[OpenChain-KWG/meeting]

LG전자 제품 보안 관리 체계 기반 오픈소스 보안 보증 표준 준수 사례 소개

Cyber Security Governance Office
CTO Software Engineering Lab.

정재욱 책임

Agenda

1. LG전자 Cybersecurity 관리 체계 소개

2. ISO/IEC 18974 표준 준수 수행 과정
   - Motivation
   - 주요 요구사항 항목 분석

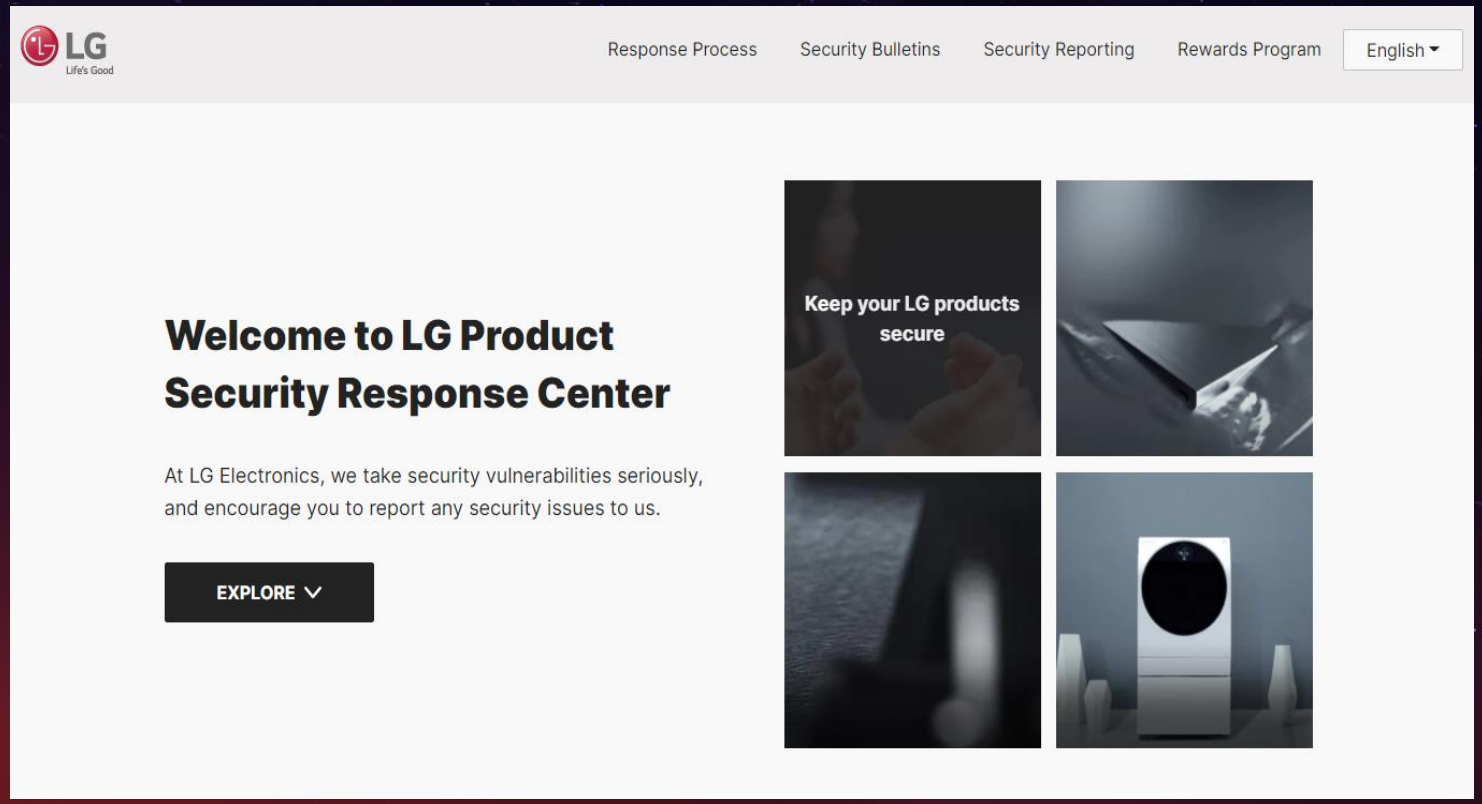
3. Summary & Discussion

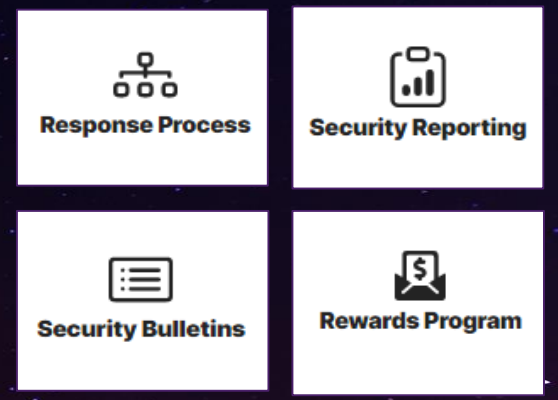
1. LG전자 Cybersecurity 관리 체계 소개

- **LG-SDL (Secure Development Lifecycle) 정책 개발 및 운영**
  - 제품 수명 주기 동안 보안 취약점 진단/제거 활동 수행 및 내·외부 보안인증 통한 보안성 검증 수행

1. LG전자 Cybersecurity 관리 체계 소개

- LGE Product Security Response Team (LG PSRT)
  - 자사 제품 보안 이슈 대응 프로세스에 따라 취약점 분석/대응
  - 제품 취약점 공개 정책을 고지하고, 이해관계자들과 적극적이고 투명한 소통을 수행





https://lgsecurity.lge.com

1. LG전자 Cybersecurity 관리 체계 소개

- CVE Numbering Authority (CNA)
  - 2021년 CNA로 등록 - CVE 번호 등록 권한을 이용하여 CVE ID를 발급

CVE-2022-23729 Detail

Current Description

When the device is in factory state, it can be access the shell without adb authentication process. The LG ID is LVE-SMP-210010.

+View Analysis Description

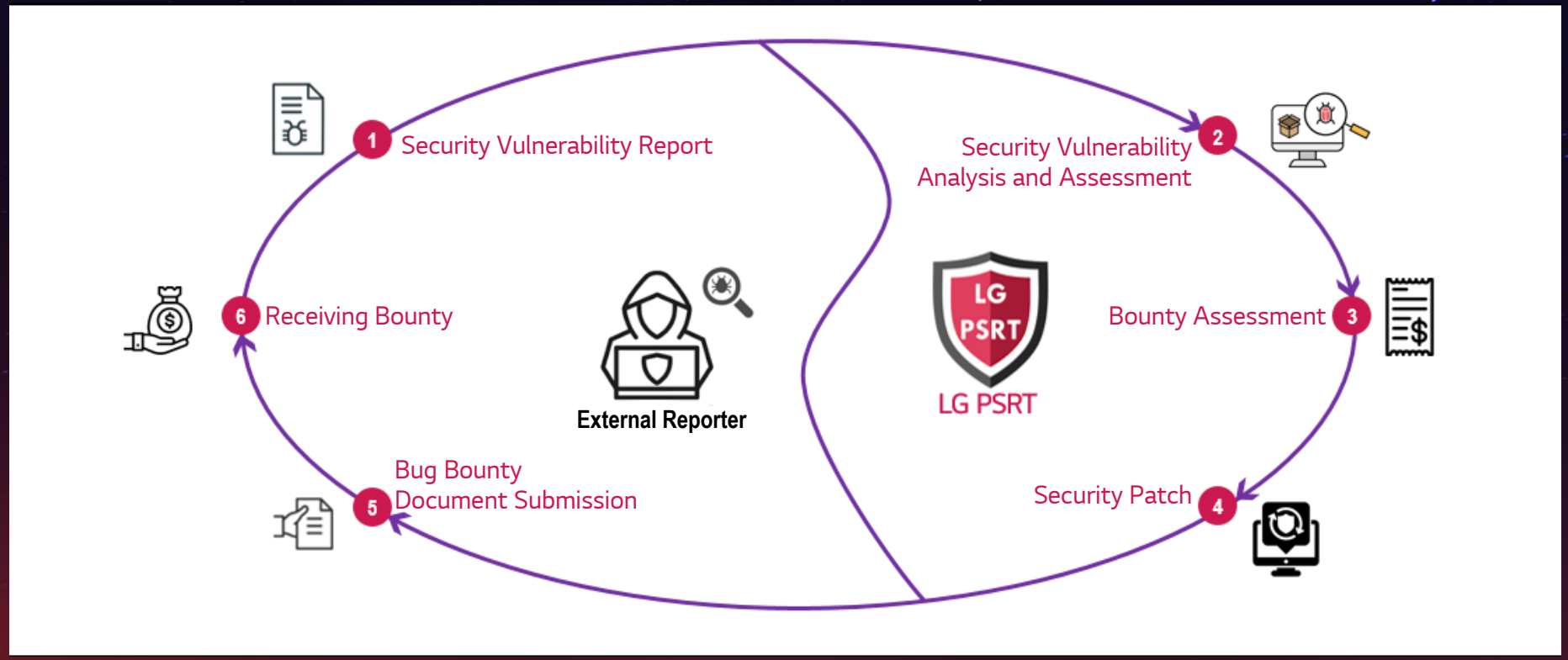
Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD | Base Score: 7.8 HIGH | Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

1. LG전자 Cybersecurity 관리 체계 소개

- **Bug Bounty Program 운영**
  - 자사에 신고 된 LG전자 제품의 보안 취약점에 대해, 신고자에게 포상금을 지급



2. ISO/IEC 18974 표준 준수 수행 과정

Motivation

보안 인증(Security Certification) 획득 !!

ISO/IEC 18974??

오픈소스 보안 관리의 중요성

세계최초? 업계최초?

기사

- Acceptance 일자 : 04/07

April 28, 2023

LG Recognized as Industry's First for Compliance With Open Source Software Security Management

Receiving Certification for ISO/IEC DIS 18974 Compliance, Company Aims to Strengthen Competitiveness of Its Software-Based Businesses

LG OPENCHAIN

SEOUL, April 28, 2023 — LG Electronics (LG) recently earned industry-first recognition for its software supply chain security management system, receiving ISO/IEC DIS 18974 certification – the international standard for open source software (OSS) security management systems established by the Linux Foundation's OpenChain Project. Comprised of a global network of companies, the OpenChain Project is a voluntary consultative body focused on building trust in the OSS supply chain.

2. ISO/IEC 18974 표준 준수 수행 과정

- 처음 내용을 접했을 때... ?!
- 현재 Online Self-Certification Checklist 기능을 제공하는것으로 파악됨
- Comment 별 대응되는 증빙자료 별도 준비

OPENCHAIN

ISO/IEC DIS 18974 Self-Certification Checklist

Section 3.1.1

- ☐ We have a documented policy governing the open source security assurance of Supplied Software.
- ☐ We have a documented procedure to communicate the existence of the open source policy to all Software Staff.

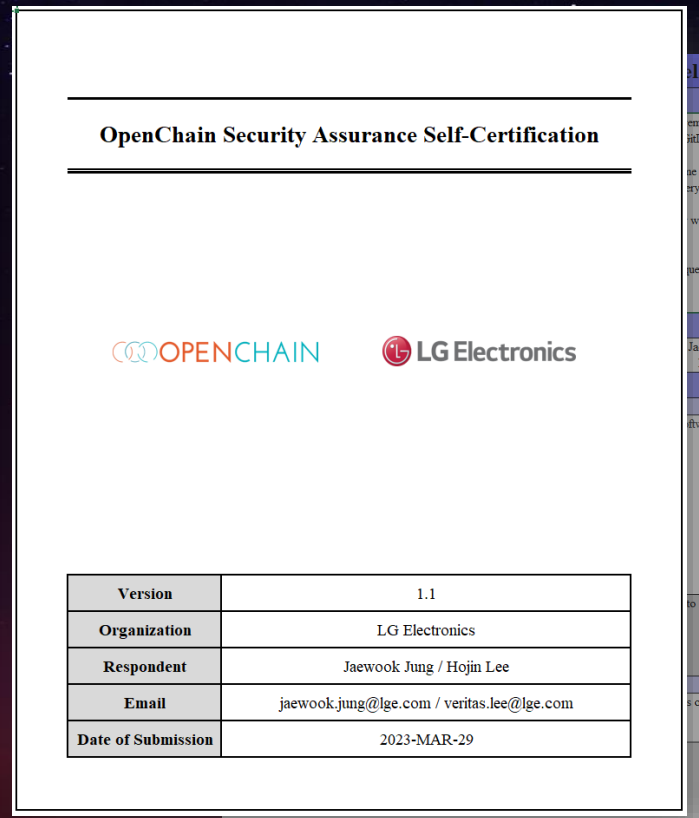
Section 3.1.2

- ☐ We have identified the roles and responsibilities that affect the performance and effectiveness of the Program.
- ☐ We have identified and documented the competencies required for each role.
- ☐ We have identified and documented a list of Program Participants and how they fill their respective roles.
- ☐ We have documented the assessed competence for each Program Participant.
- ☐ We have a way to document periodic reviews and changes made to our processes.
- ☐ We have a way to verify that our processes align with current company best practices and staff assignments.

Section 3.1.3

- ☐ We have documented the awareness of our Program Participants on the following topics:

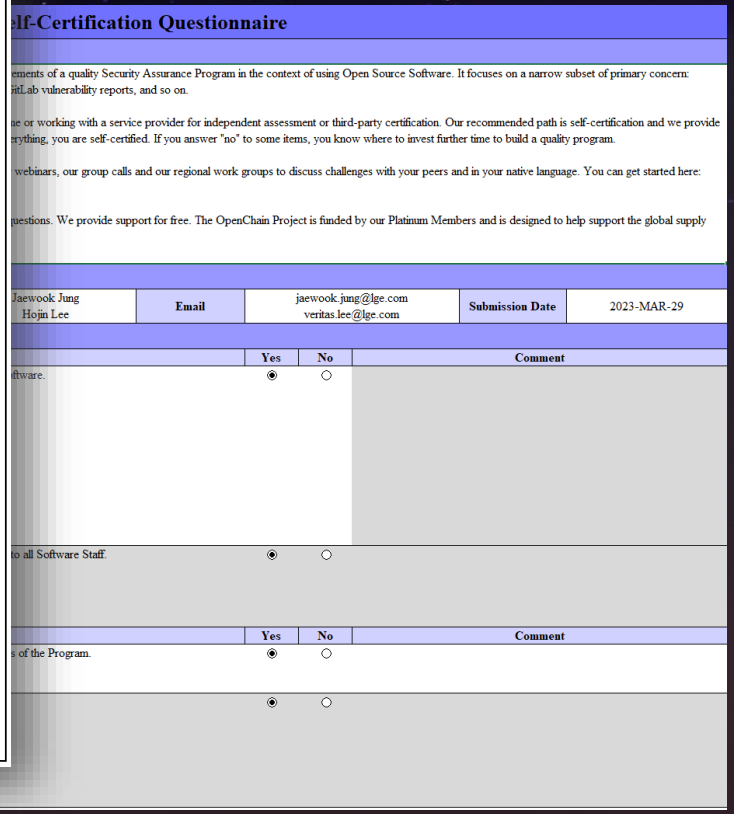
1. The open source security assurance policy and where to find it;
2. Relevant open source objectives;



OpenChain Security Assurance Self-Certification

OPENCHAIN LG Electronics

Version	1.1
Organization	LG Electronics
Respondent	Jaewook Jung / Hojin Lee
Email	jaewook.jung@lge.com / veritas.lee@lge.com
Date of Submission	2023-MAR-29



lf-Certification Questionnaire

ements of a quality Security Assurance Program in the context of using Open Source Software. It focuses on a narrow subset of primary concern: itLab vulnerability reports, and so on.

e or working with a service provider for independent assessment or third-party certification. Our recommended path is self-certification and we provide rything, you are self-certified. If you answer "no" to some items, you know where to invest further time to build a quality program.

webinars, our group calls and our regional work groups to discuss challenges with your peers and in your native language. You can get started here:

uestions. We provide support for free. The OpenChain Project is funded by our Platinum Members and is designed to help support the global supply

Jaewook Jung Hojin Lee	Email	jaewook.jung@lge.com veritas.lee@lge.com	Submission Date	2023-MAR-29

	Yes	No	Comment
ftware.	◉	○	
o all Software Staff.	◉	○	

	Yes	No	Comment
s of the Program.	◉	○	
	◉	○	

2. ISO/IEC 18974 표준 준수 수행 과정

- **Timeline**

January … **March 29** **April 07** **April 21**

ISO/IEC 18974 요구사항 항목 분석 시작


OPENCHAIN

ISO/IEC DIS 18974 Self-Certification Checklist

Section 3.1.1

- ☐ We have a documented policy governing the open source security assurance of Supplied Software.
- ☐ We have a documented procedure to communicate the existence of the open source policy to all Software Staff.

Section 3.1.2

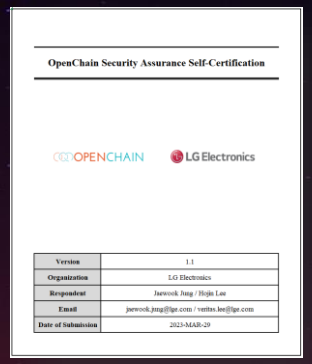
- ☐ We have identified the roles and responsibilities that affect the performance and effectiveness of the Program.
- ☐ We have identified and documented the competencies required for each role.
- ☐ We have identified and documented a list of Program Participants and how they fill their respective roles.
- ☐ We have documented the assessed competence for each Program Participant.
- ☐ We have a way to document periodic reviews and changes made to our processes.
- ☐ We have a way to verify that our processes align with current company best practices and staff assignments.

Section 3.1.3

- ☐ We have documented the awareness of our Program Participants on the following topics:

1. The open source security assurance policy and where to find it;
2. Relevant open source objectives;

Openchain에 답변서 제출


OpenChain Security Assurance Self-Certification

OPENCHAIN LG Electronics

Version	1.1
Organization	LG Electronics
Respondent	Jaewook Jung / Hojin Lee
Email	jaewook.jung@lge.com / ventus.lee@lge.com
Date of Submission	2023-MAR-29

Accept Letter 수령

OpenChain 홈페이지 및 언론사를 통해 공식 Announce


LG전자, 오픈소스 소프트웨어 보안체계 국제표준 준수

LG전자 OPENCHAIN

2. ISO/IEC 18974 표준 준수 수행 과정

- **오픈 소스 보안 보증 컴플라이언스를 위한 핵심 요구 사항을 정의** → 총 35개의 요구사항으로 구성
- **요구사항 항목 분석**
  1) 최대한 오픈 소스 보안 관점으로 해석
  2) 자사 보안 개발 라이프사이클(LG-SDL) 측면으로 해석 (오픈 소스 보안 활동 ⊂ LG-SDL)

No.	Requirement
Section 3.1.2	▪ We have identified the roles and responsibilities that affect the performance and effectiveness of the Program (프로그램 성과와 효율성에 영향을 미치는 R&R을 식별했습니다)
	▪ We have identified and documented the competencies required for each role (각 역할에 필요한 역량을 식별하고 문서화했습니다)
	▪ We have identified and documented a list of Program Participants and how they fill their respective roles (프로그램 참가자 목록과 각자의 역할을 수행하는 방법을 식별하고 문서화했습니다)
	▪ We have documented the assessed competence for each Program Participant (각 프로그램 참가자에 대해 평가된 역량을 문서화했습니다)
	▪ We have a way to document periodic reviews and changes made to our processes (정기적인 검토 및 프로세스 변경 사항을 문서화하는 방법을 갖고 있습니다)
	▪ We have a way to verify that our processes align with current company best practices and staff assignments (우리는 프로세스가 현재 회사의 모범 사례 및 직원 역할과 일치하는지를 검증하는 방법을 갖고 있습니다)

- Section 3.1.2 만 따로 분리해서 보면?
  → 오픈 소스 보안 관점으로만 접근하여 해석하는 것은 쉽지 않음!

- 주요 용어들에 대한 범위 설정 !
  - 프로그램 ⇒ LG-SDL
  - 프로세스 ⇒ 보안 개발 프로세스
  - 역량 ⇒ Security Training (in LG-SDL)
  - ...

2. ISO/IEC 18974 표준 준수 수행 과정

- **요구사항 항목 분석**
  - ✓ Supplied Software의 해석 → 제공 된 SW? / 배포 SW? / 공급 대상 SW? / 3rd Party SW ?

No.	Requirement	대응
Section 3.1.5	▪ We have a method to identify structural and technical threats to the Supplied Software (우리는 공급 대상 소프트웨어에 대한 구조적 및 기술적 위협을 식별할 수 있는 방법을 갖고 있습니다)	LG SDL
	▪ We have a method for detecting existence of Known Vulnerabilities in Supplied Software (우리는 공급 대상 소프트웨어 내 알려진 취약점을 탐지하는 방법을 갖고 있습니다)	FOSSLight
	▪ We have a method for following up on identified Known Vulnerabilities (우리는 식별된 알려진 취약점들에 대한 후속 조치 방법을 갖고 있습니다)	FOSSLight
	▪ We have a method to communicate identified Known Vulnerabilities to customer base when warranted (우리는 식별된 취약점들을 고객에게 전달/소통할 수 있는 방법을 갖고 있습니다)	LG SDL
	▪ We have a method for analyzing Supplied Software for newly published Known Vulnerabilities post release of the Supplied Software (공급 대상 소프트웨어 출시 후 새로 게시된 알려진 취약점에 대해 공급 대상 소프트웨어를 분석하는 방법을 갖고 있습니다)	FOSSLight
	▪ We have a method for continuous and repeated Security Testing is applied for all Supplied Software before release (출시 전 모든 공급 대상 소프트웨어에 대해 지속적이고 반복적인 보안 테스트를 적용하는 방법을 갖고 있습니다)	LG SDL
	▪ We have a method to verify that identified risks will have been addressed before release of Supplied Software (공급 대상 소프트웨어 출시 전 식별된 위험이 해결되었는지 확인하는 방법을 갖고 있습니다)	LG SDL
	▪ We have a method to export information about identified risks to third parties as appropriate (식별된 위험 관련 정보를 제3자에게 적절하게 내보내는 방법을 갖고 있습니다)	LG SDL

2. ISO/IEC 18974 표준 준수 수행 과정

- **요구사항 항목 분석**
  - ✓ 중복 해석이 가능한 문항이 다수 존재함

No.	Requirement
Section 3.2.1	▪ We have a method to allow third parties to make Known Vulnerability or Newly Discovered Vulnerability enquires (e.g., via an email address or web portal that is monitored by Program Participants) (제3자가 알려진 취약점 또는 새로 발견된 취약점에 대해 문의하도록 하는 방법을 갖고 있습니다 (e.g. 이메일 or 프로그램 참가자가 모니터링하는 웹 포털 등을 통해))
	▪ We have an internal documented procedure for responding to third party Known Vulnerability or Newly Discovered Vulnerability inquiries (타사의 알려진 취약점 또는 새로 발견된 취약점 문의에 응답하기 위한 문서화된 내부 절차가 있습니다)

- 취약점 관련 문의/대응/소통
  - ✓ Section 3.1.5
  - ✓ Section 3.2.1

No.	Requirement
Section 3.1.2	▪ We have identified and documented the competencies required for each role (각 역할에 필요한 역량을 식별하고 문서화했습니다)
	▪ We have documented the assessed competence for each Program Participant (각 프로그램 참가자에 대해 평가된 역량을 문서화했습니다)
Section 3.2.2	▪ We have ensured expertise available is to address identified Known Vulnerabilities (식별된 알려진 취약점을 해결하는데 사용할 수 있는 전문 지식을 확보했습니다)

- Security Training Program
  - ✓ Section 3.1.2
  - ✓ Section 3.2.2

2. ISO/IEC 18974 표준 준수 수행 과정

- **요구사항 항목 분석**
  - ✓ 중복 해석이 가능한 문항이 다수 존재함

No.	Requirement
Section 3.1.2	▪ We have a way to verify that our processes align with current company best practices and staff assignments (우리는 프로세스가 현재 회사의 모범 사례 및 직원 역할과 일치하는지를 검증하는 방법을 갖고 있습니다)
Section 3.1.4	▪ We have a set of metrics to measure Program performance (프로그램 성과를 측정하기 위한 메트릭 세트가 있습니다)
	▪ We have Documented Evidence from each review, update, or audit to demonstrate continuous improvement. (지속적인 개선을 입증하기 위해, 리뷰/업데이트/감사 결과 등으로부터 도출 된 문서화된 증거를 가지고 있습니다)

- 검증, 성과 측정, 입증
  ⇒ 감사(Audit)
  - ✓ Section 3.1.2
  - ✓ Section 3.2.4

2. ISO/IEC 18974 표준 준수 수행 과정

- **요구사항 항목 분석**
  - ✓ 다소 난해 했던 문항 ⇒ 다양한 해석이 가능함

No.	Requirement
Section 3.1.4	▪ We have a written statement clearly defining the scope and limits of the Program (우리는 프로그램의 범위와 한계를 명확하게 정의하는 진술서를 갖고 있습니다)

No.	Requirement
Section 3.2.2	▪ We have ensured the identified Program roles have been properly staffed and adequate funding has been provided (식별된 프로그램 역할에 적절한 직원이 배치되고 적절한 자금이 제공되었는지 확인했습니다)
	▪ We have a documented procedure that assigns internal responsibilities for Security Assurance (보안 보증에 대한 내부 책임을 할당하는 문서화된 절차가 있습니다.)

3. Summary & Discussion

- ISO/IEC 18974 항목 분석 및 답변
  - ✓ 범위 설정 및 다양한 접근 방식을 통한 해석
  - ✓ 모범답안?
- 다른 보안 인증과 비교해보면?
- 문의사항 : jaewook.jung@lge.com

Thank you !