

카카오뱅크 오픈소스 보안 보증 표준 ISO/IEC 18974 준수 사례 소개



카카오뱅크
이민애
하헌관



Agenda

- Intro
- ISO/IEC 5230
- ISO/IEC 18974
- Plans



Intro

◎ Change Management

- Shane says when you are involved with open source management (method, processes, policy) you are not an open source person, you are **an employee involved in change management"**



Intro

DEPLOY

PROCESS

**OPEN
SOURCE
MGT.**

JIRA

Confluence

SONARQUBE



ISO/IEC 5230

OSRB

OSRB(Open Source Review Board)는 당행의 오픈소스 컴플라이언스 위해 오픈소스 프로그램 메니저와 법무팀, 특허팀, 개발팀, 인프라팀 등 관련 조직의 책임자로 구성된 협의체이다.

- 오픈소스 컴플라이언스를 위한 정책과 프로세스를 만들고, 이를 수행하기 위한 역할과 책임을 정의한다.
- 당행 오픈소스 컴플라이언스 이슈 발생 시, 해결 방안을 논의하고, 대응책을 마련한다.
- 필요 시, 임원진에 이슈를 보고하여 리스크 완화 방안에 대한 피드백을 받는다.

No	역할	책임	업무	필요 역량	담당 조직
1	오픈소스 프로그램 메니저	오픈소스 프로그램에 대한 총괄 책임을 담당한다. 오픈소스를 사용한 제품과 서비스의 오픈소스 컴플라이언스를 보장해야 한다.	<ul style="list-style-type: none"> • 오픈소스 컴플라이언스를 위해 필요한 역할을 정의하고, 각 역할을 책임질 담당 조직 및 담당자를 지정한다. 필요 시 OSRB와 협의한다. • 오픈소스 컴플라이언스 교육을 주관하고 평가한다. • OSRB의 의장을 맡아서 활동을 지휘한다. • 외부로부터의 오픈소스 사용 및 컴플라이언스 관련 문의 및 요청에 대응한다. • 오픈소스 사용 요청을 검토하고 승인한다. • 오픈소스 BOM 기록을 유지한다. • 구성원에게 오픈소스 관련 법률 자문 받는 방법을 제공한다.(3.2.2.3) • 오픈소스 고지 및 소스 코드 공개를 위한 저장소를 유지한다. 	<ol style="list-style-type: none"> 1. 소프트웨어 개발 프로세스 이해 2. 저작권, 특허 등 오픈소스 라이선스와 관련한 지식재산 이해 3. 오픈소스 컴플라이언스에 대한 전문 지식 4. 오픈소스 개발 경험 5. 커뮤니케이션 스킬 	IT법규관리팀
2	법무 담당	오픈소스 라이선스와 의무를 해석한다. 이러한 의무를 실제 이행하는 등 오픈소스 활동을 위해 발생시킬 수 있는 법적 위험의 완화를 위한 자문을 제공한다.	<ul style="list-style-type: none"> • 포괄되지 않는 오픈소스 라이선스로 인한 충돌을 포함하여 라이선스 및 지식재산권 문제에 대해 자문을 제공한다. • 외부 오픈소스 프로젝트로의 기여 시 오픈소스 라이선스, CLA(Contributor License Agreement) 등 필요한 법적 사항을 검토한다. 	<ol style="list-style-type: none"> 1. 오픈소스 생태계에 대한 기본 지식 2. 소프트웨어 저작권에 대한 전문 지식 3. 오픈소스 라이선스에 대한 전문 지식 	법무팀
3	인프라 담당	오픈소스 분석 도구를 운영하고 자동화하여 모든 배포용 소프트웨어에 대해 라이선스 분석이 원활히 수행되도록 시스템을 구축한다.	<ul style="list-style-type: none"> • 오픈소스 라이선스 분석 도구를 운영한다. • DevOps 환경과 통합하여 라이선스 분석을 자동화한다. • 모든 배포용 소프트웨어에 대상 라이선스 분석이 수행되도록 시스템과 프로세스를 구축한다. • 모든 배포용 소프트웨어에 대한 오픈소스 BOM을 확보하고 유지한다. 	<ol style="list-style-type: none"> 1. 오픈소스 컴플라이언스 프로세스에 기본 지식 2. 오픈소스 라이선스 분석 도구에 대한 이해 3. IT 인프라에 대한 전문 지식 	IT법규관리팀
4	보안 담당	오픈소스 보안취약점 분석 도구를 운영하여 모든 배포용 소프트웨어에 대해 보안취약점 분석이 원활히 수행되도록 시스템을 구축한다.	<ul style="list-style-type: none"> • 오픈소스 보안취약점 결과에 대해 분석하고 대응한다. • 모든 배포용 소프트웨어에 대상으로 오픈소스 보안취약점 분석이 수행되도록 시스템과 프로세스를 구축한다. 	<ol style="list-style-type: none"> 1. 오픈소스 컴플라이언스 프로세스에 기본 지식 2. 오픈소스 라이선스 분석 도구에 대한 이해 3. 보안에 대한 전문 지식 	보안팀
5	개발문화담당	사내의 개발자들이 오픈소스를 적극적으로 '사용'하고 '기여'할 수 있는 문화를 조성하며, 사내의 커뮤니티에 참여해서 선진 개발문화를 사내에 습득 및 전파할 수 있도록 지원하고, 오픈소스 공개는 기술연구소를 통해서 꾸준히 하고 활발하게 진행될 수 있도록 지원한다.	<ul style="list-style-type: none"> • 기술연구소를 통한 오픈소스 공개의 활동이 지속가능할 수 있도록 촉구하고 지원한다. • 금융서비스의 보안적 특성에 따른 오픈소스 공개의 제약들이 기술연구소를 통해 극복할 수 있도록 지원해서, 금융산업에서도 오픈소스 생태계 활성화에 기여할 수 있는 사례를 만들고 문화를 조성한다. • 개발자들의 오픈소스 사용과 기여의 활동이 사내의 성과로 인정될 수 있는 문화를 조성한다. • 다양한 형태로 오픈소스 커뮤니티에 참여할 수 있도록 장려한다. 	<ol style="list-style-type: none"> 1. 소프트웨어 개발 프로세스 이해 2. 오픈소스 컴플라이언스에 대한 기본 지식 3. 오픈소스 정책에 대한 이해 	기술전략팀
6	개발팀	소프트웨어 개발/배포 조직은 올바른 오픈소스 활동을 위해 오픈소스 정책 및 프로세스를 준수한다.	<ul style="list-style-type: none"> • 오픈소스 라이선스 준수 • 오픈소스 기여 	<ol style="list-style-type: none"> 1. 소프트웨어 개발 프로세스 이해 2. 오픈소스 컴플라이언스에 대한 기본 지식 3. 오픈소스 정책에 대한 이해 4. 오픈소스 라이선스에 대한 기본 지식 	개발팀



ISO/IEC 5230



Guide

오픈소스 소프트웨어(OSS)

페이지
편집
나중에 사용하도록 저장
지켜보기
공유

페이지

블로그

공간 바로가기

팀이나 프로젝트에서 가장 중요하다 싶은 내용에 대한 바로가기를 이곳에 추가할 수 있습니다. 사이트 바 구성.

페이지 프리

- > 오픈소스 정책
- > 오픈소스 사용 가이드
- > 오픈소스 기여 가이드
- > 오픈소스 공개 가이드
- > 회의록
- > 스티디
- > 발표자료
- > 업무정리(관리자)

공간 도구

Open Source Guide

작성자: may/lee, 최근 변경: arlo/ha - 1월 11, 2022

오픈소스 소프트웨어
Open Source Guide 공간은 오픈소스 정책과 사용, 기여, 공개 관점에서 가이드하고 있는 페이지입니다.

What is Open Source?



오픈소스 소프트웨어(Open Source Software, OSS)란 소스코드가 공개되어 누구나 자유롭게 사용할 수 있는 오픈소스 라이선스를 만족하는 소프트웨어입니다. 최근 몇 년간 수많은 기업에서 오픈소스를 활용하고 있으며, 오픈소스는 아래와 같이 다양한 이점이 있습니다.

- 총 개발 비용 절감
- 최신 기술 확보
- 내부 기술 역량 강화
- 기술 경쟁력 강화
- 시장의 확대
- 우수한 개발 인재 확보



ISO/IEC 5230

Guide

FOSSID 사용자 가이드

arlo.ha@이 작성, 9월 13, 2021에 최종 변경

오픈소스 사용 비중이 높아지면서 오픈소스 관리의 중요성도 높아지고 있습니다. (참조: 오픈소스 라이선스 가이드)

오픈소스 사용에 따른 법적 리스크를 방지하기 위해 라이선스 분석 및 검증을 자동으로 진행할 수 있는 도구(FOSSID)를 도입하였습니다.

FOSSID를 통해 개발자는 언제든지 라이선스를 식별하고 검토할 수 있으며, 필요 시 CI와 연동하여 오픈소스 라이선스를 조기에 분석할 수 있습니다.

개발자는 본인이 원하는 상황에 따라 아래 3가지 환경에서 FOSSID를 사용할 수 있습니다.

자세한 내용은 해당 하위 페이지 참조바랍니다.

1) Snippet Search & Quick View (코드 & 파일 간편 검색)

- 개발자는 개발 중 오픈소스 매치 정보 확인이 필요한 경우 오픈소스 코드(Snippet)를 Copy-Paste 하여 Snippet에 대한 오픈소스 매치 정보 제공받을 수 있습니다.
- Snippet Search가 하나의 파일에 대해 Copy-Paste를 지원하는 기능이라면, Quick View에서는 폴더나 여러 파일을 업로드 한 뒤, 한 번에 분석을 수행할 수 있습니다.
- 해당 분석은 특별한 권한 요청이 요구되지 않으며, 개발자들이 언제든지 FOSSID 사이트에 로그인해서 분석할 수 있습니다.

2) 외부 배포 (앱, 웹)

- 외부에 배포되는 시스템(iOS, Android 등)의 경우 보다 각별히 오픈소스 분석을 수행해야 합니다.
- 해당 시스템의 오픈소스 담당자는 IT 변경관리팀과 함께 오픈소스 분석을 수행하며, 라이선스 의심건에 대해 식별 작업을 수행합니다.
- 배포 고지문 업데이트가 필요한 경우 해당 작업을 진행합니다.

3) 내부 배포 (빌드 파이프라인)

- 내부 배포 시스템에 해당하는 시스템의 경우 빌드, 정적분석이 수행된 후 자동으로 오픈소스 분석이 수행됩니다.
- 오픈소스 분석 후 라이선스에 대한 확인이 필요한 경우, ITSVJIRA에 자동으로 티켓이 생성됩니다.
- 개발자는 식별 완료 후 해당 티켓의 Status를 변경하면 자동으로 오픈소스가 재분석되며, 해당 티켓은 정상종료됩니다.

추가 문의사항은 @arlo.ha 에게 문의바랍니다.

1) Snippet Search & Quick View (코드 & 파일 간편 검색)

arlo.ha@이 작성, 9월 13, 2021에 최종 변경

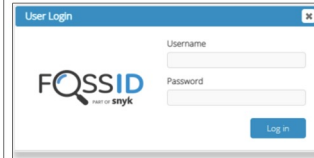
Snippet Search

개발자는 개발 중 오픈소스 매치 정보 확인이 필요한 경우 오픈소스 코드 Snippet을 Copy-Paste 하여 Snippet에 대한 오픈소스 매치 정보 제공받을 수 있습니다.

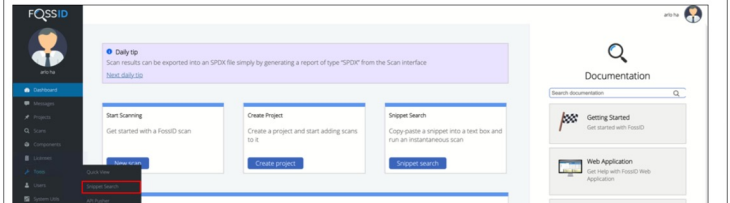
개발자는 개발 중 빠르게 오픈소스 매치 정보 확인이 가능하여 개발 마지막 단계에서 발견될 수 있는 라이선스 컴플라이언스 문제를 개발 단계에서 조기에 예방할 수 있습니다.

Snippet Search 사용방법

1) FOSSID 서버에 로그인(LDAP 연동)합니다.



2) 좌측 메뉴의 'Tools - Snippet Search' 탭으로 접속합니다.





ISO/IEC 5230

OSS Notice



← 오픈소스 라이선스

This application use Open Source Software (OSS). You can find the source code of these open source projects, along with applicable license information, below. We are deeply grateful to these developers for their work and contributions.

Any questions about our use of licensed work can be sent to oss@kakaobank.com

Apache Commons Lang
<https://github.com/apache/commons-lang>
 · Copyright © 2001-2016 The Apache Software Foundation
 · Apache License 2.0

Android Constraint Layout Library
<https://developer.android.com/reference/android/support/constraint/packages>
 · Copyright © 2017 The Android Open Source Project
 · Apache License 2.0

Android Databinding Library
<https://developer.android.com/reference/android/databinding/packages>
 · Copyright © 2018 The Android Open Source Project
 · Apache License 2.0

Android Material Components
<https://developer.android.com/reference/com/google/android/material/packages>
 · Copyright © 2018 The Android Open Source Project
 · Apache License 2.0


Android-platform-frameworks-support
<https://android.googlesource.com/platform/frameworks/support>
 · Copyright © 2018 The Android Open Source Project
 · Apache License 2.0



ISO/IEC 5230








Vulnerabilities


 **arlo.ha (하현관)**
2022년 1월 10일(월) 13:29

각 라이선스에 대한 피드백 공유드립니다. (라이선스 위험도: 하)
[Redacted]





leptonica 라이선스의 경우 보안취약점이 검출되었으니 참고 부탁드립니다.
[Redacted]

고지문 작업 진행하겠습니다.

 **may.lee (이민애)**
2022년 1월 26일(수) 14:08 수정됨

보안취약점 관련하여 라이브러리 버전 변경 예정 : 2.13.0 업 일정에 맞춰 배포 예정
[Redacted]
[Redacted]

 1   



ISO/IEC 5230



Vulnerabilities

오픈소스 / FOSS-540

오픈소스 취약점 검토 요청

[Edit](#) [Add comment](#) [Assign](#) [More](#) [종료](#) [Admin](#)

Details

Type: 보안취약점 검토 Status: [검토확인 \(View Workflow\)](#)

Priority: Medium Resolution: Unresolved

Labels: None

Description

취약점 이슈가 발견되었는데 검토 요청드립니다.

CRITICAL
1

HIGH
7

MEDIUM
6

LOW
2

취약점 관련 리뷰드립니다.

CVE	영향도	조치 필요 여부
	Critical	0

fossid 결과로 공유된 CVE의 경우 공개된 poc가 없어 실제 공격가능성은 낮으나, 공격에 성공하였을 경우 remote code execution 등의 파급도가 큰 취약점이므로 조치가 필요합니다.



ISO/IEC 5230

OpenChain ISO/IEC 5230 conformant program

Kakaobank Announces OpenChain Conformant Program

By Shane Coughlan | January 24, 2022 | Featured, News



Today Kakaobank announces an OpenChain ISO/IEC 5230 conformant program. It is the first financial company in Korea and the second worldwide to formally adopt the International Standard for open source compliance.

"The use of open source is a trend and essential for all IT industries," says Shin Jae-Hong, Chief Information Officer(CIO) of Kakaobank. "As Kakaobank is the first Korean financial company to be a part of OpenChain, We will accelerate innovative financial business possibilities through Ai, Big data, and Cloud based on our open source ability"

"The Korean community has been instrumental in building and supporting OpenChain ISO/IEC 5230, the International standard for open source license compliance," says Shane Coughlan, OpenChain General Manager. "We are delighted to celebrate today's conformance announcements by Kakao and KakaoBank, underlining the leadership and energy in the local market. Our shared supply chain is becoming clearer, more trusted and more efficient thanks to these efforts."



ISO/IEC 18974

The screenshot shows the top navigation bar of the ISO website with the ISO logo and links for Standards, About us, News, Taking part, and Store. The main content area features the title 'ISO/IEC 18974' in large bold text, followed by 'Information technology' and 'OpenChain security assurance specification'. A vertical blue bar on the left side of the content area is followed by the text 'Status : Under development'.

ISO Standards About us News Taking part Store

ISO/IEC 18974

Information technology

OpenChain security assurance specification

Status : **Under development**

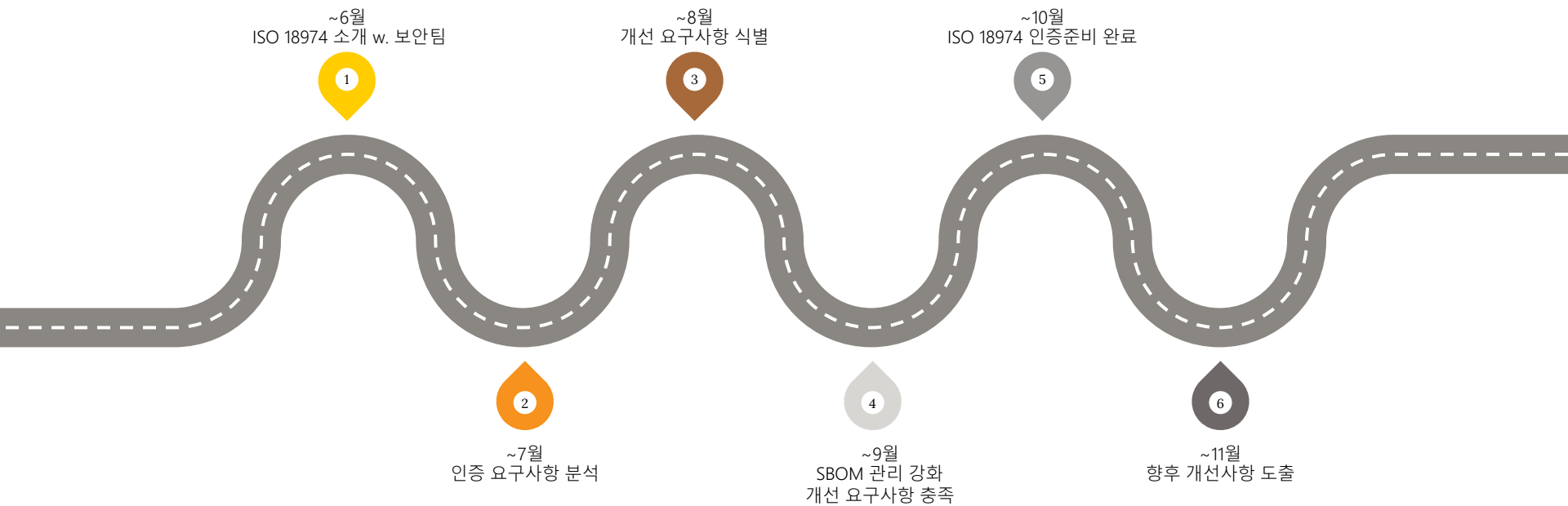


ISO/IEC 18974

STAGE	SUBSTAGE		90 Decision				
	00 Registration	20 Start of main action	60 Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Close of review			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Close of voting	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Close of comment period			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee	30.00 Committee draft (CD) registered	30.20 CD study initiated	30.60 Close of comment period	30.92 CD referred back to Working Group		30.98 Project cancelled	30.99 CD approved for registration as DIS
40 Enquiry	40.00 DIS registered	40.20 DIS ballot initiated: 12 weeks	40.60 Close of voting	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project cancelled	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval	50.00 Final text received or FDIS registered for formal approval	50.20 Proof sent to secretariat or FDIS ballot initiated: 8 weeks	50.60 Close of voting. Proof returned by secretariat	50.92 FDIS or proof referred back to TC or SC		50.98 Project cancelled	50.99 FDIS or proof approved for publication
60 Publication	60.00 International Standard under publication		60.60 International Standard published				



ISO/IEC 18974





ISO/IEC 18974



SBOM

- Olive
- FossID
- App Developers
- Fosslight hub



ISO/IEC 18974

Sections	Requirements	C	
Section 3.1.1	We have a documented policy governing the open source security assurance of Supplied Software. (배포용 소프트웨어의 오픈소스 보안 보증에 관한 문서화된 정책을 보유하고 있습니다.)	K T	
	We have a documented procedure to communicate the existence of the open source policy to all Software Staff. (소프트웨어 직원들에게 오픈소스 정책의 존재를 알리기 위한 문서화된 절차를 보유하고 있습니다.)	K V P	
Section 3.1.2	We have identified the roles and responsibilities that affect the performance and effectiveness of the Program. (본 프로그램의 성과와 효과에 영향을 미치는 역할과 책임을 식별했습니다.)	T r c V	
	We have identified and documented the competencies required for each role. (각 역할을 위해 필요한 역량을 식별하고 문서화했습니다.)	A W	
	We have identified and documented a list of Program Participants and how they fill their respective roles. (프로그램 참여자 명단과 그들의 역할을 수행하는 방법을 식별하고 문서화했습니다.)	V T	
	We have documented the assessed competence for each Program Participant. (각 프로그램 참가자에 대한 평가된 역량을 문서화했습니다.)		
	We have a way to document periodic reviews and changes made to our processes. (프로세스의 정기적인 검토와 변경 사항을 문서화할 수 있는 방법이 있습니다.)		
	We have a way to verify that our processes align with current company best practices and staff ass (프로세스가 현재 회사의 BP 사례 및 직원 배치와 일치하는지 확인할 수 있는 방법이 있습니다.)		
	Section 3.1.3	We have documented the awareness of our Program Participants on the following topics: - The open source security assurance policy and where to find it; - Relevant open source objectives; - Contributions expected to ensure the effectiveness of the Program; - The implications of failing to follow the Program requirements. (다음 주제에 대한 프로그램 참여자의 인식을 문서화했습니다: - 오픈소스 보안 보증 정책과 이를 찾을 수 있는 위치 - 관련 오픈소스 목표 - 프로그램의 효과를 보장하기 위해 기대되는 기여도 - 프로그램 요건을 준수하지 않을 경우의 영향)	변경관리팀 식별
	Section 3.1.4	We have a written statement clearly defining the scope and limits of the Program. (프로그램의 범위와 한계를 명확하게 정의한 기술서가 있습니다.) We have a set of metrics to measure Program performance. (프로그램 성과를 측정하기 위한 일련의 지표가 있습니다.) We have Documented Evidence from each review, update, or audit to demonstrate continuous improvement. (지속적인 개선을 위해 검토, 업데이트 또는 감사에 대한 문서화가 있습니다.)	



ISO/IEC 18974

보안팀 식별

Section 3.1.5	We have a method to identify structural and technical threats to the Supplied Software; (배포용 소프트웨어에 대한 구조적 및 기술적 위협을 식별하는 방법을 가지고 있습니다.)
	We have a method for detecting existence of Known Vulnerabilities in Supplied Software; (배포용 소프트웨어에 알려진 취약점의 존재를 탐지하는 방법을 가지고 있습니다.)
	We have a method for following up on identified Known Vulnerabilities; (식별된 알려진 취약점에 대한 후속 조치를 취할 수 있는 방법을 보유하고 있습니다.)
	We have a method to communicate identified Known Vulnerabilities to customer base when warranted; (식별된 알려진 취약점을 보증된 경우 고객층에 전달하는 방법을 가지고 있습니다.)
	We have a method for analyzing Supplied Software for newly published Known Vulnerabilities post release of the Supplied Software; (배포용 소프트웨어의 릴리스 후 새로 발표된 알려진 취약점에 대해 배포용 소프트웨어를 분석하는 방법을 가지고 있습니다.)
	We have a method for continuous and repeated Security Testing is applied for all Supplied Software before release; (배포용 소프트웨어에 대해 출시 전에 지속적이고 반복적인 보안 테스트를 적용하는 방법을 보유하고 있습니다.)
	We have a method to verify that identified risks will have been addressed before release of Supplied Software; (식별된 위험이 배포되는 소프트웨어의 출시 전에 해결되었는지 확인할 수 있는 방법을 가지고 있습니다.)
	We have a method to export information about identified risks to third parties as appropriate. (식별된 위험에 대한 정보를 적절히 제3자에게 내보낼 수 있는 방법을 가지고 있습니다.)



ISO/IEC 18974

조직

정책

도구

교육

프로세스

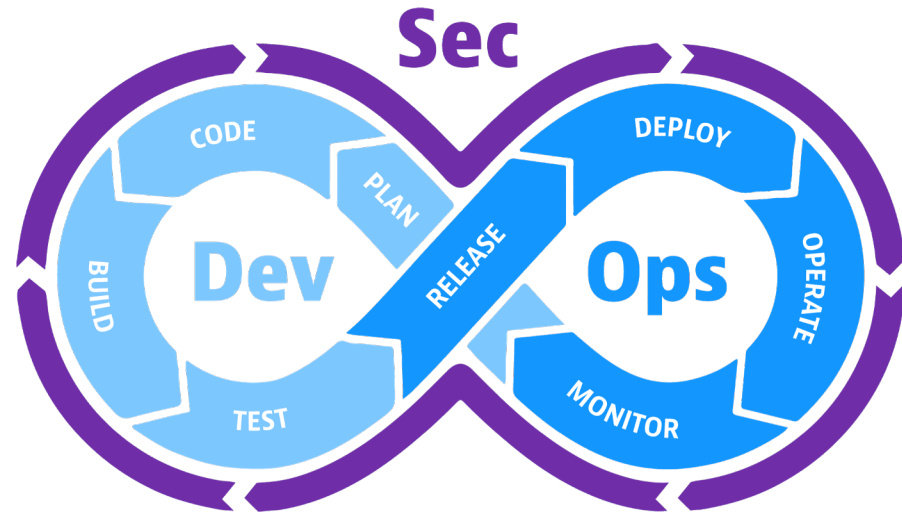
And
more..



Plans

DevSecOps

- Vulnerability
- Dependency
- Checklist
- Cultures
- Automation
- Containers
- ...





References

- ① https://openchain-project.github.io/OpenChain-KWG/guide/opensource_for_enterprise/
- ① <https://nipa-openup.github.io/oss-governance-guide/>



Thanks!

Any **questions** ?

You can find us at

- arlo.ha@kakaobank.com
- may.lee@kakaobank.com