

# 삼성SDS ISO/IEC 18974 준수 사례 소개

2024/06

삼성SDS

채진영, 김기륜

# ISO/IEC 18974 추진 배경

SW 공급망의 보안과 안정성 측면에서 글로벌 수준의 경쟁력을 확보를 위해 오픈소스 보안 국제 표준 기준을 충족 하기로 함

구분	오픈소스 라이선스 (SDS '22.7 인증)	오픈소스 보안 (추진 중)
국제인증	ISO/IEC 5230	ISO/IEC 18974
주요 항목	프로그램 설립, 컴플라이언스 산출물 생성 및 제공, 업무 정의 및 지원 등  38개 체크리스트	프로그램 설립, 전담조직, 보안 정책, 보안 검증 프로세스, 검증 도구, 오픈소스 콘텐츠 검토 및 승인 등  32개 체크리스트

# ISO/IEC 18974 Plan



# 보안 표준 세부항목 분석

리눅스 재단의 OpenChain Project가 규정한 '오픈소스 보안 관리 체계 국제 표준'으로 보안 관리 체계에 대한 32개 보안 요건 충족 필요

ISO/IEC 18974 Certification Checklist

Section 구분	Section	Checklist	구분	
		We have a method to verify that identified risks will have been addressed before release of Supplied Software.	우리는 확인된 위험이 공급 소프트웨어 출시 전에 해결되었는지 확인하는 방법을 가지고 있습니다.	보안검증
		We have a method to export information about identified risks to third parties as appropriate.	우리는 식별된 위험에 대한 정보를 제3자에게 적절하게 안내하는 방법을 가지고 있다.	취약점 관리/대응
취약점 문의	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);	우리는 제 3자가 알려진 취약성 또는 새롭게 발견된 취약성 문의 (예 : 프로그램 참가자가 모니터링하는 이메일 주소 또는 웹 포털을 통해)를 할 수 있도록 허용하는 방법을 가지고 있습니다.	홈페이지-문의
		We have an internal documented procedure for responding to third party Known Vulnerability or Newly Discovered Vulnerability inquiries.	우리는 알려진 취약성 또는 새로 발견된 취약성 문의에 대응하기 위한 내부 문서화된 절차를 가지고 있습니다.	취약점/위험관리
조직 및 역량	Section 3.2.2	We have documented the people, group or functions related to the Program.	우리는 프로그램과 관련된 사람, 그룹 또는 기능을 문서화했습니다.	조직/문서화
		We have ensured the identified Program roles have been properly staffed and adequate funding has been provided.	우리는 확인된 프로그램 역할이 적절하게 채용되고 적절한 자금이 제공되도록 보장했다.	역할/비용
		We have ensured expertise available is to address identified Known Vulnerabilities;	우리는 알려진 취약성을 해결하기 위해 이용 가능한 전문 지식을 보장했습니다.	취약점 관리/역량/컨설팅조직
		We have a documented procedure that assigns internal responsibilities for Security Assurance.	우리는 보안 보증에 대한 내부 책임을 부여하는 문서화된 절차를 가지고 있습니다.	프로세스
		We have a documented procedure	우리는 공급된 소프트웨어에서 사용되는 모든 오	

주요 항목	체크리스트
정책	2
프로세스 및 R&R	10
취약점 분석 / 대응	8
취약점 문의	2
조직 및 역량	4
오픈소스 관리	2
SBOM	2
문서화 증빙	2
	32개

# R&R과 프로세스 정리

대부분 기존에 하고 있는 것들이나, 흩어져있는 R&R/프로세스/시스템을 정리하고 부족하거나 모호한 부분을 보완함



# 오픈소스 보안 정책서 제작

기존 보안 정책 및 프로세스 관리, 점검 영역에 오픈소스에 특화된 SW 식별, 오픈소스 소프트웨어 자재 명세서 SBOM관리, 보안취약점 관리 및 추적 방안을 강화하여 문서화 하고 시스템을 체계화 함

ISO/IEC 18974 Certification Checklist

Section 구분	Section	Checklist
정책	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.
프로세스 및 R&R	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.

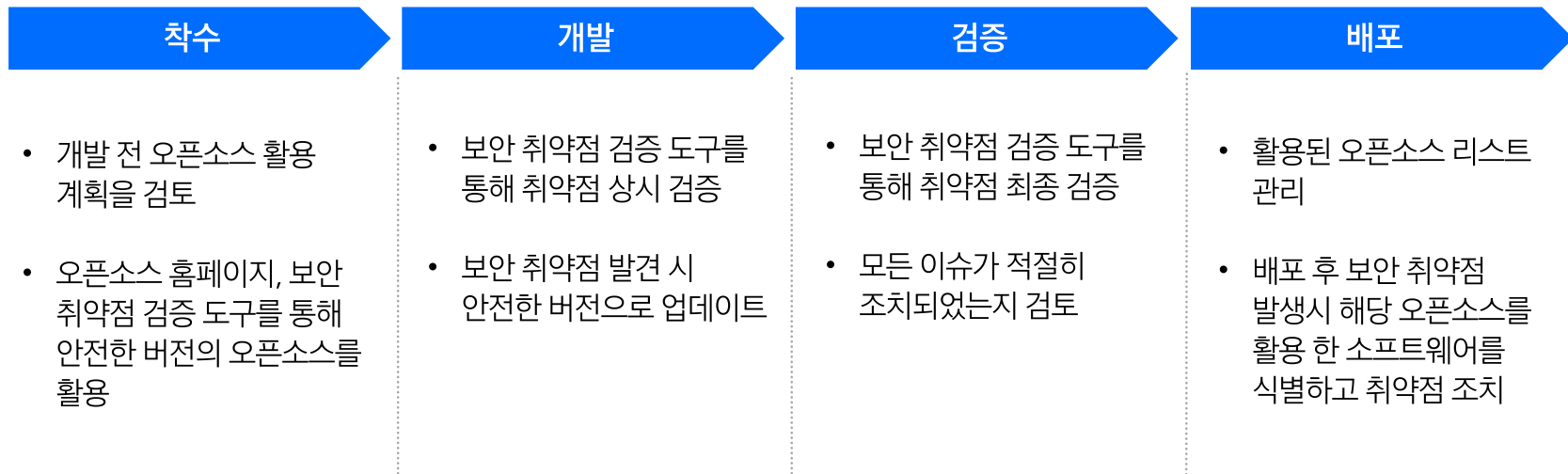
documented 16회 등장!!

오픈소스 보안 정책

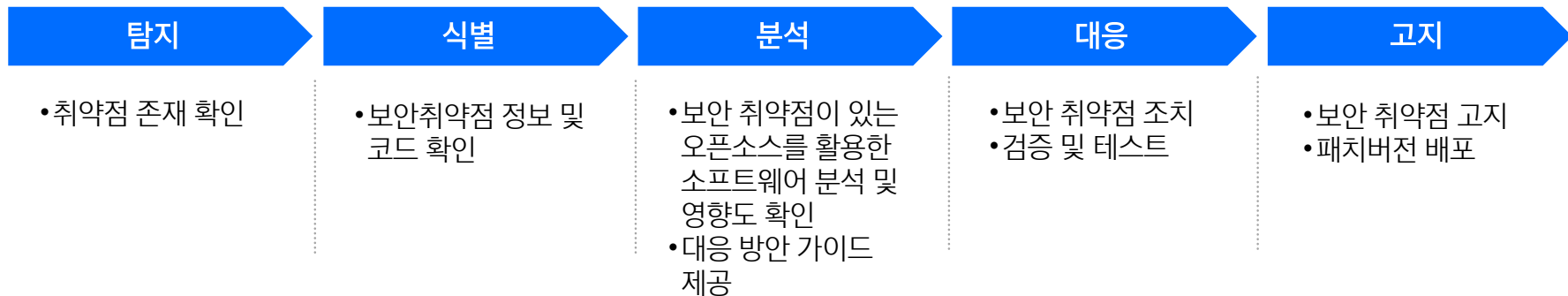
오픈소스 사무국

1. 목적
2. 적용 범위 및 구성
3. 조직 및 역할
4. 오픈소스 개발 보안 정책
5. 신규 보안 취약점 대응 정책
6. SBOM 생성 및 관리 정책
7. 외부 문의 대응 정책
8. 오픈소스 정책 관리 및 준수
9. OpenChain 적합성
10. 용어

# 정책서 주요 내용: 오픈소스 개발 보안 정책



# 정책서 주요 내용: 보안 취약점 대응 체계



## 관리 및 모니터링

### 운영 관리

- 소프트웨어에 활용된 오픈소스 관리
- 안전한 오픈소스 관리

### 취약점 문의

- 제 3자가 문의할 수 있는 이메일 주소 또는 웹 포털 보유

### 교육

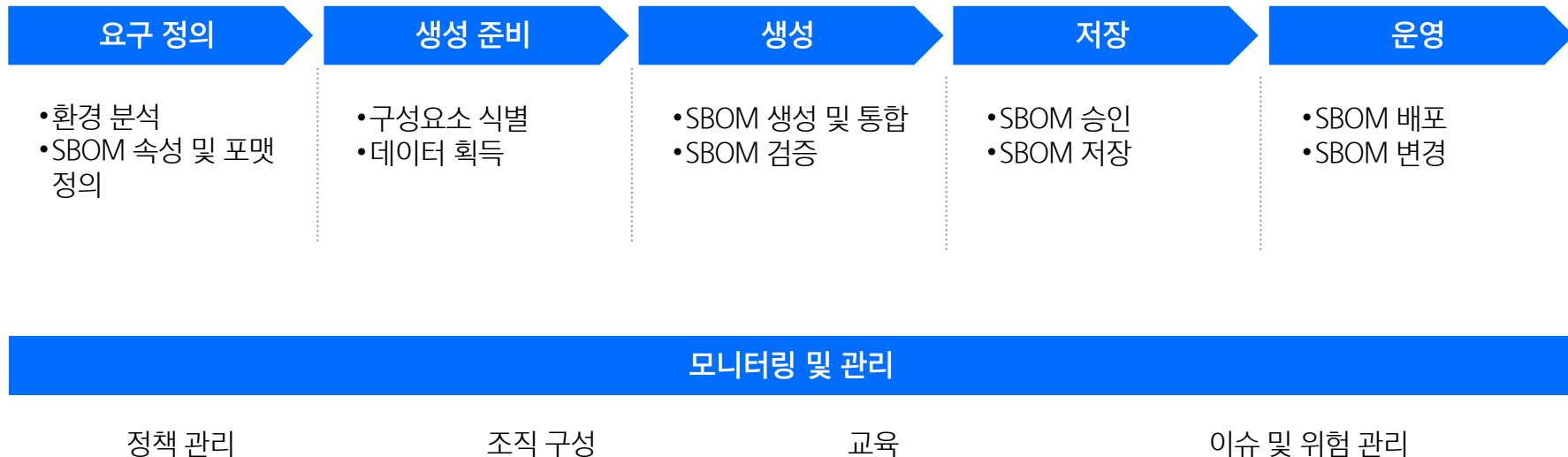
- 보안 교육 및 전문 지식 제공

### 이슈 및 위험 관리

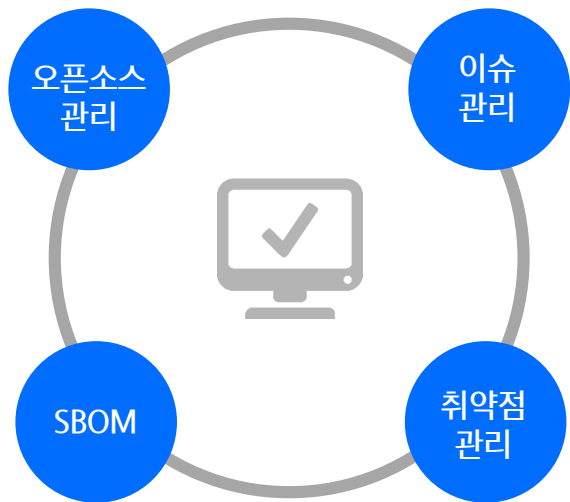
- 모니터링/주기적 점검
- 이슈 추적



# 정책서 주요 내용: SBOM 프로세스



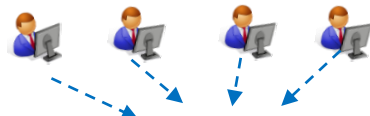
# 오픈소스 보안 관련 시스템 정비



Data 통합 및  
DB 이력화



오픈소스명	버전명	취약점
PostgreSQL	9.6.15	취약
Tomcat	9.0.52	안전
Nginx	1.21.0	안전



활용 현황/취약점/SBOM 조회



이슈 발생 시 추적 관리  
및 정기 모니터링을  
통해 리스크 예방

# 오픈소스 보안 인증 홍보 예정

회사정보

회사소개

특약정보

자녀가능성

제품

NEED LAB

정보보호 | AI 윤리 | 오픈소스 정책 | 개인정보보호

삼성SDS는 오픈소스 컴플라이언스를 준수하고 오픈소스 생태계에 기여하고자 노력하고 있습니다.

삼성SDS는 공유와 협력의 가치에 기반하여 오픈소스 커뮤니티와 개발자들이 함께 성장할 수 있도록 다양한 활동을 추진하고 있습니다. 또한 오픈소스의 적절한 사용을 보장하고 자물적으로 준수하기 위한 오픈소스 정책을 운영하고 있습니다. 이를 통해 오픈소스 라이선스 의무 및 무분별한 사용 또는 배포로 인해 발생할 수 있는 법적 책임과 가치 있는 독점적 권리의 침해를 방지하며, 오픈소스를 활용한 가치창출에 기여하고자 합니다.

삼성SDS의 오픈소스 정책은 다음과 같은 내용을 담고 있습니다.

공유와 협력

교육 및 평가

비밀유지 내용

합동라이선스 준수

오픈소스 사용 및 고지

오픈소스 기여

동반성장 가치창출

SAMSUNG SDS  
오픈소스 정책

보안 내용 추가

외부 문의 대응

삼성SDS 소식

삼성SDS, 오픈소스 국제 표준 인증 획득

2022-07-14 | 삼성SDS

삼성SDS가 국내 IT서비스 기업 최초로 '오픈체인(OpenChain) 프로젝트'가 부여하는 오픈소스 국제 표준 인증(ISO/IEC 5230:2020)을 획득했다.

이 인증은 2016년 리눅스 재단 주도로 시작된 '오픈체인 프로젝트'가 오픈소스 라이선스 준수 체계와 활용 역량을 갖춘 전 세계 기업을 대상으로 심사 후 수여하고 있다.

# 느낀점

- 보안이 간소한 회사라면.. 회사에서 하고있는 보안 검증 정책이 많은 부분을 커버하고 있음
- 프로세스와 룰은 만들면 되지만 시스템적 투자가 필요한 보안 취약점 검증 툴, 활용 이력 추적을 위한 오픈소스 관리 시스템, SBOM 체계 구축은 선행되어야 함

문의: 채진영([jy73.chae@samsung.com](mailto:jy73.chae@samsung.com)), 김기륜([kiryun.kim@samsung.com](mailto:kiryun.kim@samsung.com))

\_\_\_\_**Thank you**\_\_\_\_

Q&A

**SAMSUNG SDS**