OpenChain
Security Assurance Specification

SK텔레콤 장학성

2023-03-28

OPENCHAIN
KOREA WORK GROUP

OPENCHAIN

Building Trust in the Supply Chain Since 2016

Our vision is a supply chain where open source is delivered with trusted and consistent compliance information. **Our mission** is to make that happen.

This Is Where You Will Find:

- The ISO/IEC standard for open source license compliance programs
- The industry standard for open source security assurance programs
- The community that powers these standards

OPENCHAIN KOREA WORK GROUP

We maintain **OpenChain ISO/IEC 5230:2020**, the International Standard for open source license compliance. This is a simple, effective standard suitable for **companies of all sizes in all markets**. It is **developed openly** by a **vibrant user community** and **freely available** to all. It is supported by free online **self-certification**, extensive **reference material** and official **service provider partners**.

Did You Know...

> 20% of German companies with over 2,000 employees have already implemented ISO/IEC 5230.
>
> Source: Bitkom Open Source Monitor 2021

ISO/IEC 5230 Conformant Programs Announced Via Our Website

O kakaobank KEITARO KIA KKCOMPANY L. D. College of Engineering Ahmedabad, Gujarat, India LG Life's Good Liferay LYRA Infosystems

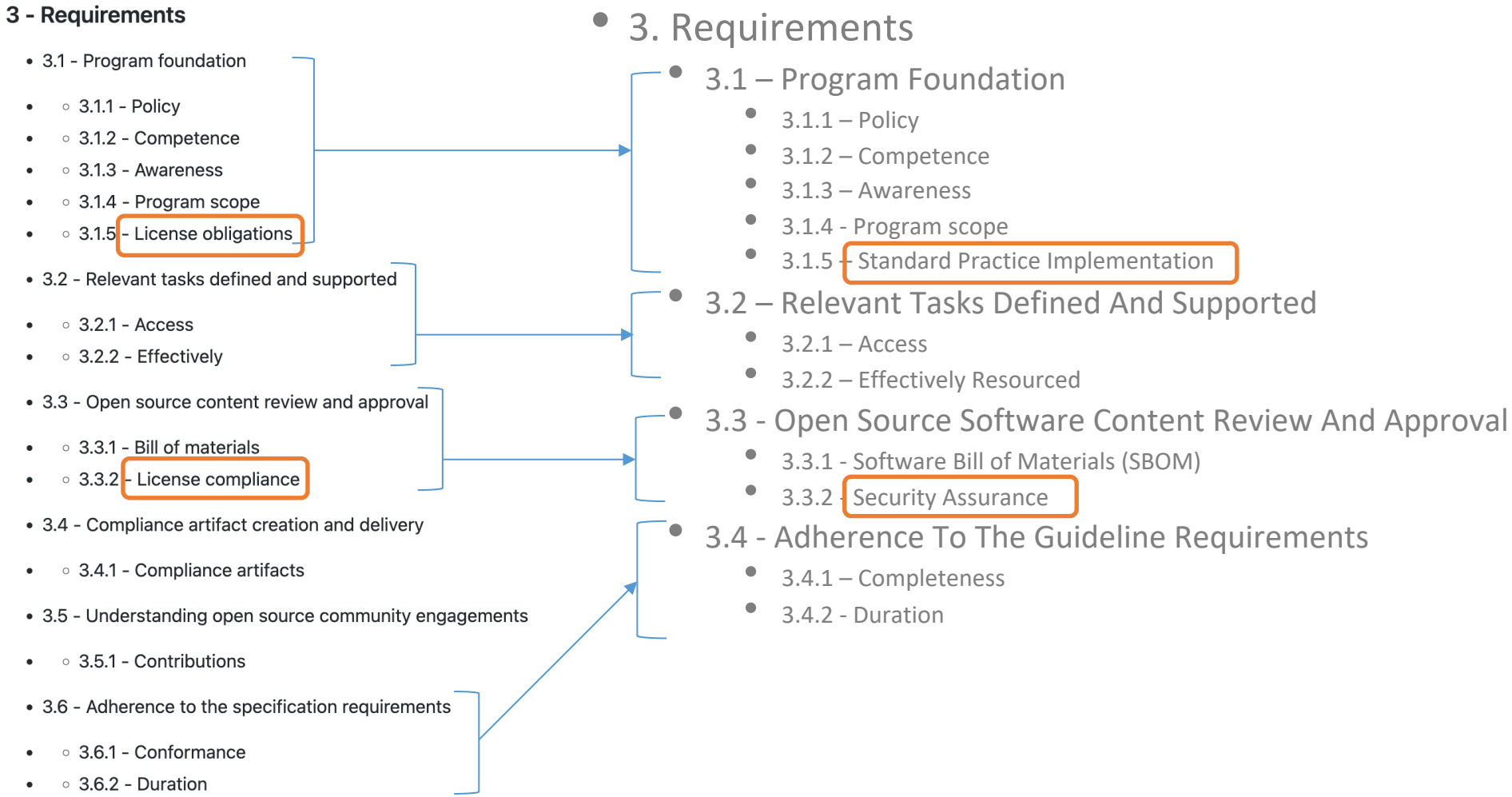
OpenChain Korea Work Group

We also maintain **DIS 18974, OpenChain Security Assurance Specification**. This industry standard describes the key requirements of a quality open source security assurance program. It is currently in the JTC-1 PAS Transposition Process and is expected to graduate mid-2023 as an ISO/IEC standard. The ISO/IEC standard will be **ISO/IEC 18974:2023, OpenChain Security Assurance Specification**.

You can adopt **DIS 18974** via self-certification or through one of the official Third-Party Certification Partners. Adoption of DIS 18974 is also valid for ISO/IEC 18974:2023.

The first company to announce a program using the OpenChain Security Assurance Specification via our website was Interneuron in the UK. The first company to announce whole entity adoption of the OpenChain Security Assurance Specification via our website was BlackBerry. If you adopt the OpenChain Security Assurance Specification and want to announce it via our website, let us know via email.

ISO/IEC 5230 vs. DIS 18974



OpenChain Korea Work Group

3.1.5 – Standard Practice Implementation

The Program demonstrates a sound and robust handling procedures of Known Vulnerabilities and Secure Software Development by defining and implementing following procedures:

- Method to identify structural and technical threats to the Supplied Software is defined;
- Method for detecting existence of Known Vulnerabilities in Supplied Software;
- Method for following up on identified Known Vulnerabilities;
- Method to communicate identified Known Vulnerabilities to customer base when warranted;
- Method for analyzing Supplied Software for newly published Known Vulnerabilities post release of the Supplied Software;
- Method for continuous and repeated Security Testing is applied for all Supplied Software before release;
- Method to verify that identified risks will have been addressed before release of Supplied Software;
- Method to export information about identified risks to third parties as appropriate.

A process shall exist for the Security Assurance methods listed above.

3.1.5 – 표준 사례 구현

프로그램은 다음 절차를 정의하고 구현하여 알려진 취약점 및 보안 소프트웨어 개발을 건전하고 강력하게 처리하는 절차를 갖춘다.:

- 배포용 소프트웨어에 대한 구조적 및 기술적 위협을 식별하는 방법
- 배포용 소프트웨어에서 알려진 취약점 존재 여부를 탐지하는 방법
- 확인된 알려진 취약점에 대한 후속 조치 방법
- 확인된 알려진 취약점을 보증 대상인 고객에게 알리는 방법
- 배포용 소프트웨어의 릴리스 후 새롭게 알려진 취약점이 공개되었을 때 이미 배포된 소프트웨어에 존재하는지 확인하는 방법
- 지속적이고 반복적인 보안 테스트가 출시 전에 모든 배포용 소프트웨어에 적용되기 위한 방법
- 식별된 위험이 배포용 소프트웨어의 출시 전에 해결되었는지 확인하는 방법
- 식별된 위험에 대한 정보를 제3자에게 적절하게 내보내는 방법

위에 나열된 보안 보증 방법에 대한 프로세스가 존재해야 한다.

3.3.2 - Security Assurance

- For each Open Source Software component in the bill of materials for the Supplied Software release under review;
- Apply method for detecting existence of Known Vulnerabilities;
- For each identified Known Vulnerability assign a risk/impact score;
- For each detection and assigned score determine and document necessary remediation steps suitable for the use-case of the software and get Customer Agreement at or above a previously determined level (i.e., all severity scores above 4.5 …);
- Depending on the risk/impact score take the appropriate action (e.g., contact customers if necessary, upgrade software component, no further action, …);
- If a Newly Discovered Vulnerability is present in previously distributed Supplied Software, depending on the risk/impact score take the appropriate action (e.g., contact customers if warranted);
- An ability to monitor Supplied Software after their release to market and to respond to Known Vulnerability or Newly Discovered Vulnerability disclosures.

Verification Material(s):

- 3.3.2.1: A documented procedure for handling detection and resolution of Known Vulnerabilities for the Open Source Software components of the Supplied Software;
- 3.3.2.2: For each Open Source Software component a record is maintained of the identified Known Vulnerabilities and action(s) taken (including even if no action was required).

OpenChain Korea Work Group

3.3.2 – 보안 보증

- 검토 중인 배포용 소프트웨어 릴리스에 대한 BOM의 각 오픈소스 소프트웨어 컴포넌트에 대해 다음 사항을 확인한다.
- 알려진 취약점의 존재를 발견하기 위한 방법을 적용한다.
- 각각의 발견된 취약점과 할당된 점수에 대해 소프트웨어의 사용 사례에 적합하게 필요한 수정 단계를 결정 및 문서화하고 이전에 결정된 수준 이상(즉, 심각도 점수 4.5 이상인 모든 경우 등)에서는 고객 동의를 얻는다.
- 위험/영향 점수에 따라 적절한 조치를 취한다(예: 필요한 경우 고객에게 연락, 소프트웨어 컴포넌트 업그레이드, 추가 조치 없음 등).
- 새로 발견된 취약점이 이전에 배포된 배포용 소프트웨어에 있는 경우 위험/영향 점수에 따라 적절한 조치를 취한다(예: 보증이 필요한 고객에게 연락).
- 배포용 소프트웨어가 시장에 출시된 후 모니터링하고 알려진 취약점 또는 새로 발견된 취약점 노출에 대응하는 기능을 확보한다.

입증 자료:

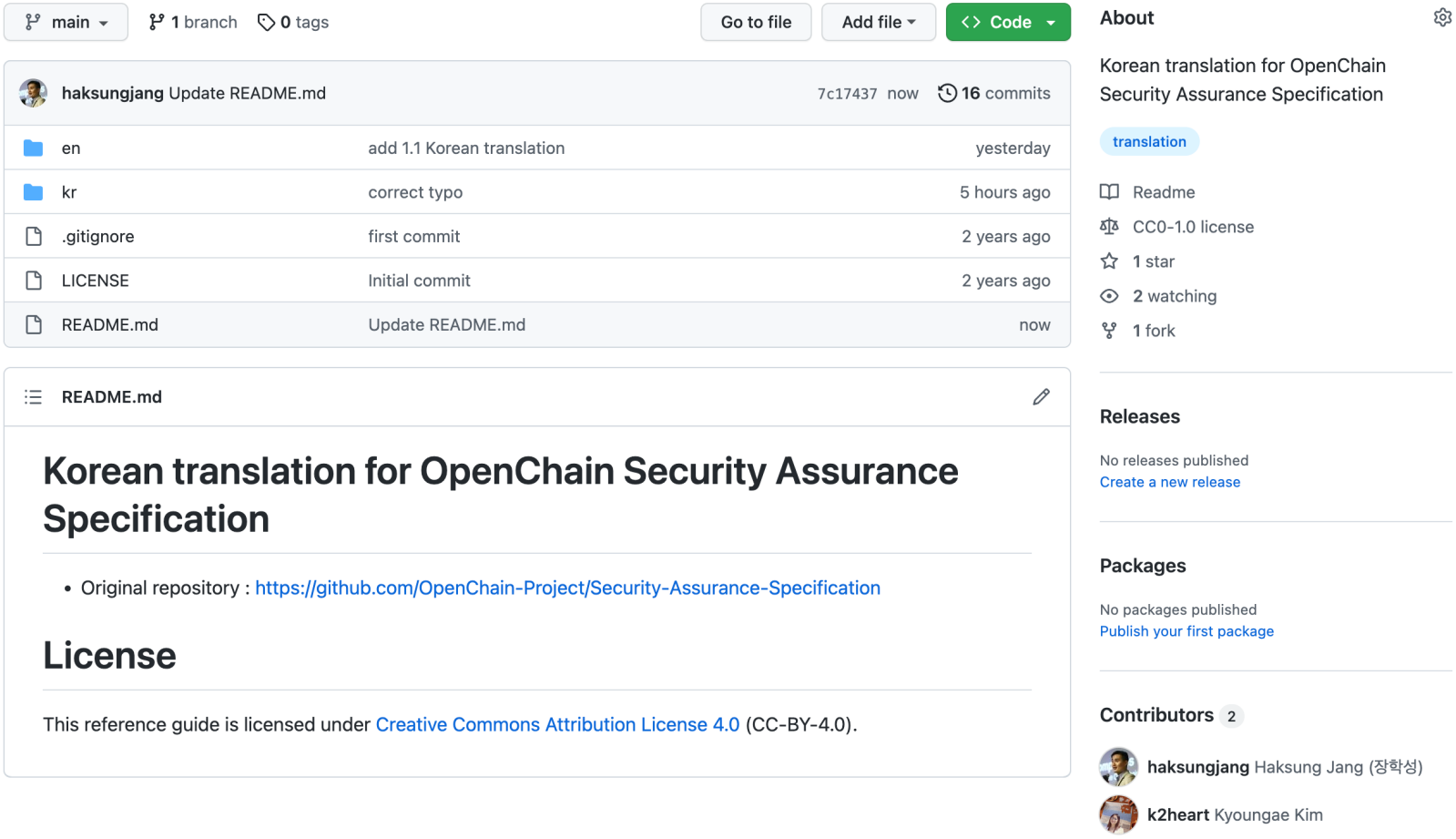
- 3.3.2.1: 배포용 소프트웨어의 오픈소스 소프트웨어 컴포넌트에 대한 알려진 취약점의 탐지 및 해결을 위한 문서화된 절차
- 3.3.2.2: 각 오픈소스 소프트웨어 컴포넌트에 대해 식별된 알려진 취약점 및 수행된 조치에 대한 기록을 유지한다(조치가 필요하지 않은 경우도 포함).

결국, 보안취약점 검출하고, 이를 해결할 수 있어야 하고,
새로운 보안취약점이 보고됐을 때 이미 출시된 모델에 영향이 있는지 확인할 수 있어야 한다.
→ 철저한 SBOM 관리와 보안취약점 발견 시 대응 프로세스 필요

OPENCHAIN KOREA WORK GROUP

한국어 번역

- https://github.com/OpenChain-KWG/Security-Assurance-Specification_Kor



Contributions are welcome!

OpenChain Korea Work Group

감사합니다.

Thank you.

OPENCHAIN KOREA WORK GROUP