SCRM




ICT SCRM 계획 및 라이프사이클
일반 SDLC (NIST)
개시
개발 획득
구현 평가
운용 유지보수
폐기
정부(계층3) SCRM 계획 활동
기업 및 최종사용자 위험 판단
계획 초안 의사교환
계층 3 SCRM 계획 아웃라인
획득 SCRM 계획 과제 수행
SCRM 계획 훈련
계층 2 계획 검증
계층 3 SCRM 계획 적합성 검증
SCRM 계획 취약점을 처리하기 위해POA&M
SCRM 계획 갱신
SCRM 계획 훈련 수행
계층 2 계획 검증
계층 3 SCRM 계획 적합성 검증
비상/ 응급 대응
SCRM 계획 갱신
SCRM 계획 훈련 수행
계층 2 계획 검증
계층 3 SCRM 계획 적합성 검증
시스템 공학 라이프사이클 (DHS)
솔루션 공학
기획
요구사항 정의
설계
개발
통합 테스트
구현
운용 유지보수
폐기
예제 라이프사이클 단계 (15288)
개념
개발
생산
활용
지원
폐기


ICT SCRM 기관 구현
계층 1과 2 (정부)
계층 3 (정부)
시장 참가자 (시스템 통합 사업자, 외부 서비스 제공자)
계층 1 ICT SCRM 계획
기업 및 임무/업무 위험 판단
정보
계층 2 ICT SCRM 계획
준수 점검
준수 점검
기업 및 임무/업무와 최종 사용자 위험 판단 결과
계층 3 ICT SCRM 계획 아웃라인
산업계 RFI를 사용하여 ICT SCRM 요구사항에 산업계 입력을 탐구
시스템 통합사업자/외부 서비스 제공자로부터 필요한 사항을 판단
RFP/RFQ에 ICT SCRM 계획 요구사항을 공시
평가 및 선택
최종 입력을 승인하고 정부 계획에 구축
ICT SCRM 계획 준수의 독립 검증
ICT SCRM 요구사항에 권고안 제공
선택 기준을 만족하는 고-수준 계획 제공
최종 ICT SCRM 계획에 임무 관련 입력을 배달(회사 기밀 정보)
ICT SCRM 계획에 따라 계약 실행
계약 체결
韓 根熙

ICT SCRM 제어 항목 사례

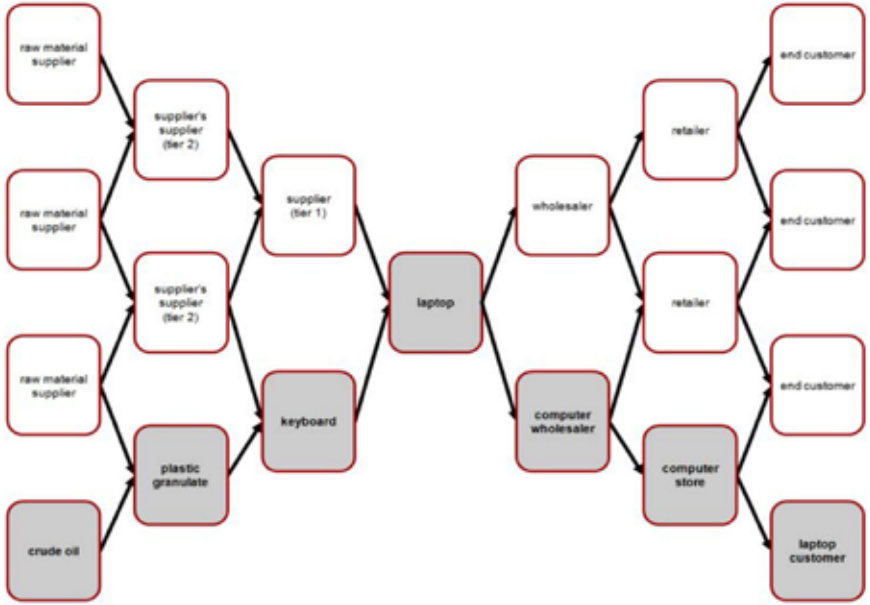
Control No.	제어 이름 / 제어 기능 향상 이름	800-53 r4 높은 기준	SCRM 기준	단계 Tier 1	2	3
AC-1	액세스 제어 정책 및 절차	X	X	X	X	X
AC-2	계정 관리	X	X		X	X
AC-3	액세스 집행	X	X		X	X
AC-3 (8)	액세스 집행 | 액세스 권한의 해지		X		X	X
AC-3 (9)	액세스 집행|제어된 릴리즈		X		X	X
AC-4	정보 흐름 집행	X	X		X	X
AC-4 (6)	정보 흐름 집행 | 메타데이터		X		X	X
AC-4 (17)	정보 흐름 집행 | 도메인 인증				X	X
AC-4 (19)	정보 흐름의 집행 | 메타 데이터의 유효성				X	X
AC-4 (21)	정보 흐름의 집행 | 정보의 물리적/논리적 분리 흐름					X
AC-5	의무의 분리	X	X		X	X
(AC-6)	(최소 권한)	(X)	(N/A)			
AC-6 (6)	최소 권한|비 조직의 사용자가 권한있는 액세스		X		X	X
AC-17	원격 액세스	X	X		X	X
AC-17 (6)	원격 액세스 | 정보의 보호		X		X	X
AC-18	무선 액세스	X	X	X	X	X
AC-19	모바일 장치를 위한 액세스 제어	X	X		X	X
AC-20	외부 정보 시스템의 사용	X	X	X	X	X

ICT SCRM TF

- 2018년 7월 DHS(미국 국토안보부, U.S. Department of Homeland Security)는 국가적 공급망 위험 관리를 위한 태스크포스(ICT Supply Chain Risk Management Task Force)를 신설.
- 미국 ICT 공급망에 대한 위험을 식별하고 관리하기 위한 권고안을 작성하기 위해 신설되었으며 정부 기관과 민간 기업이 공동으로 참여
- DHS National Protection and Programs Directorate's(NPPD) Cyber Supply Chain Risk Management (C-SCRM) 프로그램의 일부로써, 연방정부기관을 위해 공급망 위험 관리 기능을 개발 및 배포.
- TF는 기존의 공급망 위험 관리 방안을 조사하여 목록화하는 것 이외에 아래 4가지의 주요 계획안을 발표.
  - 정부와 산업계 간 공급망 위험에 대한 정보의 양방향 공유를 위하여 공통된 위험 관리 프레임 워크 개발
  - ICT 공급, 제품 및 서비스의 위협 기반 평가를 위한 프로세스 및 평가 기준 정립
  - 적격 입찰자 및 제조업체의 목록에 대한 시장 식별 및 평가 기준 정립
  - 제품의 제조업체 또는 공인된 판매업체로부터 ICT 구매를 장려하기 위한 정책 권고안 작성

Supply Chain Assurance
공급망 보증

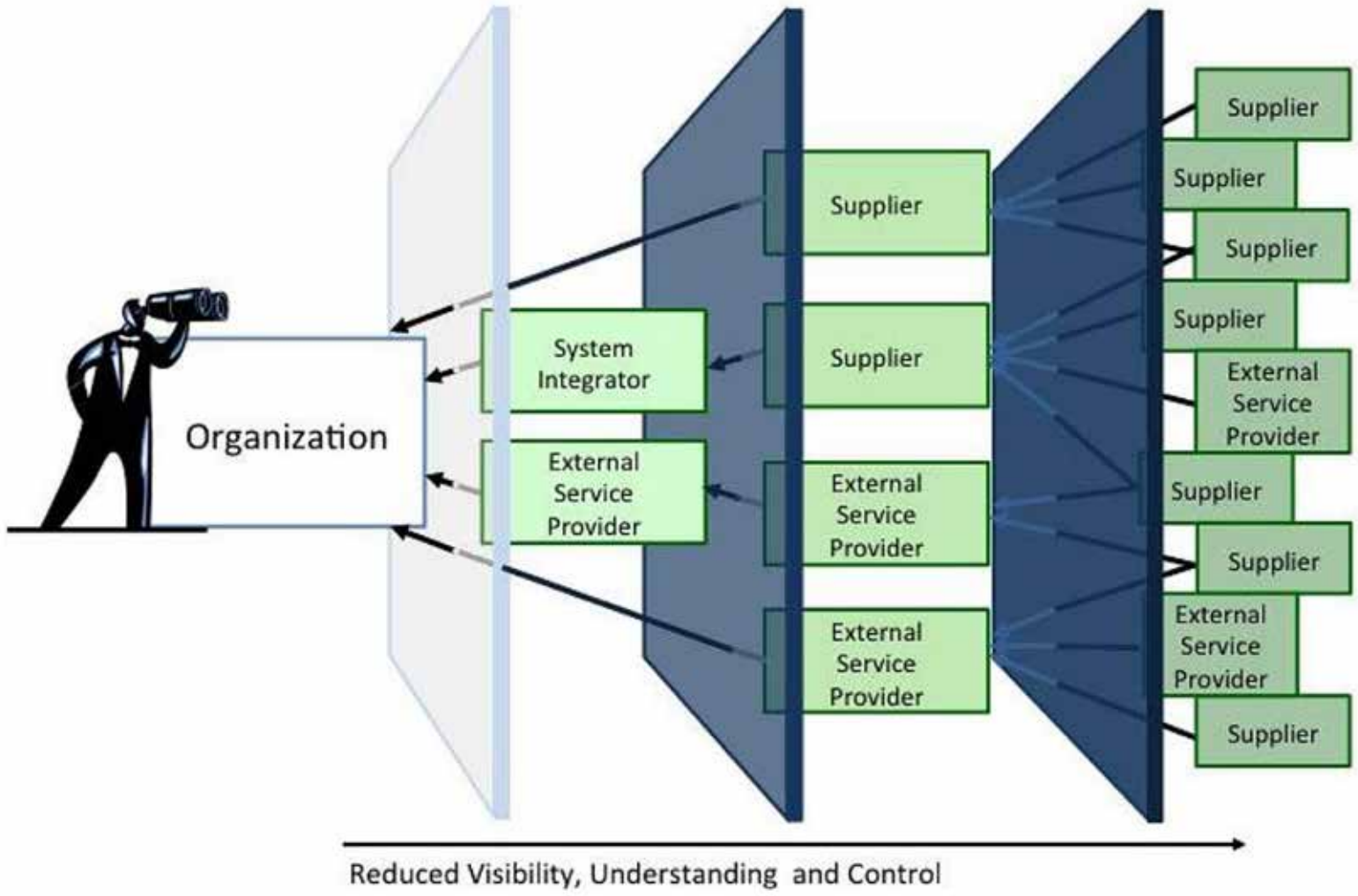
Supply Chain Test



- 공급망 사슬 위험관리 (Supply Chain Risk Management)
  - "The World is Flat", Thomas L, Friedman, 2005 → 2013. Feb 개정판 출간
  - 메릴랜드 집에서 델 고객서비스센터(인도에 위치)에 노트북 전화 주문후 추적
  - 하드웨어 : 공동설계(오스틴 델 엔지니어팀 + 대만), 마더보드 설계(대만), 마더보드 생산(대만 혹은 중국), 인텔 프로세서(필리핀, 코스타리카, 말레이시아, 혹은 중국), 메모리(삼성, 독일 혹은 일본), 그래픽 카드(중국), 키보드(중국), 무선랜(말레이시아, 대만, 중국), 하드디스크(싱가폴, 태국), 컴퓨터 조립(말레이시아 페낭), 배송(미국 UPS 택배사) : 전체 공급망 사슬은 모든 하위 제조업체까지 약 400여개 회사로 구성
  - 소프트웨어 : 운영체제(4,000만 LOC, 전 세계 10여 국가 지역에서 작성)
- 복잡하고 역동적인 수요/공급 네트워크에서 공급망을 어떻게 신뢰할 수 있는가?

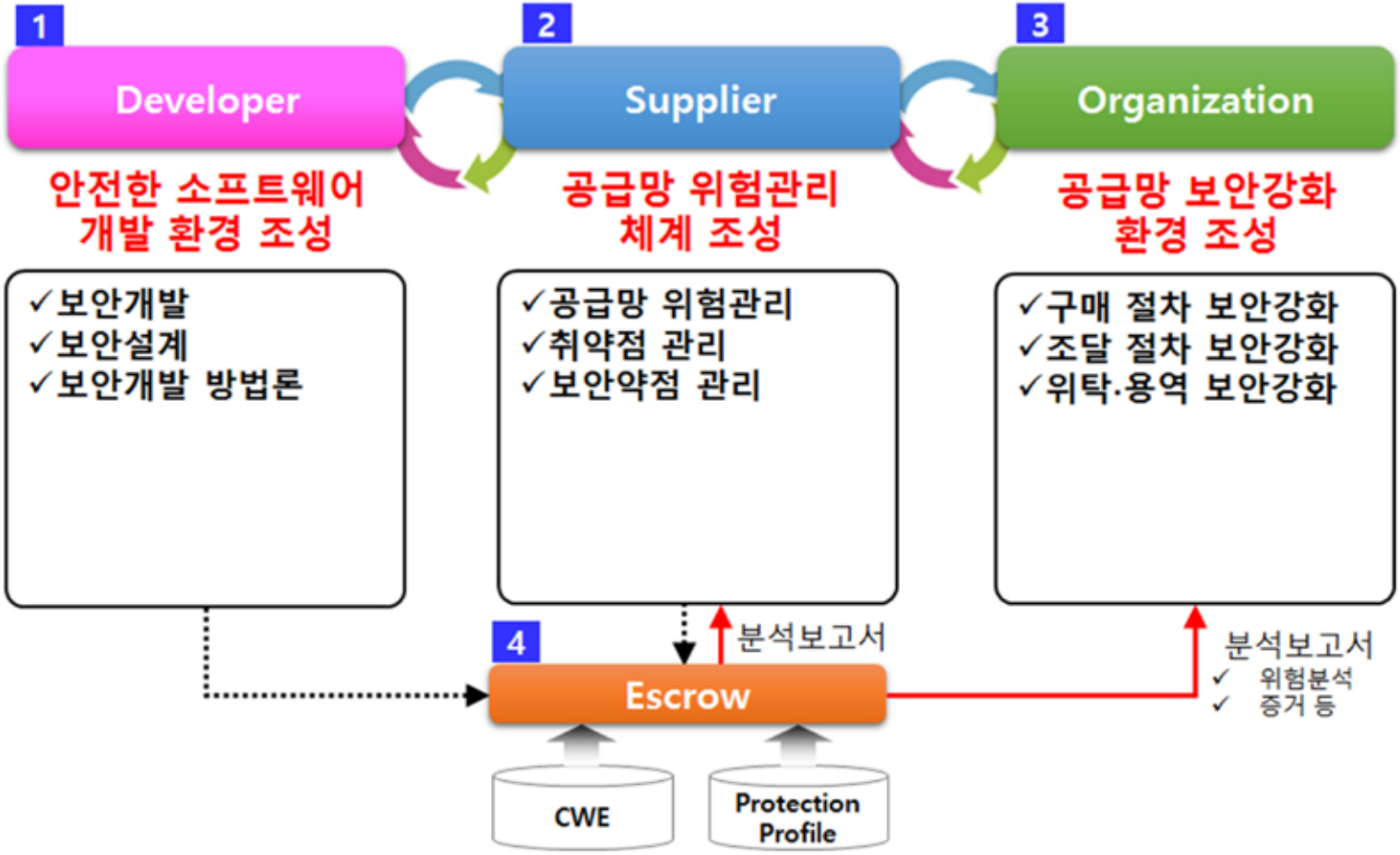
韓 根熙

Visibility, Understanding, and Control



韓 根熙

공급망 보안(Supply Chain Security) 강화 방안



출처 : KISA, 상용 및 공개 SW 도입 시 보안성 점검 동향 조사 연구(2015.11)

Acquirer취득자 & Supplier공급자 관계 유형

- 시스템은 취득자가 소유하고, 공급자가 관리하는 ICT 시스템 관리 지원
- 시스템 또는 자원이 공급자에 의해 소유되고 관리되는 ICT 시스템 또는 서비스 제공자.
- 공급자가 ICT 제품 생산과 관련된 서비스의 전부 또는 일부를 제공하는 제품 개발, 설계, 엔지니어링 및 구축.
- 상용 제품 공급업체
- 오픈 소스 제품 공급업체 및 유통업체.

제품 취득에 따른 보안 위험 사례

	유형	설명
1	보안 기능 (Feature)	공급된 제품에 취약성이 있는 경우에는 취득자의 파생상품, 서비스 또는 프로세스가 취약할 수 있음.
2	품질	공급되는 제품의 품질 부진은 취득자의 파생상품, 서비스 및 프로세스의 보안 취약성을 야기할 수 있음.
3	지적 재산권	식별되지 않은 지적재산권은 취득자의 파생상품이나 서비스와 관련하여 나중에 분쟁 소지 발생 가능.
4	진본성 (Authenticity)	가짜 또는 사기성 제품이 공급된 경우, 지적 재산권의 인식, 품질과 보안 기능에 대한 취득자의 기대는 보안 약점이 도입되고 사업 관계 신뢰성의 상실을 초래할 수 있음.
5	보증	취득자는 적절한 정보보안 특징, 제품 품질, 지적재산권 및 진본성 파악에 대한 확신이 없으면 공급자의 제품에 대한 신뢰 하락.

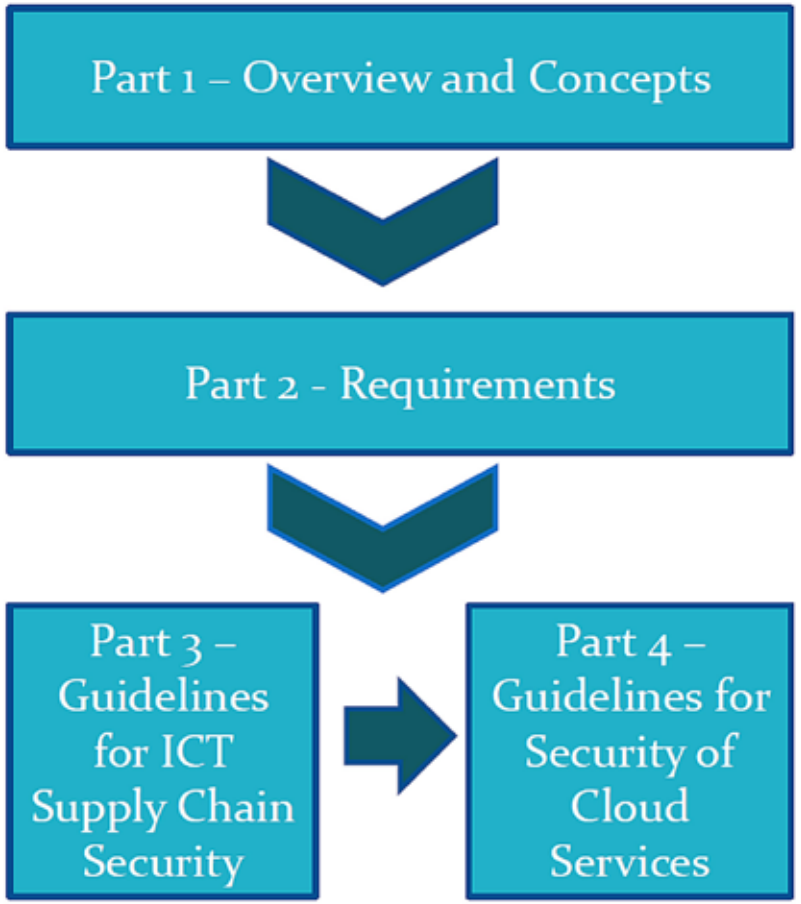
서비스 취득에 따른 보안 위험 사례

	유형	설명	사용(Use Case) 사례
1	현장에서(On site) 물리적접근	공급자는 취득자의 정보처리설비에 물리적으로 접근할 수 있지만 논리적으로 접근할 수 없다.	경비원 서비스, 배달 서비스, 청소 서비스 또는 장비 유지보수 서비스
2	현장에서 정보 및 정보 시스템에 대한 접속	공급자 직원은 현장에 있으며 취득자의 장비를 사용하여 취득자의 정보와 정보 시스템에 논리적으로 접근할 수 있다	취득자의 팀에 통합된 아웃소싱 전문 지식을 가진 현장 작업자.
3	사내 정보 및 정보 시스템에 대한 원격 액세스	공급자는 취득자의 정보 및 정보 시스템에 원격으로 접근할 수 있다.	원격 개발 및 유지보수 활동, 원격 정보 시스템 및 장비 관리, 물류, 콜 센터 운영, 자동화된 설비 관리 시스템.
4	외부(Off Site) 정보 처리	취득자의 책임 하에 있는 정보는 공급자가 통제하고 관리하는 응용 프로그램과 시스템을 사용하여 공급자가 외부에서 처리한다.	컨설팅(시장 조사, 판매 촉진, 기술 연구 등), 정보 처리, R&D, 제조, 저장 및 보관, 애플리케이션 서비스(ASP), 여행 또는 금융 서비스와 같은 비즈니스 프로세스(BPaaS), 서비스로서의 인프라(IaaS) 또는 서비스로서의 소프트웨어(SaaS) 제공자.
5	외부 애플리케이션	취득자가 운영하는 애플리케이션이 PaaS 또는 IaaS를 실행하고 있다.	공급업체가 개발 플랫폼을 제공하는 경우 서비스로서의 플랫폼(PaaS) 제공자 또는 공급업체가 네트워크, 컴퓨팅 및 스토리지 서비스를 제공하는 IaaS 제공자.
6	외부 장비	취득자가 소유한 취득자가 전용하는 장비가 공급자 사이트, 외부에 호스팅된다.	정보 시스템 하우징의 외부 호스팅 또는 IaaS.
7	외부 정보 저장	외부 보존 또는 보관을 위해 취득자는 정보 저장을 공급업체에 아웃소싱한다.	사내 정보 처리로 생성된 정보의 백업 복사본을 유지하기 위한 스토리지 서비스 이용.
8	소스 코드 위탁(Escrow)	취득자가 사용하는 공급자 작업품(Artefacts)이 포함된 서비스는 신뢰받는 제3자에게 위탁보관되고, 정해진 상황하에서 취득자가 사용 가능하게 된다.	소프트웨어 공급자가 폐업하는 경우에 취득자가 소프트웨어 사용성을 유지하기 위해 독립적 제3자에게 보관된 소스 코드.

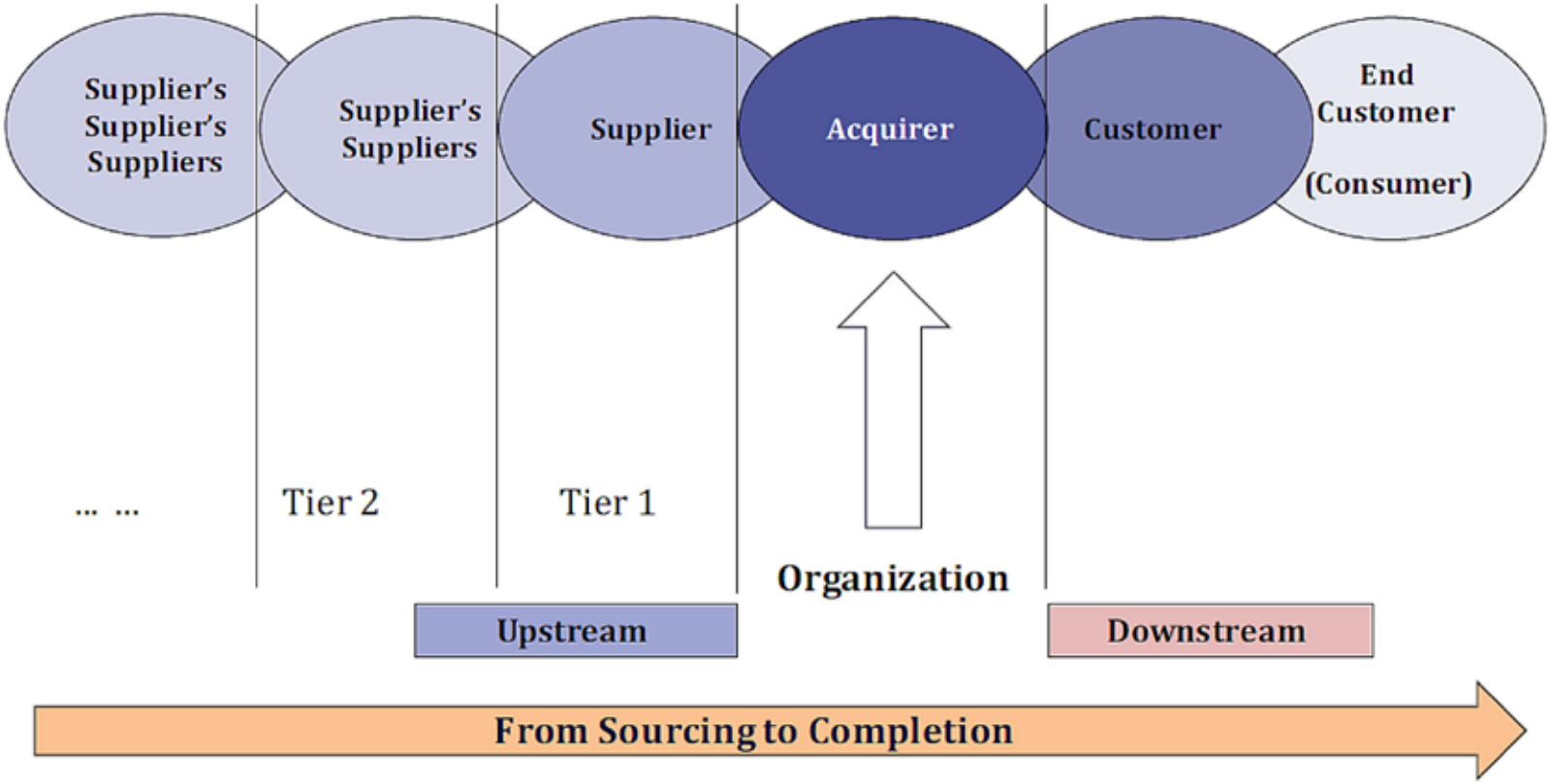
韓 根熙

ISO/IEC 27036

- Information Technology – Security Techniques – Information Security for Supplier Relationships
  - 획득자 및 공급업체 실행 해결
  - 보안에 영향을 미칠 수 있는 모든 유형의 기관(예: 상업, 공공 부문, 비영리 및 모든 유형의 공급업체 관계)에 적용
  - 시스템/소프트웨어 엔지니어링 및 정보 보안을 위한 ISO 표준과 조화



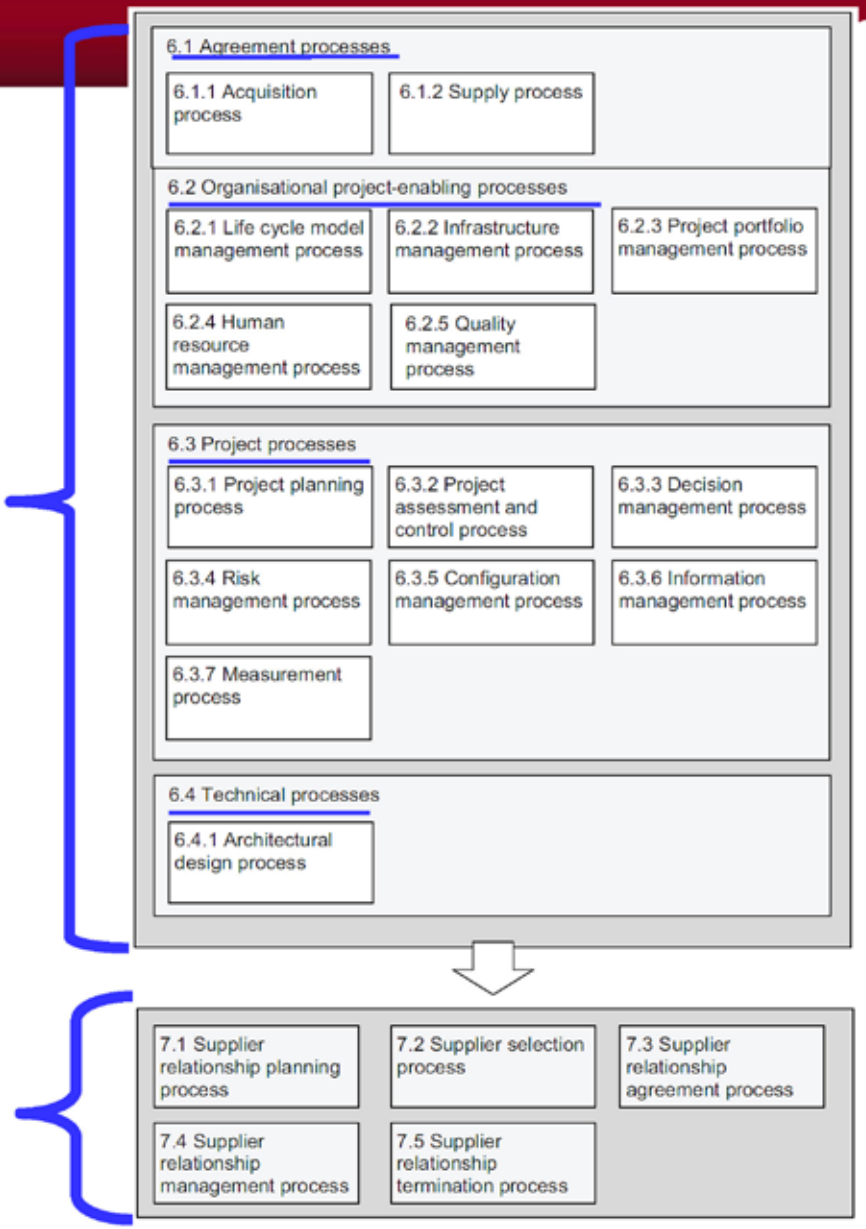
ISO 27036-1 Supply Chain Relationships

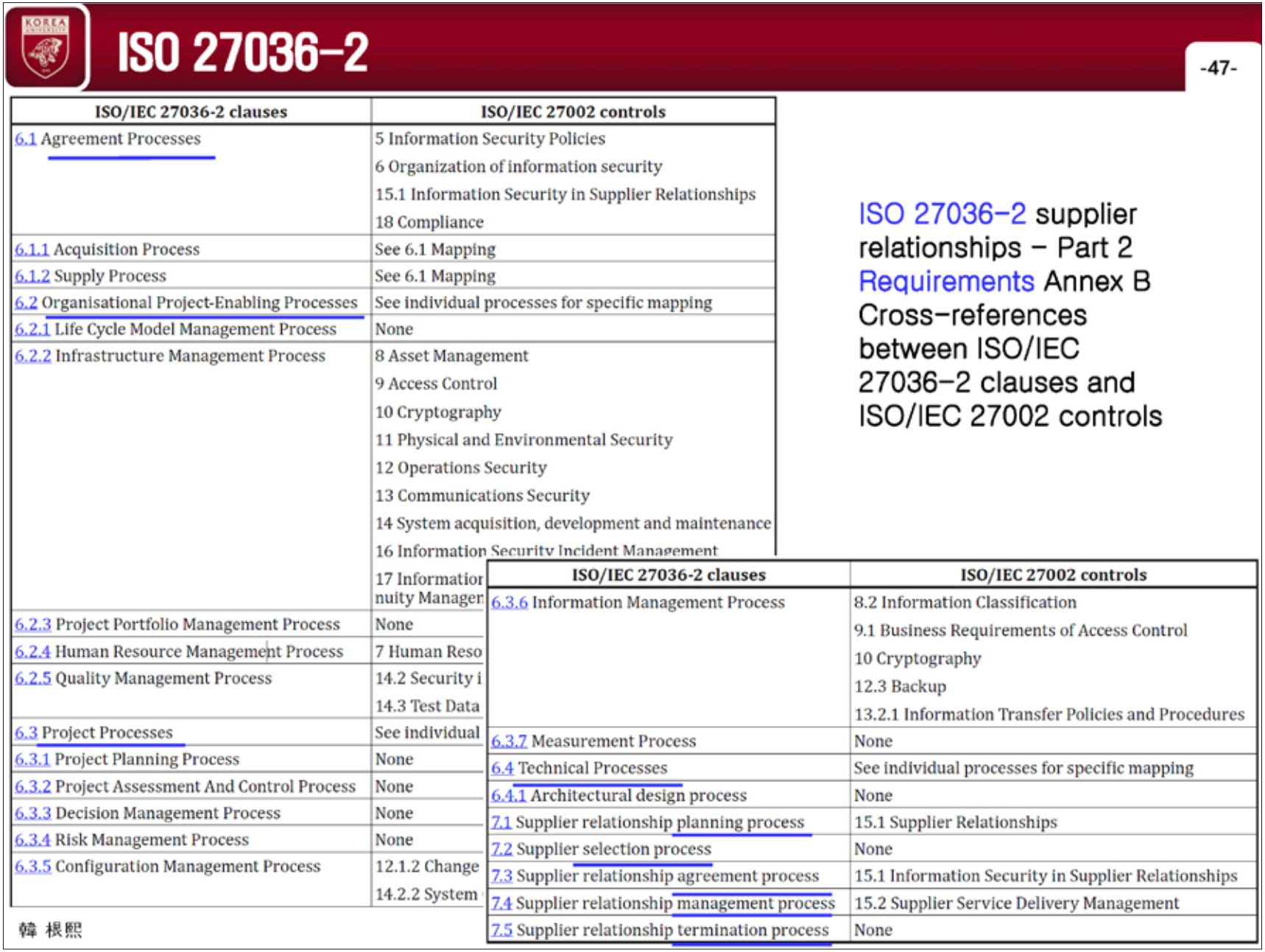


ISO/IEC 27036-1 Information security for supplier relationships - Overview and concepts

ISO 27036-2

- Information security for supplier relationships – Part 2: Requirements
- Fundamental and highlevel information security requirements for acquirers and suppliers as organizational scheme commonly applicable to instances of supplier relationship.
- 공급업체 관계의 사례에 일반적으로 적용할 수 있는 조직 체계로서 획득자와 공급자에 대한 기본적이고 높은 수준의 정보 보안 요건.
- 공급자 관계의 예를 수립하고 유지할 때 획득자와 공급자에 대한 기본적인 정보 보안 요건.
- amental information security requirements for acquirers and suppliers when establishing and maintaining an instance of supplier relationship.




ISO 27036-2
-47-
ISO 27036-2 supplier relationships – Part 2 Requirements Annex B Cross-references between ISO/IEC 27036-2 clauses and ISO/IEC 27002 controls
ISO/IEC 27036-2 clauses
ISO/IEC 27002 controls
6.1 Agreement Processes
5 Information Security Policies
6 Organization of information security
15.1 Information Security in Supplier Relationships
18 Compliance
6.1.1 Acquisition Process
See 6.1 Mapping
6.1.2 Supply Process
See 6.1 Mapping
6.2 Organisational Project-Enabling Processes
See individual processes for specific mapping
6.2.1 Life Cycle Model Management Process
None
6.2.2 Infrastructure Management Process
8 Asset Management
9 Access Control
10 Cryptography
11 Physical and Environmental Security
12 Operations Security
13 Communications Security
14 System acquisition, development and maintenance
16 Information Security Incident Management
17 Information
nuity Manager
6.2.3 Project Portfolio Management Process
None
6.2.4 Human Resource Management Process
7 Human Reso
6.2.5 Quality Management Process
14.2 Security i
14.3 Test Data
6.3 Project Processes
See individual
6.3.1 Project Planning Process
None
6.3.2 Project Assessment And Control Process
None
6.3.3 Decision Management Process
None
6.3.4 Risk Management Process
None
6.3.5 Configuration Management Process
12.1.2 Change
14.2.2 System
ISO/IEC 27036-2 clauses
ISO/IEC 27002 controls
6.3.6 Information Management Process
8.2 Information Classification
9.1 Business Requirements of Access Control
10 Cryptography
12.3 Backup
13.2.1 Information Transfer Policies and Procedures
6.3.7 Measurement Process
None
6.4 Technical Processes
See individual processes for specific mapping
6.4.1 Architectural design process
None
7.1 Supplier relationship planning process
15.1 Supplier Relationships
7.2 Supplier selection process
None
7.3 Supplier relationship agreement process
15.1 Information Security in Supplier Relationships
7.4 Supplier relationship management process
15.2 Supplier Service Delivery Management
7.5 Supplier relationship termination process
None
韓 根熙

- ISO 27036-3 supplier relationships – Part 3 Guidelines for ICT Supply Chain Security Annex A Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
6.1.1 Acquisition Process 6.1.1.1 Purpose The purpose of the Acquisition Process is to obtain a product or service in accordance with the acquirer's requirements.	6.1.2 Supply Process 6.1.2.1 Purpose The purpose of the Supply Process is to provide an acquirer with a product or service that meets agreed requirements.	6.1.1 Acquisition Process 6.1.1.1 Purpose The purpose of the Acquisition Process is to obtain the product and/or service that satisfies the need expressed by the acquirer. The process begins with the identification of customer needs and ends with the acceptance of the product and/or service needed by the acquirer.	6.1.2 Supply Process 6.1.2.1 Purpose The purpose of the Supply Process is to provide a product or service to the acquirer that meets the agreed requirements.
6.1.1.2 Outcomes As a result of the successful implementation of the Acquisition Process: a) A strategy for the acquisition is established. b) One or more suppliers are selected. c) Communication with the supplier is maintained. d) An agreement to acquire a product or service according	6.1.2.2 Outcomes As a result of the successful implementation of the Supply Process: a) An acquirer for a product or service is identified. b) A response to the acquirer's request is made. c) An agreement to supply a product or service according to defined acceptance criteria is established.	6.1.1.2 Outcomes As a result of successful implementation of the Acquisition Process: a) acquisition needs, goals, product and/or service acceptance criteria and acquisition strategies are defined; b) an agreement is developed that clearly expresses the expectation, responsibilities and liabilities of both the	6.1.2.2 Outcomes As a result of successful implementation of the Supply Process: a) an acquirer for a product or service is identified; b) a response to an acquirer's request is produced; c) an agreement is established between the acquirer and the supplier for developing, maintaining, operating, packaging, delivering, and

ISO 27036-3

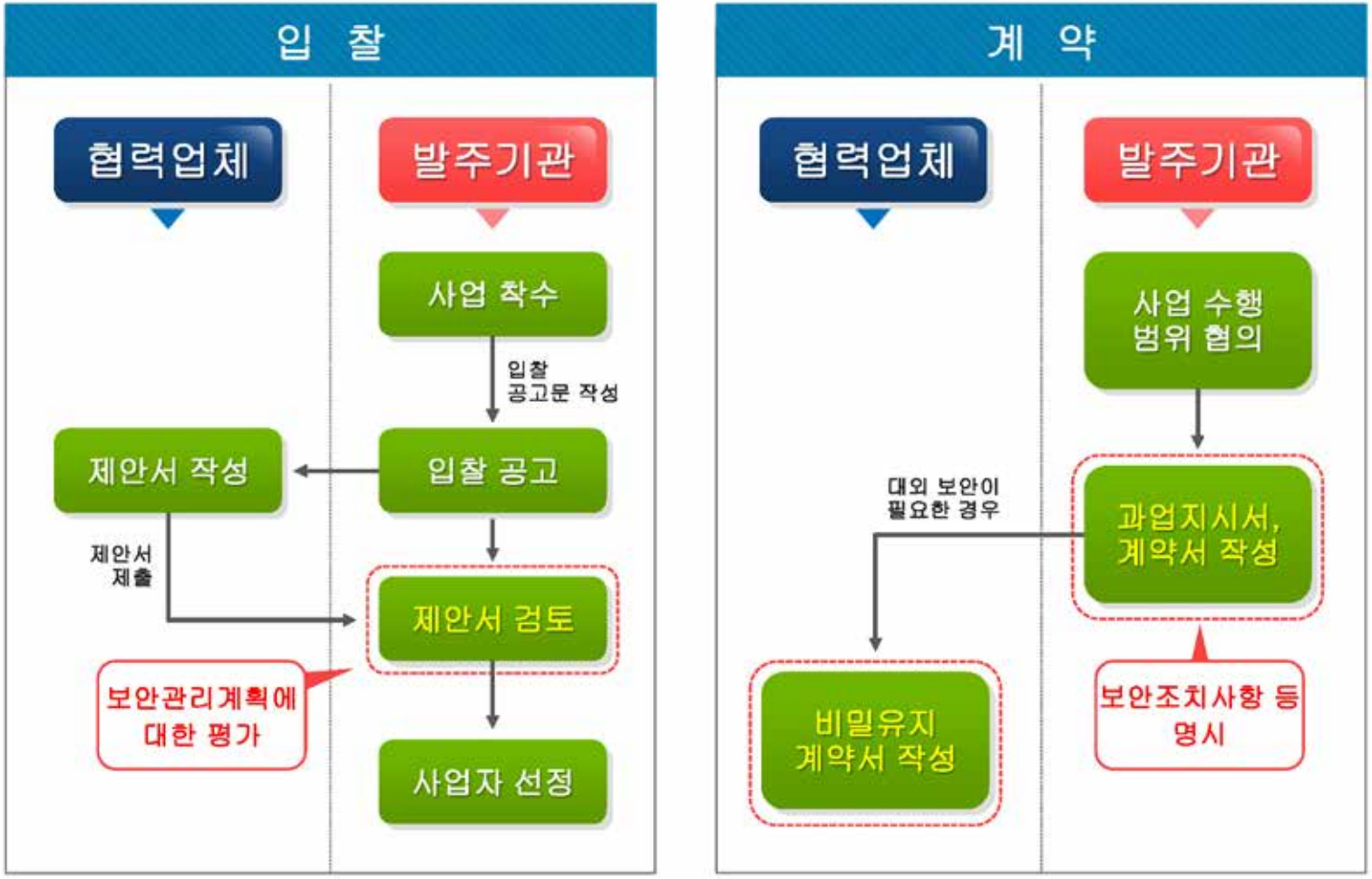
ISO 27036-3 supplier relationships – Part 3 Guidelines for ICT Supply Chain Security Annex B Clause 6 mapping to ISO/IEC 27002

ISO/IEC 27036-3 Clause/Subclause	ISO/IEC 27002 Clause/Subclause
6 ICT supply chain security in Lifecycle Processes	See individual processes for specific mapping
6.1 Agreement Processes	5. Security Policies 6. Organization of Information Security 15. Supplier Relationships 18. Compliance
6.1.1 Acquisition Processes	See 6.1 mapping
6.1.2 Supply Process	See 6.1 mapping
6.2 Organization Project-Enabling Processes	See individual processes for specific mapping
6.2.1 Lifecycle Model Management Process	None
6.2.2 Infrastructure Management Process	8. Asset Management 9. Access Control 10. Cryptography 11. Physical and Environmental Security 12. Operations Security 13. Communications Security 16. Information Security Incident Management 17. Information Security aspects of Business Continu Management
6.2.3 Project Portfolio Management Process	None
6.2.4 Human Resource management Process	7. Human Resources Security
6.2.5 Quality Management Process	14.2 Security in development and support processes 14.3 Test data
6.3 Project Processes	See individual processes for specific mapping
6.3.1 Project Planning Processes	None
6.3.2 Project Assessment and Control Process	None
6.3.3 Decision Management Process	None
6.3.4 Risk Management Process	ISO/IEC 27005
6.3.5 Configuration Management Process	12.1.2 Change management 14.2.2 Change control procedures
6.3.6 Information Management Process	8.2 Information classification 9.1 Business requirements of access control 10 Cryptography 12.3 Backup 13.2.1 Information transfer policies and procedures
6.3.7 Measurement Process	ISO/IEC 27004

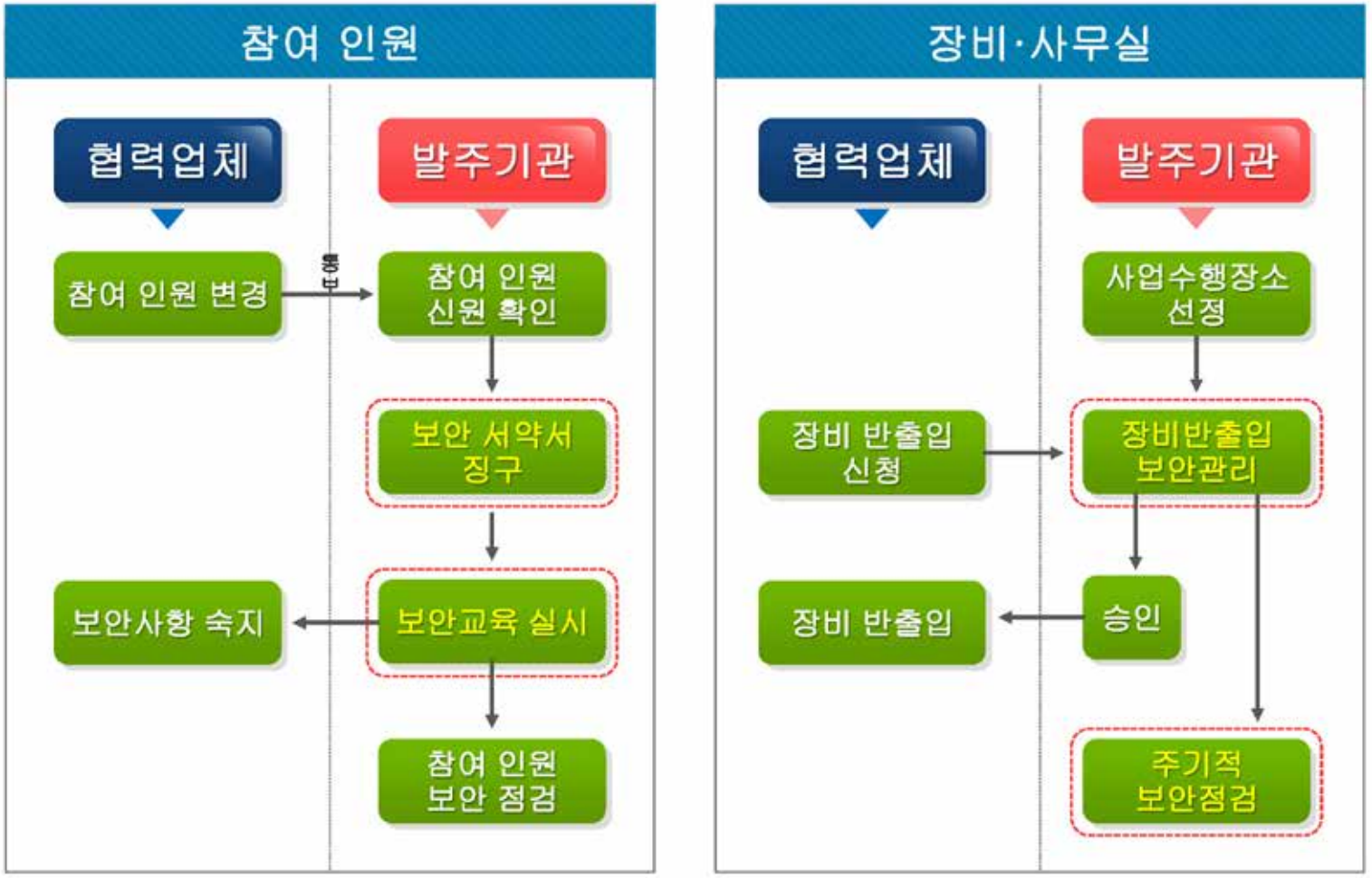
ISO/IEC 27036-3 Clause/Subclause	ISO/IEC 27002 Clause/Subclause
6.4 Technical Processes	See individual processes for specific mapping
6.4.1 Stakeholder Requirements Definition Process	14.1 Security requirements of information systems
6.4.2 Requirements Analysis Processes	14.1 Security requirements of information systems
6.4.3 Architectural Design Processes	None
6.4.4 Implementation Processes	14.2 Security in development and support processes
6.4.5 Integration Process	14.2 Security in development and support processes
6.4.6 Verification Process	14.2 Security in development and support processes 14.3 Test data
6.4.7 Transition Process	14.2.8 System security testing
6.4.8 Validation Process	14.2 Security in development and support processes 14.3 Test data
6.4.9 Operation Process	8. Asset Management 9. Access Control 10. Cryptography 12. Operations Security 13. Communications Security 16. Information Security Incident Management 17. Information Security aspects of Business Continuity Management 18. Compliance
6.4.10 Maintenance Process	8.3. Media Handling 13. Communications Security 17. Information Security aspects of Business Continuity Management
6.4.11 Disposal Process	8. Asset Management 13.2. Information Transfer

韓 根熙

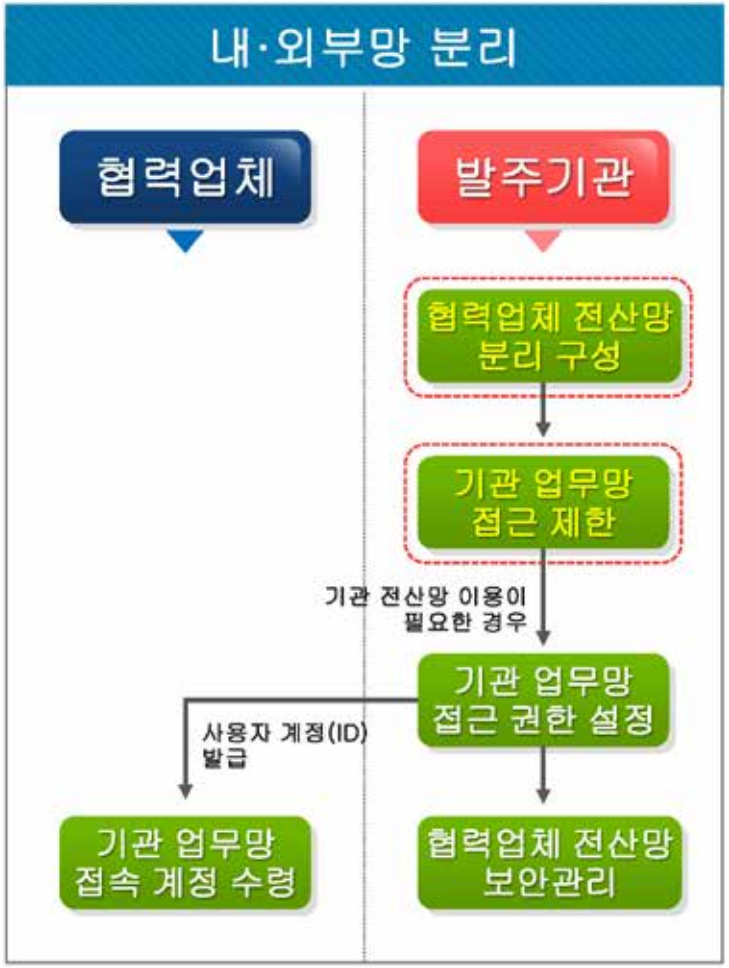
과업 발주 단계 : 입찰 및 계약

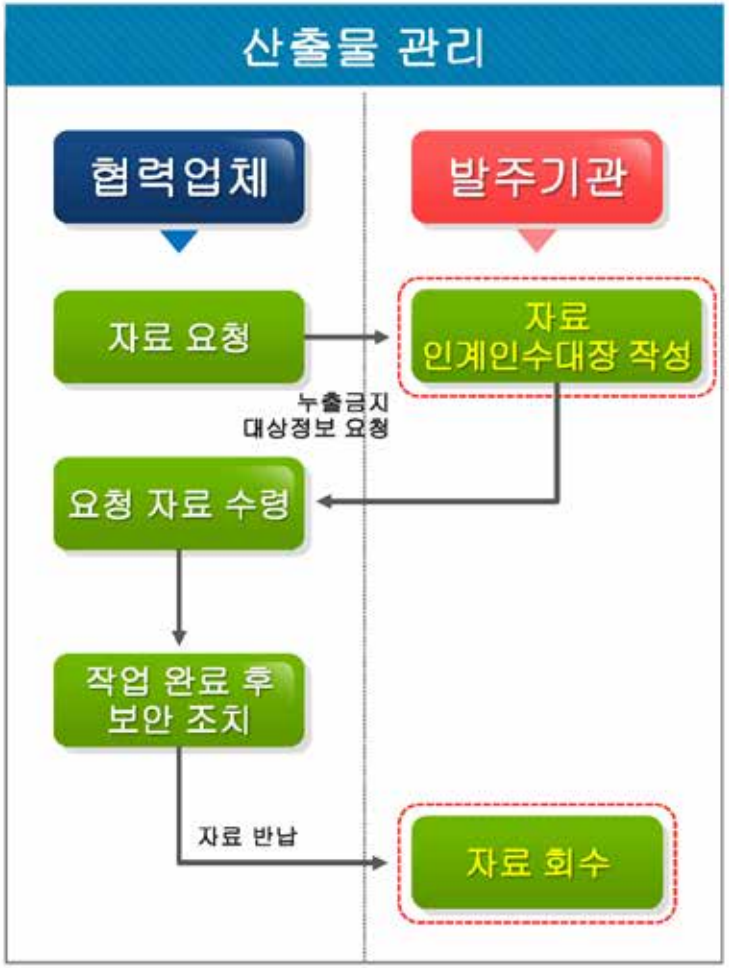


과업 수행 단계 : 인원 및 장비 · 사무실 관리

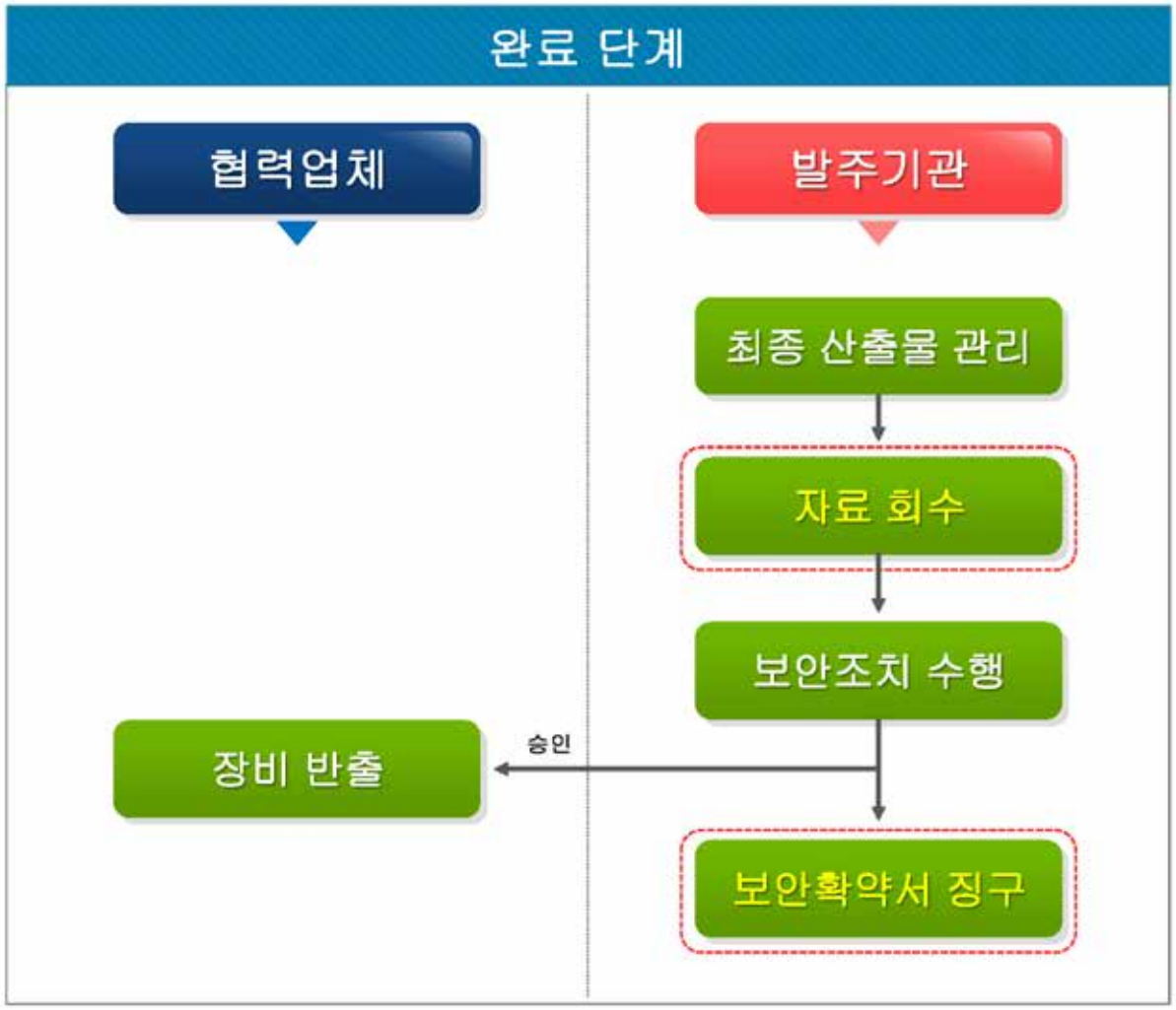


과업 수행 단계 : 망 분리 및 산출물 관리





과업 종료 단계



ICT 공급망 보안 고려사항

- 제품과 서비스에 대한 공급자(Supplier)의 생산, 제공 및 운용에 대한 취득자(Acquirer)의 수용은 취득자가 자신의 조직 내에서 원하는 수준의 정보보안을 보장하는 기준에 기초해야 한다.
  - 정보, 정보시스템 및 서비스의 연속성을 포함하여 취득자의 정보보안에 영향을 미치는 지역 환경과 관련된 정치적, 법적, 정보 보안 위험의 관리.
  - 제공된 제품 및 서비스와 관련된 물리적, 전자 문서 및 기타 정보의 기밀성 관리.
  - 적절한 취급, 즉 고유 표시 및 보호 라벨링을 보장하기 위한 재료 및 요소의 무결성 관리.
  - 소프트웨어 또는 제공된 제품 또는 서비스와 관련된 기타 전자 정보의 무결성 관리, 즉 암호 해시 함수 또는 디지털 워터마크가 손상되지 않도록 보장.
  - 제품 및 서비스가 제공되는 시설의 물리적 보안 관리.
  - 공급업체의 비즈니스 측면과 관련된 정보 보안 관리 및 다른 고객과의 관계.
  - 공급업체의 사업, 공급업체와의 상호 작용 및 다른 취득자와의 상호 작용과 관련된 정보 보안 관리.
- ICT 공급망 전체에 걸친 공급자 관계의 정보보안을 적절하게 관리하기 위해, 취득자는 제품 및 서비스 취득을 위한 표준화된 조직 전체의 프로세스를 갖춘 프레임워크를 채택해야 한다.
  - 정보·정보 시스템의 안전한 교환이나 공유를 위한 정보보안 및 규정준수 요건 확립.
  - 모든 제품, 서비스의 취득 전, 공급망과 관련된 정보보안 위험 평가와 모니터링.
  - ICT 공급망의 다계층 전체(Multi Tier)에 걸쳐 업스트림 공급자에 대한 감사권 및 제한 조건을 포함하여 정보보안 및 준수 요건을 통합한 ICT 공급망 협정 또는 협정의 협상 또는 재교섭 절차 확립.
  - 공급자 관계 변경의 결과로 정보보안 및 규정준수 요건을 준수하는 ICT 공급망 내 공급자 성과의 지속적 모니터링, 보고.
- 취득하는 제품이나 서비스의 성격과 그것이 창출할 것으로 예상되는 위험에 근거하여 맞춤화할 수 있는 다양한 ICT 공급망 합의를 가능하게 하기 위해 유연하게 적용.

ICT Supply Chain Security 필수 사례

- ICT 공급망 위험의 일부는 라이프사이클 프로세스(ISO/IEC 15288 및 ISO/IEC 12207), ISMS 구축 요건(ISO/IEC 27001), 보안 통제(ISO/IEC 27002) 등을 제공하여 해결할 수 있다.
- 1. 관리 연속성: 취득자와 공급자는 요소의 존속 기간 동안 이루어진 각 변경과 전달(Handoff)이 승인되고 투명하며 검증 가능하다는 확신을 가지고 있다.
- 2. 최소 권한 액세스: 직원은 업무에 필요한 권한만 가지고 중요한 정보 및 정보 시스템에 액세스할 수 있다.
- 3. 업무 분리: 한 사람 또는 역할만으로 업무를 완료할 수 없도록 하여 데이터의 생성, 수정 또는 삭제 프로세스 또는 하드웨어 및 소프트웨어의 개발, 운영 또는 제거 프로세스를 제어한다.
- 4. 부정조작 방지 및 증거: 변조 시도가 발생 시 방지되어야 하고, 증빙되어야 하고 되돌릴 수 있어야 한다.
- 5. 지속적인 보호: 데이터 또는 정보가 생성되거나 수정된 위치에서 전송되더라도 효과적인 방법으로 중요한 데이터와 정보를 보호한다.
- 6. 법규 준수 관리: 협정 내 보호의 성공을 지속적이고 독립적으로 확인한다.
- 7. 코드 평가 및 검증 : 코드검사 방법 적용 및 의심스러운 코드 검출
- 8. ICT 공급망 보안교육: 정보보안 실무에 관한 관련자를 효과적으로 교육할 수 있는 조직의 능력. 여기에는 보안 개발 관행, 부정조작 인식 등이 포함되어야 한다.
- 9. 취약성 평가 및 대응: 공급업체가 연구원, 고객 또는 원천(source)에서 발생한 취약성에 대한 정보를 수집하는 능력을 얼마나 잘 갖추고 있는지, 그리고 짧은 시간 내에 의미있는 영향 분석 및 적절한 해결책을 얻을 수 있는지에 대한 공식적인 이해. 여기에는 체계적인 반복적 취약성 대응 프로세스에 대한 취득자 및 공급 업체 합의가 포함되어야 한다.
- 10. 정의된 기대사항: 요소 및 설계/개발 환경에서 충족되어야 할 요건에 관해 명확한 언어로 합의서에 명시. 여기에는 사용된 개발, 통합 및 제공 프로세스에 대한 보안 테스트, 코드 수정 및 보증 제공에 대한 약속이 포함되어야 한다.
- 11. 소유권 및 책임: 지적재산권에 대한 취득자 및 공급자의 소유권 및 지적재산권 보호에 대한 상대방의 책임을 계약에서 식별.
- 12. 회색시장(재판매) 구성요소의 회피: 시스템 구성요소의 신뢰성 확인을 요구함으로써 많은 ICT 공급망 위험을 피할 수 있다.
- 13. 익명 취득: 적절하고 실현 가능한 경우, 익명 취득: 취득자 신분이 민감한 경우, ICT 공급망과 취득자 사이의 연결을 모호하게 한다.
- 14. 일괄 취득: 수명이 긴 시스템(내구성있는 자동제어기)을 위한 요소들이 오래되어(구식이 되어) ICT 공급망 위험을 증가시킬 수 있으나, 지정된 기간 내에 모든 예비 부품을 확보하면 이러한 위험이 감소한다.
- 15. 공급자에 대한 재귀적 요구: 계약을 통해 공급업체는 업스트림 공급업체에게 ICT 공급망 요구 사항을 배치하고 유효성을 확립할 수 있다.

韓 根熙

위협 시나리오 분석 프레임워크 샘플

위협 시나리오	위협 출처	
	취약성	
	위협 이벤트 설명	
	결과	
조직 단위 / 영향을 받는 프로세스		
위험	영향	
	가능성	
	위험 지수 (영향 x 가능성)	
	수용 가능한 위험 레벨	
완화	잠재적 완화 전략 /SCRM통제	
	완화 전략 추정 비용	
	가능성 변화	
	영향 변화	
	선택된 전략	
	추정된 잔여 위험	

韓 根熙

위협 시나리오 분석 프레임워크 샘플

위협 시나리오	위협 출처	공급망 내부로 유입된 위조 통신 요소		
	취약성	OEM에서 더 이상 생산되지 않는 요소 구매 권한자가 정품 요소만을 인식하고 구입하려는 능력/의도가 없다.		
	위협 이벤트 설명	위협 에이전트가 진입할 수 있는 유통망으로 위조 요소를 삽입한다. → 구매 권한자가 위조 요소를 구입한다. → 위조 요소가 시스템 내에 설치된다.		
	결과	요소가 이전보다 빈번하게 실패하고, 정전 횟수가 증가한다.		
조직 단위 / 영향을 받는 프로세스		획득, 유지 OEM/ 공급자 관계 임무(Mission)-필수 기능		
위험	영향	고 - 80%로 정전 증가	중 –40%로 정전 증가	하 – 10%로 정전 증가
	가능성	15 %	40 %	45 %
	위험 지수 (영향 x 가능성)	고		
	수용 가능한 위험 레벨	하		
완화	잠재적 완화 전략 /SCRM통제	수용 테스트 기능 [SCRM_SA-9을 증가; SCRM_SA-10 (7)], 시스템 [SCRM_PL-3 SCRM_SC-13]의 설계에서 보안 요구를 증가시키고 공급 다양성 요건을 이용 [SCRM_PL-3 (1)].	요소 업그레이드를 수용하도록 시스템 변경	
	완화 전략 추정 비용	$180,000	$1 million	
	가능성 변화	낮음	큼	
	영향 변화	중급	없음	
	선택된 전략	기관-계층 검사와 테스트 규정된 수락 테스트 기준을 통과할 때까지 요소를 위탁 보관(escrow)한다. 다수의 요소 공급자를 탐색한다.		
	추정된 잔여 위험	낮음		

韓 根熙

고려대학교
KOREA UNIVERSITY

Question & Answer

韓 根熙
고려대학교 정보보호대학원
0505-747-3300
khhan1@korea.ac.kr

고려대학교
KOREA UNIVERSITY