제3회

스마트 의료 안전 컨퍼런스 2026

규제를 넘어 혁신으로: AI, 사이버 보안, 그리고 eQMS

Strategy, Implementation and AI Integration

SaMD 사이버보안 관리체계 구축 · 운영 전략

브이웨이 오동석



스마트 의료 안전
컨퍼런스 2026

CONTENTS

01 SaMD 제조업체의 CSMS 구축 · 운영 어프로치 분석

02 타 컨설팅 사의 대응 전략 분석

03 실질적 대응 방안 – 브이웨이가 여러분께 제안드리는 것

01

SaMD 제조업체의 CSMS 구축 · 운영 어프로치 분석



들어가며

0 왜 지금 이 논의인가

2025년 1월 **디지털의료제품법** 시행, 2025년 4월 식약처 **「디지털의료기기 전자적 침해행위 보안지침」** 고시, 이어진 심사 업무지침서와 민원인 가이드라인까지 — SaMD 제조업체에게 사이버보안은 더 이상 품질활동의 하위 항목이 아니라 **허가·변경관리·사후관리와 직접 연결된 규제 대응 영역**이 되었습니다.

> **"제품의 보안성"과 "조직의 운영체계"가 동시에 요구되며,**
> **심사 제출자료와 실제 운영이 일치해야 한다.**

따라서 제조업체의 선택지는 *"보안 기능을 넣느냐"*가 아니라 **"어떤 어프로치로 관리체계를 도입하고 운영할 것인가"**입니다. 강의 초반부에서는 이 선택지들을 구조적으로 분석합니다.

분석 프레임

1 분석 프레임 — 두 축, 세 옵션

SaMD 제조업체가 고려할 수 있는 어프로치는 **도입(Build)**과 **운영(Operate)**의 두 축으로 나뉘며, 각 축에서 세 가지 옵션이 존재합니다.

구분	도입 단계	운영 단계
옵션 1	자체 수립	자체 운영
옵션 2	외부 전문가 조력 수립	외부 전문가 운영 대행
옵션 3	AI 활용	AI 적용

> 옵션 1·2는 **"주체"**의 문제, 옵션 3(AI)은 **"수단"**의 문제.
> AI는 단독 어프로치라기보다 **1과 2를 가속·보강하는 레이어**로 이해해야 합니다.

도입 어프로치 (1/3)

2 도입 어프로치 분석

2.1 자체 수립

내부 인력이 정책·절차·양식·운영기준을 직접 설계·정착시키는 방식.

✓ 강점

- 제품 아키텍처·SDLC·조직 문화에 최적화된 설계 가능
- 장기적 내재화, 외부 의존도 최소화
- 초기 컨설팅 비용 절감

⚠ 약점

- 규제 해석 오류 리스크 (IEC 62304 등 해석 편차)
- 수립 기간 장기화 (6~12개월)
- "문서는 있으나 운영은 안 되는" 형식화 위험

적합 조건: RA/QA·SW개발 리더가 내부에 있고, 제품 수가 적으며, 장기 내재화를 지향하는 조직.

도입 어프로치 (2/3)

2.2 외부 전문가 조력 수립

컨설팅사·전문기관의 도움을 받아 단기간에 체계를 구축하되 운영 주체는 내부가 유지하는 방식.

✓ 강점

- 법령·고시·심사 기대수준을 즉시 반영 → 인허가 리스크 최소화
- 3자 관점의 Gap 분석으로 사각지대 해소
- 수립 기간 단축 (3~6개월), 표준 템플릿 조기 확보

⚠ 약점

- 초기 비용 발생
- 외부 산출물이 내부 현실과 괴리 시 "형식 문서" 고착
- 내부 온보딩이 약하면 운영 전환 실패

성공 조건: 컨설턴트가 "문서를 대신 써주는" 구조가 아니라, **내부 실무자 워크숍 기반으로 공동 설계**해야 합니다. 인수인계와 모의점검이 종료 시점의 핵심 활동입니다.

도입 어프로치 (3/3)

2.3 AI 활용

도입 단계에서 AI는 **수립을 대체하지 않고 가속**합니다.

✓ 효과적 활용 영역

- 법령·고시·가이드 기반 Gap 분석 자동화
- 정책서·절차서·체크리스트 초안 생성 (시간 60~80% 단축)
- STRIDE/TARA 기반 위협 시나리오 초안 도출
- 심사 제출자료 간 정합성 점검
- 교육자료·FAQ 자동 생성

⚠ 한계와 통제 원칙

- 규제 해석의 최종 판단과 환자안전 영향은 사람이 책임
- 민감 정보를 공개형 AI에 입력하는 것은 통제 필요
- AI 산출물도 기록 관리, 사람의 검토·승인 절차 필수

운영 어프로치 (1/3)

3 운영 어프로치 분석

3.1 자체 운영

내부 조직이 취약점 모니터링, 변경 검토, 사고 대응, 문서 유지관리를 직접 수행.

✓ 강점

- 제품·고객·배포환경에 대한 깊은 이해 → 대응 속도와 정확도
- 개발·QA·CS와 자연스러운 연계
- 역량의 조직 내 축적

⚠ 약점

- 24/7 모니터링 체계 유지의 현실적 어려움
- 고급 보안 분석 인력 채용·유지의 고정비
- 일상업무에 밀려 정기점검 형식화 가능성

운영 어프로치 (2/3)

3.2 외부 전문가 운영 대행

취약점 모니터링, 정기점검, 사고 대응 지원 등을 외부 전문기관(MSSP)이 수행.

✓ 강점

- 24/7 SOC, 최신 위협 인텔리전스 활용
- 내부 인력 부족 완화
- 객관적 점검으로 사각지대 해소

⚠ 약점과 한계

- 지속적인 구독·위탁 비용
- 제품·임상 맥락 이해 부족 시 오탐 증가
- **법적 책임은 위탁해도 제조업자에게 귀속**

현실적 모델: 완전 대행보다 **부분 대행형**이 효과적 — 월간 취약점 모니터링, 분기 정기점검, 반기 문서 갱신 리뷰, 사고 발생 시 포렌식 지원, 심사 직전 집중 지원.

운영 어프로치 (3/3)

3.3 AI 적용

운영 단계는 **AI의 효과가 가장 크게 나타나는 영역**입니다.

✓ 효과적 활용 영역

- **SBOM + CVE 자동 매칭:** 컴포넌트 목록과 신규 CVE를 자동 대조, CVSS 기반 우선순위 자동 알림
- **AI 이상 탐지:** 접근 로그·API 호출 패턴의 정상 베이스라인 학습, 편차 탐지
- **사고 대응 어시스턴트:** 증상 입력 시 플레이북 가이드, 식약처 신고 양식 초안 생성
- **정기 보고서 자동화:** 취약점·패치·사고 이력 집계, 보고서 초안 생성
- **변경영향분석 보조:** 변경요청서와 위험평가서 간 영향항목 자동 추출

⚠ 통제 원칙

- AI는 "보조", 최종 판단은 사람
- Human-in-the-Loop 필수
- AI 자동화 실패 감지 알림·수동 점검 병행

비교 요약 (1/2)

4 어프로치 비교 요약

도입 단계

기준	자체 수립	외부 조력 수립	AI 활용
초기 속도	느림	빠름	매우 빠름
규제 해석 정확도	내부 역량 의존	높음	검토 없으면 불안정
내재화 수준	높음	중~높음	낮음~중
문서 품질 일관성	편차 큼	비교적 높음	매우 높음
단독 권장도	제한적	가장 권장	보조수단

비교 요약 (2/2)

운영 단계

기준	자체 운영	외부 운영 대행	AI 적용
제품 이해도	매우 높음	중간	낮음
지속 가능성	인력 확보 시 높음	계약 의존	운영체계 의존
전문분석 깊이	편차 큼	높음	보조적
비용 구조	인건비 중심	용역비 중심	도구·통제비
단독 권장도	필수 기반	부분 대행 권장	강한 보조수단

결론

5 결론 — 어느 하나만으로는 부족하다

세 옵션을 개별적으로 분석하면 공통된 결론이 도출됩니다.

1. **자체만으로는 느리고 위험하다** — 규제 해석 편차, 수립 기간, 전문성 공백
2. **외부만으로는 내재화가 안 된다** — 문서는 완성되나 운영은 공회전
3. **AI만으로는 책임을 질 수 없다** — 가속기일 뿐, 판단과 승인은 사람의 몫

> SaMD 제조업체가 마주한 현실은 **"하나를 선택하는" 문제가 아니라**
> **"어떻게 조합할 것인가"**의 문제입니다.

도입 단계 최적해
외부 전문가 조력 + AI 가속 + 내부 책임 승인

운영 단계 최적해
자체 운영 중심 + 외부 부분 대행 + AI 자동화

이것이 초반부 분석이 가리키는 방향이며, **이어지는 중반부에서는 "그렇다면 컨설팅사들은 이 수요에 어떻게 대응하고 있는가"를 분석**하고, 후반부에서 구체적인 실행 방안을 제시하겠습니다.

02

타 컨설팅 사의 대응 전략 분석



분석의 관점

0 왜 타 컨설팅사의 대응을 들여다보는가

초반부에서 확인한 것은 명확합니다. SaMD 제조업체는 도입·운영 어느 단계에서도 **단독 해결이 어렵고, 하이브리드 조합이 불가피**합니다.

그렇다면 이 수요에 컨설팅 시장은 어떻게 반응하고 있을까요?

> **타 컨설팅사들이 자신의 서비스 모델·조직·도구·수익구조를 어떻게 재편하고 있는지**를 분석합니다.
> 이는 단순한 시장 관찰이 아니라, **"제조업체 입장에서 어떤 컨설팅사를 골라야 하는가"를 판단하기 위한 기준**을 만드는 작업입니다.

공통 방향성 (1/3)

1 타 컨설팅사들이 합의하는 5가지 방향

여러 컨설팅사가 각기 다른 프레임으로 전략을 제시하지만, 바닥에 깔린 흐름은 놀랍도록 일치합니다.

1.1 포지셔닝의 근본적 전환

> **"보안 문서 작성 지원업체" → "SaMD 규제형 사이버보안 관리체계 구축·운영 파트너"**

규제가 허가 시점에서 끝나지 않고 **변경관리·취약점 대응·사후관리**로 이어지는 전주기 구조라는 점이, 컨설팅사의 역할 자체를 재정의하고 있습니다.

1.2 수익모델의 재편: 일회성 → 리커링(Recurring)

단발성 구축 컨설팅만으로는 지속 가능성이 없으며, **운영 단계의 월정 리테이너·연간 감사·SLA 기반 사고 대응**으로 수익 기반을 재설계해야 한다는 공통 인식.

계층	성격	예시
프로젝트형	초기 도입, 일회성	Gap 분석, 관리체계 수립, 파일럿 적용
리테이너형	월정·연간 계약	vCISO, 취약점 모니터링, 정기점검, 변경영향평가
플랫폼형	구독·도구 기반	AI 문서 생성기, CVE-SBOM 매칭, SaaS 대시보드

공통 방향성 (2/3)

1 타 컨설팅사들이 합의하는 5가지 방향

여러 컨설팅사가 각기 다른 프레임으로 전략을 제시하지만, 바닥에 깔린 흐름은 놀랍도록 일치합니다.

1.3 서비스 통합: RA/QA + 제품보안 + DevSecOps

기존 **의료기기 RA 컨설팅**(기술 보안 구현 역량 부족)과 **일반 정보보안 컨설팅**(의료기기 규제 이해 부족)의 **교차점 공백**이 곧 새로운 시장입니다.

- **규제/품질 리드** — 디지털의료제품법, 식약처 가이드라인, GMP/QMS 연계
- **제품보안 리드** — 위협모델, SDL, 취약점 대응
- **SW/클라우드 아키텍처 리드** — SaaS형 SaMD, CI/CD, API 구조
- **운영서비스 리드** — 리테이너, 정기점검, 사고대응
- **AI/자동화 리드** — 내부 도구화, 산출물 정합성 검증

1.4 AI는 "대체"가 아니라 "증폭" 수단

> **전문가가 프레임을 설계하고, AI가 초안·정리·추적성·반복업무를 가속한다.**

원가 절감	품질 일관성	고객 자립 지원
1인 컨설턴트의 서비스 범위 확장	개인 역량 편차를 AI 검증이 보완	도구를 고객사에 이전해 관계 장기화

공통 방향성 (3/3)

1 타 컨설팅사들이 합의하는 5가지 방향

여러 컨설팅사가 각기 다른 프레임으로 전략을 제시하지만, 바닥에 깔린 흐름은 놀랍도록 일치합니다.

원가 절감	품질 일관성	고객 자립 지원
1인 컨설턴트의 서비스 범위 확장	개인 역량 편차를 AI 검증이 보완	도구를 고객사에 이전해 관계 장기화

1.5 글로벌 규제 정합성이 차별화 요소로 부상

국내 식약처 보안지침만 다루는 타 컨설팅사와, **FDA Cybersecurity Guidance·EU MDR·IMDRF N60·IEC 81001-5-1**을 통합 프레임워크로 제시하는 컨설팅사 사이의 격차가 벌어지고 있습니다. 해외 진출 수요가 있는 고객에게는 **글로벌 Crosswalk 매핑 역량**이 선택 기준이 됩니다.

4가지 유형 (1/2)

2 대응 전략의 4가지 유형 — 시장의 분화

공통 방향은 있지만, 구체적 실행 모델에서는 네 가지 유형으로 분화되고 있습니다.

유형 A

전주기 하이브리드형 (정통 접근)

"프로젝트 + 리테이너 + 플랫폼"의 3층 구조를 균형 있게 가져가는 모델.
Basic(진단) → Standard(구축) → Premium(운영)의 고객 성숙도별 패키지.

✓ 고객 락인 효과, 안정적 재무구조 ⚠ 초기 조직 구축 비용 🛠 중견 이상 적합

유형 B

CaaS(Compliance-as-a-Service) 중심형

인력 부족 중소 SaMD 제조사를 겨냥, **구독형 보안 관리 서비스**를 전면에 내세우는 모델.
MSSP와의 전략적 제휴로 24/7 운영 역량을 확보.

✓ 중소 고객 진입장벽 해소, 반복 매출 ⚠ MSSP 의존도, 커스터마이징 제한 🛠 MSSP 파트너십 보유 조직

4가지 유형 (2/2)

2 대응 전략의 4가지 유형 — 시장의 분화

공통 방향은 있지만, 구체적 실행 모델에서는 네 가지 유형으로 분화되고 있습니다.

유형 C

AI-Native 플랫폼형

AI를 **서비스 전달 방식 자체**로 전환하는 모델.
컨설팅 수수료 → Annual Retainer → SaaS 구독으로 비즈니스 모델을 진화. 1인 또는 소규모 조직이 AI를 통해 확장성을 확보.

✓ 원가 경쟁력, 확장성, 차별화 | ⚠ 초기 플랫폼 개발 투자 | 🛠 소규모·1인 전문가, AI 역량 보유자

유형 D

기술 심층 특화형

SBOM 관리, 전문 침투 테스트, 위협 인텔리전스, VDP 대행 등 **기술적 심층 서비스**에 집중.
Cybellum·HatBOM 등 글로벌 보안 벤더와의 파트너십으로 도구 오케스트레이션 제공.

✓ 기술적 차별화, 대형 고객 대상 경쟁력 | ⚠ 규제 문서화 영역 공백 | 🛠 보안 기술 중심 기업

서비스 포트폴리오 (1/3)

3 서비스 포트폴리오의 실제

여러 컨설팅사가 제시하는 서비스를 종합한 시장 상품 현황.

도입 단계 상품

상품명(통칭)	기간	성격	가격대
Quick Scan / 진단형	2~4주	현황 진단 + 로드맵	저가 진입
Full Build / 풀패키지	4~6개월	관리체계 전체 수립	핵심 수익
Co-Build / Advisory	6~9개월	내부 주도 + 전문가 동행	중간 가격
우수 관리체계 인증 지원	6~12개월	허가 혜택 연계 전략	고부가

서비스 포트폴리오 (2/3)

3 서비스 포트폴리오의 실제

여러 컨설팅사가 제시하는 서비스를 종합한 시장 상품 현황.

운영 단계 상품

상품명(통칭)	주기	성격
Annual Retainer	월정	취약점 모니터링, 보고서, IR 지원
Annual Audit	연 1회	보안지침 준수 독립 검증
침해행위 긴급 대응	사고 발생 시	신고 지원, RCA, 재발 방지
vCISO 지원	월간	외부 보안책임자 역할
변경영향평가 지원	상시	통신기능 변경 ↔ 보호조치 ↔ 변경관리

서비스 포트폴리오 (3/3)

3 서비스 포트폴리오의 실제

여러 컨설팅사가 제시하는 서비스를 종합한 시장 상품 현황.

AI/도구 기반 상품

모듈	기능
CVE-SBOM 자동 매칭 봇	SBOM 업로드 → 신규 CVE 자동 알림
사이버보안 문서 자동 생성기	제품 정보 → 절차서·IRP 초안
식약처 신고 보조 챗봇	증상 입력 → 신고 양식 + 조치 가이드
보안 감사 체크리스트 자동화	증적 업로드 → 준수 대시보드
규제 모니터링 봇	식약처·FDA 공고 → 고객 영향 분석

> 공통점: **"허가 시점 문서 작성"이라는 단일 상품에서 벗어나, 도입-운영-도구화로 이어지는 다층 포트폴리오**가 되었다.

피해야 할 함정

4 타 컨설팅사들이 경고하는 함정

여러 컨설팅사의 전략 문서에서 피해야 할 대응 방식에 대한 경고가 거의 동일하게 나타납니다.

1. **문서 대행 중심 접근**
   심사 시점에는 그럴듯하지만, 실제 운영 증적이 없으면 곧 무너집니다.

2. **일반 정보보안 프레임의 단순 이식**
   ISMS·일반 기업 보안통제를 그대로 가져오면 SaMD의 환자안전·임상성·인허가 문서 구조가 반영되지 않습니다.

3. **개발조직과 분리된 규제문서 작성**
   실제 제품 아키텍처·API·배포방식·패치 구조를 모르면 완성도 높은 체계를 만들 수 없습니다.

4. **AI 무통제 사용**
   빠른 문서 생산이 가능하지만, 최신 규정 오반영·고객정보 유출·부정확한 기술서술이 오히려 리스크를 증폭시킵니다.

역으로 말하면: 컨설팅사를 고를 때 **"이 네 가지 함정을 피하고 있는가"**가 핵심 체크포인트입니다.

시장의 신호

5 컨설팅 시장이 가리키는 세 가지 신호

1 "제대로 된" 컨설팅사의 모습이 바뀌고 있다

과거의 기준: 템플릿이 많다, 심사 통과 경험이 많다.
현재의 기준: 규제 해석 + 제품 아키텍처 이해 + 운영 연속성 + AI 활용 통제가 하나의 조직 안에 결합되어 있는가.

2 리테이너가 핵심이 된다 = 제조업체도 그렇게 계약해야 한다

타 컨설팅사들이 순환환 구조로 재편하는 이유는 **규제 자체가 운영 중심**이기 때문입니다. 제조업체가 여전히 "한 번에 끝나는 구축 프로젝트"만 찾는다면, 그것은 **규제 구조와 어긋난 계약**입니다.

3 AI는 선택이 아니라 전제 조건이 되었다

AI를 활용하지 않는 컨설팅사는 **원가 경쟁력에서 밀리고, 품질 일관성에서 편차가 커지며, 고객 자립 지원 도구를 제공할 수 없습니다.** 제조업체 입장에서도 "AI를 통제된 방식으로 활용하는 컨설팅사"를 선택하는 것이 장기적으로 유리합니다.

후반부 연결

6 후반부로의 연결

그렇다면 제조업체는 무엇을 해야 하는가?

여기까지 우리는 두 가지를 확인했습니다.

PART 1 · 초반부

SaMD 제조업체의 어프로치 분석

→ **단독 옵션은 없고, 하이브리드가 답이다**

PART 2 · 중반부

타 컨설팅사의 대응 전략

→ **전주기 파트너·순환 구조·AI-Native로 시장 재편**

그러나 이 둘 사이에는 여전히 간극이 있습니다.

"컨설팅사가 이렇게 바뀌고 있다"는 공급 측 분석만으로는, 제조업체가 내일 아침 무엇을 해야 할지 알 수 없습니다.

후반부에서 다룰 내용

- 기업 규모·보안 성숙도·규제 대응 시급성에 따른 **구체적 의사결정 가이드**
- **컨설팅사 선택 체크리스트**
- **단계별 실행 로드맵**
- "오늘부터 무엇을 시작할 것인가"에 대한 답

03

실질적 대응 방안
브이웨이가 여러분께 제안드리는 것



앞선 분석 요약

0 앞선 두 분석이 말해준 것

PART 1 · 초반부

SaMD 제조업체의 어프로치 분석

→ **하이브리드 조합이 불가피**

PART 2 · 중반부

컨설팅사의 대응 전략

→ **전주기·리커링·AI-Native로 재편**

여기까지는 공급 측 분석입니다. 여러분께 필요한 것은 **"내일 아침 무엇을 해야 하는가"**에 대한 답입니다.

> **"여러분이 직접 하든, 브이웨이와 함께 하든, AI를 쓰든 — 결국 규제 적합성과 운영 가능성이 중요합니다. 브이웨이는 그 세 가지 접근을 모두 지원할 수 있는 하이브리드 조력자입니다."**

기본 원칙 (1/2)

1 브이웨이가 드리는 제안의 기본 원칙

구체적 서비스로 들어가기 전에, 브이웨이가 일하는 방식의 세 가지 원칙입니다.

1 "대신 써드리는 사람"을 넘어, 구조와 체계를 장악한 "전문가 그룹"

여러분의 제품과 조직을 가장 잘 아는 건 여러분 자신입니다. 브이웨이의 역할은 **규제 해석과 체계 설계를 제공**하고, 여러분이 실제로 운영 가능한 형태로 남기는 것입니다. 심사 제출 문서와 실제 운영이 분리되는 순간, 체계는 무너집니다.

2 IEC 62304·ISO 14971·IEC 81001-5-1 기반 프로세스 품질 컨설턴트

일반 정보보안 컨설턴트가 아닙니다. 의료기기 규제와 SW 개발 프로세스를 동시에 이해하기에, 보안지침 요구사항을 **기존 IEC 62304 SDL·QMS와 연결하는 방식**으로 설계합니다. 새로 쌓는 게 아니라 기존 체계를 확장하는 접근이기에, 훨씬 빠르고 현실적입니다.

기본 원칙 (2/2)

1 브이웨이가 드리는 제안의 기본 원칙

구체적 서비스로 들어가기 전에, 브이웨이가 일하는 방식의 세 가지 원칙입니다.

3 AI-Native 방식으로 일합니다

단순한 효율화가 아니라 세 가지를 동시에 달성합니다.

가격대	품질 일관성	자립 운영
1인·소규모 조직도 감당 가능	개인 역량 편차를 AI 검증이 보완	AI 도구를 여러분께 이전

도입 단계 (1/3)

2 도입 단계 — 여러분의 선택에 따른 역할

여러분이 어떤 도입 방식을 선호하시든, 거기에 맞춰 역할을 조정합니다.

코치형

"내부에서 직접 만들고 싶다"고 하실 때

여러분의 목적은 내부 역량 내재화와 외부 의존도 축소. 좋은 방향입니다. 브이웨이는 **코치이자 리뷰어**로 들어갑니다.

브이웨이가 해드리는 것	형태
규제 요구사항 해설 워크숍	1~2일 집합 세션
현행 체계 Gap 분석 진단	1주 집중 진단
정책서·절차서·양식 목차 설계안	템플릿 라이브러리 기반
내부 작성 문서 리뷰·보완	격주 리뷰 세션
파일럿 제품 보안 요구사항·위협분석 리뷰	공동 워크숍
심사 제출자료 정합성 점검	제출 전 최종 리뷰
모의심사·인터뷰 대응 훈련	심사 직전 Mock Audit

"여러분이 직접 만드시되, 틀리지 않게 만들도록 브이웨이가 옆에서 받쳐드립니다."

도입 단계 (2/3)

2 **도입 단계 — 여러분의 선택에 따른 역할**

여러분이 어떤 도입 방식을 선호하시든, 거기에 맞춰 역할을 조정합니다.

설계형

"빠르고 정확하게 구축되길 원하신다"고 하실 때

첫 규제 대응이거나, 허가 일정이 촉박하거나, 보안과 GMP를 동시에 정비해야 할 때. 브이웨이는 **체계 설계자이자 구축 리드**로 들어갑니다.

- 착수 진단·범위 정의 → 정책/절차/양식/RACI 전체 체계 설계
- 제품군·서비스 구조 분석 기반 위협모델(TARA) 프레임 구축
- 취약점 관리·변경관리·사고대응·침해신고 프로세스 설계
- 허가 제출용 "보호조치 자료" 패키지 정리
- SBOM 생성·관리 절차와 초기 SBOM 구축
- 내재화 교육·인수인계·시범 운영까지

차별화: 규제 문서와 운영 문서를 분리하지 않고, 제품별 기술문서와 조직 절차를 연결하며, 개발/클라우드/배포 구조까지 고려한 설계.
ISO 13485·IEC 62304 경험으로 기존 QMS 위에 보안지침을 올리는 작업이 매끄럽습니다.

"브이웨이가 설계하고, 여러분이 운영하실 수 있게 남겨드립니다."

도입 단계 (3/3)

2 **도입 단계 — 여러분의 선택에 따른 역할**

여러분이 어떤 도입 방식을 선호하시든, 거기에 맞춰 역할을 조정합니다.

AI 통제형

"AI를 써서 빠르게 구축하고 싶다"고 하실 때

브이웨이는 **AI 적용 설계자이자 품질 통제자**로 들어갑니다.

- AI 활용 범위 정의 및 경계 설정
- 규제형 문서 초안 생성을 위한 **프롬프트·템플릿 라이브러리** 제공
- 보안 요구사항 코파일럿 구축
- 위협 시나리오 후보 자동 도출 체계
- 변경영향분석 초안 자동화
- 문서 간 정합성 자동 검토 파이프라인
- AI 결과의 전문가 검토·승인 기준 수립 (Human-in-the-Loop)

장점: 도구가 여러분 조직에 남습니다. 프로젝트가 끝나도 계속 AI를 활용해 문서를 생성·갱신할 수 있습니다.

"AI로 빠르게 만들되, 규제형 품질로 다듬어 드립니다. 그리고 그 도구는 여러분께 남습니다."

운영 단계 (1/3)

3 운영 단계 — 구축 후가 진짜 시작입니다

취약점 모니터링, 변경영향평가, 사고 대응, 증적관리가 **매일·매월·매분기** 돌아가야 합니다.

고도화 파트너형

"내부 인력으로 운영하겠다"고 하실 때

내부 운영은 제품 이해도 면에서 가장 강력한 선택. 브이웨이는 **정기적으로 받쳐드리는 방식**으로 조력합니다.

월간	분기	반기	연간
운영 리뷰 1회 취약점 이슈 해석	내부점검 체크리스트 문서 개정 리뷰	보안 운영 현황 감사 개선 권고	모의심사(Mock Audit) 신규 인력 온보딩

수시
경영층 KPI 대시보드 설계

"여러분이 운영하시되, 무너지지 않도록 브이웨이가 정기적으로 받쳐드립니다."

운영 단계 (2/3)

3 운영 단계 — 구축 후가 진짜 시작입니다

취약점 모니터링, 변경영향평가, 사고 대응, 증적관리가 **매일·매월·매분기** 돌아가야 합니다.

vCISO형 운영 파트너

"전문가 지원이 상시 필요하다"고 하실 때

내부 인력이 부족하거나 보안 운영 전문성이 약한 경우, **외부 보안책임자(vCISO) 역할**을 맡아드립니다.

- 월간 취약점 모니터링 보고 (NVD/KISA/OSS 공지 연동)
- SBOM 갱신 검토 및 신규 CVE 영향 분석 (분기)
- 변경요청 보안 영향 검토 (상시)
- **침해행위 긴급 대응 SLA** — 초기 대응, 식약처 신고 서류, RCA, 재발방지까지
- 경영층 보고자료·규제기관 질의 대응 보조
- 연간 심사 대비 집중 지원

계약 형태: 월정 리테이너 + 긴급 대응 옵션. 법적 책임은 여러분께 귀속, 브이웨이는 실무의 지속성을 보강.

"여러분의 책임은 여러분께 두고, 운영 실무는 브이웨이가 보강해드립니다."

운영 단계 (3/3)

3 운영 단계 — 구축 후가 진짜 시작입니다

취약점 모니터링, 변경영향평가, 사고 대응, 증적관리가 **매일·매월·매분기** 돌아가야 합니다.

자동화 파트너형

"AI로 운영을 가볍게 만들고 싶다"고 하실 때

운영 단계는 AI가 가장 큰 효과를 내는 영역입니다.

모듈	기능
CVE-SBOM 자동 매칭 봇	SBOM 업로드 → 신규 CVE 매칭 → 심각도 분류 → 담당자 알림
사이버보안 문서 자동 생성기	제품 정보 → 절차서·IRP·보안 평가서 초안
식약처 신고 보조 챗봇	증상 입력 → 신고 양식 + 조치 가이드
보안 감사 체크리스트 자동화	증적 업로드 → 8개 영역 준수 대시보드
변경영향평가 코파일럿	변경요청서 → 보호조치 영향 + 변경관리 해당 여부
월간 보고서 자동 생성기	모니터링 + 조치 이력 → 경영진·규제기관용 보고서

원칙: AI는 판단을 "보조"합니다. 배포 중단·사고 판정·환자안전 영향 판단·대외 통지는 반드시 사람이 결정합니다. Human-in-the-Loop 구조 자체를 설계해드립니다.

"AI가 운영을 가볍게 만들고, 브이웨이는 그 AI가 규제에 맞게 작동하도록 설계해드립니다."

상황별 추천 (1/3)

4 여러분의 상황별 추천 조합

"저라면 이렇게 제안드립니다" — 규모·역량·시급성에 따라 다른 조합을 권합니다.

소형 SaMD 기업

인원 30명 미만, 보안 역량 부재

규제 대응 방법을 모르고, 전담 인력 채용은 비현실적이며, 비용에 민감합니다.

제안: Quick Scan (2~4주 현황 진단) → Full Build (풀 패키지 구축) → Annual Retainer (월정 운영 지원)
AI 자동화 포함 → 기존 컨설팅 대비 훨씬 낮은 가격에 가능

"규제 처벌 리스크보다 브이웨이와의 계약이 훨씬 저렴합니다. 그리고 내부 인력 채용 부담이 사라집니다."

상황별 추천 (2/3)

4 여러분의 상황별 추천 조합

"저라면 이렇게 제안드립니다" — 규모·역량·시급성에 따라 다른 조합을 권합니다.

중형 SaMD 기업

인원 30~200명, 일부 보안 역량 보유

QA/RA 담당자가 있지만, 사이버보안 전문성이 부족. 내부 역량을 키우고 싶지만 방법을 모릅니다.

제안: Co-Build / Advisory 동행 + 담당자 양성 교육

기존 IEC 62304 SDL 프로세스에 보안지침을 "연결"하는 방식 — 새로 시작하는 것이 아닙니다.

"외부 의존 없이 여러분이 스스로 운영할 수 있는 역량을 이식해드립니다."

상황별 추천 (3/3)

4 여러분의 상황별 추천 조합

"저라면 이렇게 제안드립니다" — 규모·역량·시급성에 따라 다른 조합을 권합니다.

대형 / 글로벌 진출 기업

내부 보안팀 보유, FDA·EU MDR 정합성 필요

의료기기 특화 규제 이해가 부족하고, 글로벌 규제 정합성이 필요합니다.

제안: Annual Audit (연 1회 독립 검증) + 글로벌 규제 Crosswalk + 우수 관리체계 인증

브이웨이는 기술 보안이 아니라 **규제 해석 전문가**로 역할을 분리합니다.

"여러분의 규제 준수 증거를 국내 식약처와 글로벌 심사 기관이 모두 인정하는 형태로 만들어드립니다."

실행 3단계 (1/3)

5 지금 바로 시작할 수 있는 3단계

오늘 이후 여러분께서 바로 실행 가능한 세 가지입니다.

1 단계 **진단 — 이번 주 내**

3가지 질문으로 자가 진단해 보십시오.

- (a) 사이버보안 담당자가 지정되어 있는가?
- (b) 침해행위 인지 시 식약처 신고 프로세스가 문서화되어 있는가?
- (c) 제품 SBOM이 존재하는가?

하나라도 "아니오"라면, 이미 규제 리스크에 노출되어 있습니다.

실행 3단계 (2/3)

5 **지금 바로 시작할 수 있는 3단계**

오늘 이후 여러분께서 바로 실행 가능한 세 가지입니다.

2 단계 **Gap Scan — 이번 달 내**

자가 진단으로 부족하다면, **Quick Scan 서비스**로 2~4주 내에 보안지침 8개 영역 전체에 대한 현황을 파악하실 수 있습니다.

이 진단만으로도 **경영진 의사결정에 쓸 수 있는 단계별 로드맵과 예산 시뮬레이션**이 나옵니다.

실행 3단계 (3/3)

5 **지금 바로 시작할 수 있는 3단계**

오늘 이후 여러분께서 바로 실행 가능한 세 가지입니다.

3 단계 **파일럿 착수 — 3개월 내**

제품 1종에 대해 관리체계를 먼저 적용해 보십시오. 전 제품 동시 적용은 비현실적입니다.

1개 제품으로 **성공 경험**을 쌓고, 이를 **템플릿화**하여 나머지 제품으로 확산하는 것이 가장 안전한 경로입니다.

마치며

6 마치며

오늘 짧은 시간이지만 많이 생각할 내용을 함께 해 주셔서 감사드립니다.
초반에는 여러분의 어프로치를 분석했고, 중반에는 컨설팅 시장이 어떻게 바뀌고 있는지 보여드렸으며, 후반에는 브이웨이가 실제로 어떻게 조력해드릴 수 있는지 말씀드렸습니다.

"규제 대응은 혼자 하기 어렵고, 외주만으로도 안 되며, AI만으로는 책임질 수 없습니다.

브이웨이는 이 세 가지를 통합해 여러분의 규제 적합성과 운영 가능성을 하나로 묶어드리는 하이브리드 실행 파트너입니다.

여러분이 어떤 선택을 하시든, 브이웨이가 그 선택을 성공시킬 방법을 가지고 있습니다.

규제 시행 초기는 기회의 창입니다.
먼저 준비한 기업이 시장의 기준을 정의합니다.
언제든 편하게 연락 주십시오. 감사합니다.



스마트 의료 안전
컨퍼런스 2026

Thank You

주식회사 브이웨이