

우 수 관 리 체 계 인 증 기 준 에
관 한 규 정

1. 제정이유

「디지털의료제품법」 제정(법률 제20139호, 2024. 1. 23. 공포, 2025. 1. 24. 시행) 및 「디지털의료제품법 시행규칙」에 따라 우수 관리체계 인증 기준에 관하여 필요한 사항을 규정하려는 것임

2. 주요내용

가. 인증심의위원회(안 제2조)

우수 관리체계 인증과 관련하여 인증심의위원회의 구성 및 운영에 대하여 세부 규정을 마련함

나. 우수 관리체계 인증 기준(안 제3조)

디지털의료기기 우수 관리체계 인증 기준에 대하여 명확하게 규정함

다. 우수 관리체계의 인증 접수(안 제4조)

디지털의료기기 우수 관리체계 인증 접수 절차에 대한 세부 규정을 마련함

라. 우수 관리체계의 인증 심의(안 제5조)

우수 관리체계 인증 심의를 위한 심의위원회 개최와 심의 결과에 대하여 규정을 마련함

마. 우수 관리체계의 인증 평가(안 제6조)

우수 관리체계 인증 평가를 위한 서면 및 현지조사 계획에 대한 세부 내용을 규정함

바. 우수 관리체계의 인증서 교부(안 제7조)

우수 관리체계 인증서 발급에 대한 세부 내용을 마련함

사. 이의 신청(안 제8조)

우수 관리체계 인증 기준 결과에 이의가 있는 경우에 대한 세부 내용을 마련함

아. 우수 관리체계의 인증 유효기간(안 제9조)

우수 관리체계 인증 유효기간에 대하여 세부 내용을 마련함

자. 재검토 기한(안 제10조)

우수 관리체계 인증 기준 규정에 대한 타당성 검토를 위하여 규정을 마련함

3. 참고사항

가. 관계법령 : 디지털의료제품법, 같은 법 시행령 및 시행규칙

나. 예산조치 : 별도조치 필요 없음

다. 합 의 : 해당사항 없음

라. 기 타

1) 행정예고('24. 12. 16. ~ '25. 1. 6.) 결과, 특이사항 없음

2) 국무조정실 규제심사(2025. 6. 2.) : 특이사항 없음

식품의약품안전처 고시 제2025-38호

「디지털의료제품법」 제16조 및 「디지털의료제품법 시행규칙」 제31조에 따라 「우수 관리체계 인증 기준에 관한 규정」을 다음과 같이 제정 고시합니다.

2025년 6월 9일

식품의약품안전처장

우수 관리체계 인증 기준에 관한 규정

제1조(목적) 이 고시는 「디지털의료제품법」 제16조 및 「디지털의료제품법 시행규칙」 제31조에 따라 우수 관리체계 인증 기준 및 절차 등에 관한 세부사항을 규정함을 목적으로 한다.

제2조(인증심의위원회) ① 「디지털의료제품법」 제48조제1항에 따른 인증업무등 대행기관의 장(이하 "인증업무등 대행기관의 장"이라 한다)은 우수 관리체계 인증과 관련하여 다음 각 호의 사항을 심의하기 위하여 인증 심의위원회(이하 "심의위원회"라 한다)를 운영할 수 있다.

1. 별표 1의 우수 관리체계 인증 기준의 변경
2. 우수 관리체계 인증을 받고자 하는 디지털의료기기제조업자 및 디지털의료기기수입업자(이하 "디지털의료기기제조업자등"라 한다)에

대한 인증·인증취소 여부 및 조사계획서 심의

3. 우수 관리체계 인증을 받은 디지털의료기기제조업자등에 대한 지원 방안, 관련 정책

4. 그 밖에 우수 관리체계 인증 제도와 관련하여 인증업무등 대행기관의 장이 필요하다고 인정하는 사항

② 제1항에 따른 심의위원회의 구성 및 운영과 관련한 사항은 식품의약품안전처장의 승인을 받아 인증업무등 대행기관의 장이 정한다.

제3조(인증 기준) 「디지털의료제품법」(이하 "법"이라 한다) 제16조제4항에 따른 우수 관리체계 인증 기준의 세부 내용은 별표 1과 같다.

제4조(인증 접수) ① 인증업무등 대행기관의 장은 시행규칙 제31조제1항에 따라 우수 관리체계 인증을 신청 받은 경우 다음 각 호의 사항을 준수하여야 한다.

1. 「디지털의료제품법 시행규칙」(이하 "시행규칙"이라 한다) 제31조제1항에 따른 신청서 및 첨부자료의 제출여부를 5일 이내에 확인하여 흠이 없는 경우에는 접수한다.

2. 제1호에 따른 첨부자료의 제출여부 확인결과 첨부자료의 미비 등 흠이 있는 경우에는 행정절차법에서 정한 바에 따라 첨부자료의 제출에 대한 보완기한을 설정하여 신청인에게 보완 요구하여야 한다.

② 인증업무등 대행기관의 장은 제1항에 따른 신청을 조사계획서를 작성하여 심의위원회에 회부하고 그 사실을 신청인에게 통보하여야 한다.

제5조(인증 심의) ① 인증업무등 대행기관의 장은 제4조제2항에 따른 조사계획서를 심의하기 위하여 심의위원회를 개최할 수 있다.

② 인증업무등 대행기관의 장은 제1항에 따른 심의 결과를 평가계획서에 반영하고 조사계획을 수립하여 신청인에게 통보하여야 한다.

제6조(인증 평가) ① 제5조제2항에 따른 조사계획에는 서면 및 현지조사를 포함한다.

② 인증업무등 대행기관의 장은 현지실사를 실시하기 전 신청자와 협의하여 현지조사 일정을 선정할 수 있다.

③ 인증업무등 대행기관의 장은 조사결과를 분석 및 평가한 후 평가 결과보고서를 작성하여 10일 이내에 식품의약품안전처장에게 보고하여야 한다.

제7조(인증서 교부) ① 인증업무등 대행기관의 장은 제6조제3항에 따른 평가결과 적합한 경우에는 시행규칙 제31조제4항에 따라 우수 관리체계 인증서를 발급한다.

② 인증업무등 대행기관의 장은 제1항에 따른 심사결과를 우수 관리체계 인증신청서가 접수된 날로부터 90일 이내에 신청인에게 문서로 통보하여야 한다. 다만, 제6조제2항에 따라 현지실사를 실시하는 경우에는 그 계획이 신청인에게 통보된 날부터 현지실사 시작일까지의 기간은 처리기한에 산입하지 않는다.

③ 인증업무등 대행기관의 장은 인터넷 홈페이지에 우수 관리체계 인증을 받은 디지털의료기기제조업자들을 공개해야 한다.

제8조(이의신청) ① 우수 관리체계 인증을 신청한 자는 제6조제3항에 따른 결과에 이의가 있는 경우에는 민원처리에 관한 법률이 정하는 바에 따라 이의신청을 할 수 있다.

② 인증업무등 대행기관의 장은 제1항에 따라 이의신청을 받은 경우에는 신청 내용에 따른 처리결과를 작성하고 보관하여야 한다.

③ 인증업무등 대행기관의 장은 제1항의 이의신청을 받았을 때는 심의위원회의 심의를 거쳐 처리할 수 있다. 다만 경미한 사항에 대해서는 심의위원회의 심의를 거치지 아니할 수 있다.

제9조(인증 유효기간) ① 우수 관리체계 인증의 유효기간은 인증서 발행일로부터 3년으로 한다.

② 법 시행규칙 제31조제6항에 따라 다시 우수 관리체계 인증을 받은 경우 그 인증의 유효기간은 기존 인증의 유효기간 만료일 다음날부터 3년으로 한다. 다만, 불가피한 사유로 새로운 인증서가 기존 인증의 유효기간 만료일 이후에 발급된 경우에는 새로운 인증서 발행일로부터 3년으로 하되, 그 발급일까지 우수 관리체계 인증이 유효한 것으로 본다.

제10조(재검토 기한) 식품의약품안전처장은 「행정규제기본법」 제8조 및 「훈령 예규 등의 발령 및 관리에 관한 규정」에 따라 2025년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

이 고시는 고시한 날부터 시행한다.

[별표 1]

우수 관리체계 인증 기준

1. 적용범위

1.1 적용 영역

가. 이 기준은 조직이 보유하고 있는 디지털의료기기소프트웨어(이하 "소프트웨어") 품질관리 분야 관리체계 역량에 대한 인증 기준이다.

1.2 적용 기준 항목

2. 일반사항, 3. 품질관리, 4. 안전관리, 5. 전자적 침해행위 예방 및 대응체계, 6. AI/ML 제어 조치 절의 기준 항목에 대하여 인증을 심사한다.

2. 일반사항

가. 조직은 3, 4, 5, 6절의 기준 항목 요구 활동들에 대하여 각 활동을 위한 프로세스, 실행 기록, 프로세스 산출물을 문서화하고 이를 통하여 각 활동을 수행할 수 있는 역량을 갖추었음을 입증하여야 한다.

3. 품질관리

3.1 품질관리시스템

3.1.1 소프트웨어 품질관리시스템

가. 소프트웨어 품질관리시스템(이하 "품질관리시스템")은 다음 요소들을 포함하여야 한다.

1) 디지털의료기기소프트웨어에 요구되는 안전성, 유효성, 성능의 만족을 보장하기 위하여 필요한 리더십, 경영 책임과 권한, 자원을 제공할 수 있는 조직 구조

2) 소프트웨어의 기획, 개발 및 유지보수를 위해 정의된 소프트웨어

수명주기 프로세스 그룹(이하 "소프트웨어 실현 및 사용 프로세스 그룹")

3) 모든 소프트웨어 실현 및 사용 프로세스들이 공통적으로 필요한 지원 기능을 수행하는 소프트웨어 수명주기 프로세스 그룹(이하 "소프트웨어 수명주기 지원 프로세스 그룹")

4) 소프트웨어 실현 및 사용 프로세스 그룹은 다음 업무에 대한 하위 그룹을 가지며, 한 개 이상의 프로세스를 포함

가) 요구사항 분석

나) 설계

다) 구현

라) 검증(Verification) & 밸리데이션(Validation)

마) 배포

바) 유지보수

5) 소프트웨어 수명주기 지원 프로세스 그룹은 다음 업무에 대한 하위 그룹을 가지며, 한 개 이상의 프로세스를 포함

가) 제품 계획

나) 위험관리

다) 문서 및 기록 관리

라) 형상관리

마) 측정, 분석 및 개선 관리

바) 아웃소싱(Outsourcing) 관리

3.1.2 프로세스

가. 조직의 규모 및 수행하는 역할을 고려하여 품질관리시스템에 필요한 프로세스를 정의하고 해당 업무에 프로세스를 적용하여야 한다.

나. 조직이 정의하는 프로세스는 다음 내용을 포함하여야 한다.

1) 해당되는 경우, 프로세스 입력 이전에 수행된 프로세스의 산출물, 품질관리시스템 내의 문서관리시스템에 기록된 기타 자료 등 프로세

스 입력 사항

2) 프로세스 내 활동 수행 절차

3) 수행된 프로세스의 산출물 등 프로세스 출력 사항

다. 품질관리시스템을 위하여 정의된 모든 프로세스와 실행 기록 및 산출물은 문서화되어야 한다.

라. 조직이 제품의 적합성 요구사항에 영향을 미치는 어떠한 프로세스를 위탁하는 경우, 조직은 이러한 프로세스가 모니터링되고 관리됨을 보장하도록 하여야 하며 이를 문서화하여야 한다.

3.1.3 경영책임

3.1.3.1 경영의지

최고 경영자는 품질관리시스템의 개발 및 실행, 그리고 품질관리시스템의 효과성을 유지하기 위한 의지의 증거를 다음을 통하여 제시하여야 한다.

- 1) 적용되는 법적 요구사항 뿐만 아니라 고객 요구사항 충족의 중요성에 대한 내부 의사소통
- 2) 품질방침 수립
- 3) 품질목표 수립을 보장
- 4) 경영검토 수행
- 5) 자원의 이용 가능성을 보장

3.1.3.2 고객중심

최고 경영자는 품질관리시스템이 고객 요구사항과 적용되는 법적 요구사항이 결정되고 충족됨을 보장하여야 한다.

3.1.3.3 품질방침

최고 경영자는 품질관리시스템의 품질방침이 다음과 같음을 보장하여야 한다.

- 1) 조직의 목적에 적절할 것
- 2) 요구사항을 준수하고 품질관리시스템의 효과성을 유지하려는 의지를 포

함할 것

- 3) 품질목표를 수립하고 검토하기 위한 틀을 제공할 것
- 4) 조직 내에서 의사소통이 이루어지고 이해될 것
- 5) 지속적인 적절성을 위하여 검토될 것

3.1.3.4 품질목표

가. 최고 경영자는 품질관리시스템 품질목표가 적용되는 법적 요구사항과 제품에 대한 요구사항을 충족시키는데 필요한 사항을 포함하고, 조직 내의 관련 기능 및 계층에서 수립됨을 보장하여야 한다.

나. 품질관리시스템 품질목표는 측정 가능하여야 하고 품질 방침과 일관성이 있어야 한다.

3.1.4 책임, 권한 및 의사소통

3.1.4.1 책임과 권한

가. 최고 경영자는 조직 내에서 품질관리시스템에 대한 책임과 권한이 규정되고, 문서화되어 의사소통됨을 보장하여야 한다.

나. 최고 경영자는 소프트웨어 품질에 영향을 미치는 업무를 관리, 수행 및 검증하는 모든 인원의 상호관계를 문서화하고, 이러한 업무를 수행하는데 필요한 권한과 독립성을 보장하여야 한다.

3.1.4.2 품질책임자

가. 최고 경영자는 다른 책임과 무관하게 다음 사항을 포함하는 책임과 권한을 갖는 사람을 조직의 구성원 중에서 선임하여야 한다.

- 1) 품질관리시스템에 필요한 프로세스가 문서화됨을 보장
- 2) 최고 경영진에게 품질관리시스템의 효과성 및 개선의 필요성에 대해 보고
- 3) 조직 전반에 걸쳐 적용되는 법적 요구사항과 품질관리시스템 요구사항에 대한 인식의 증진을 보장

나. 최고 경영자는 품질책임자의 자격은 「의료기기법 시행규칙」 제11조(품질책임자 자격 등) 제2항에 명시된 자격과 부합하는지 검토해야 한다.

3.1.4.3 내부 의사소통

최고 경영자는 조직 내에서 품질관리시스템에 대한 적절한 의사소통 프로세스가 수립되고, 품질관리시스템 효과성에 대하여 의사소통이 이루어지고 있음을 보장하여야 한다.

3.1.5 경영검토

가. 조직은 품질관리시스템 경영검토에 대한 절차를 문서화하여야 한다.
나. 최고 경영자는 문서화된 계획된 주기로 품질관리시스템을 검토하여, 품질관리시스템의 지속적인 적합성, 적절성 및 효과성을 보장하여야 한다.

다. 경영검토에서는 품질방침 및 품질목표를 포함하여 품질관리시스템의 변경 필요성 및 개선 가능성에 대한 평가가 이루어져야 한다.

라. 경영검토에 관한 기록은 문서화되어 유지하여야 한다.

3.1.6 자원의 확보

가. 조직은 다음에 필요한 자원을 결정하고 확보하여야 한다.

- 1) 품질관리시스템의 실행 및 그 효과성 유지
- 2) 적용되는 법적 요구사항 및 고객 요구사항의 충족

3.1.7 인적자원

가. 소프트웨어 제품 품질에 영향을 미치는 업무를 수행하는 인원은 적절한 교육, 훈련, 숙련도 및 경험을 바탕으로 능력을 갖추어야 한다.

나. 조직은 품질관리시스템 운영에 필요한 인원이 갖추어야 할 역량을 확립하고, 인원에게 필요한 훈련을 제공하며, 인원의 인식을 보장하기 위한 프로세스를 문서화하여야 한다.

다. 조직은 소프트웨어 품질관리시스템 운영에 필요한 다음의 사항들을 실행하여야 한다.

- 1) 제품 품질에 영향을 미치는 업무를 수행하는 인원에게 필요한 역량을 결정
- 2) 필요한 역량을 갖추거나 유지하기 위해 훈련을 제공하거나 그 밖의

조치 실시

3) 취해진 조치의 효과성 평가

4) 조직의 인원들이 자신의 활동에 대한 관련성 및 중요성을 인식하고 있으며, 이들이 어떻게 품질목표의 달성에 기여하는지 인식함을 보장

5) 학력, 교육, 훈련, 숙련도 및 경험에 대한 적절한 기록을 유지

3.1.8 기반시설

가. 조직은 품질관리시스템 운영에 필요한 제품 요구사항에 대한 적합성을 확보하고 제품의 혼입을 방지하며 순차적인 취급을 보장하기 위해, 필요한 기반시설에 대한 요구사항을 문서화하여야 한다. 해당되는 경우, 기반시설은 다음을 포함한다.

1) 건물, 작업 공간 및 관련된 부대시설

2) 프로세스 장비(하드웨어 및 소프트웨어)

3) 운송, 통신 또는 정보시스템 등 지원 서비스

나. 조직은 기반시설의 유지보수 활동 또는 이러한 활동의 부족으로 인하여 제품 품질에 영향을 미칠 수 있는 경우, 주기를 포함하여 유지보수 활동에 대한 요구사항을 문서화하여야 한다. 해당되는 경우, 요구사항은 제조, 작업환경관리 그리고 모니터링 및 측정에 사용된 설비에 적용하여야 한다.

다. 이러한 유지보수 활동 기록은 보관하여야 한다.

3.1.9 작업환경

가. 조직은 품질관리시스템 운영에 필요한 제품 요구사항에 대한 적합성을 확보하는데 필요한 작업환경의 요구사항을 문서화하여야 한다.

나. 만일 작업환경조건이 제품 품질에 부정적인 영향을 미칠 수 있는 경우, 작업환경에 대한 요구 사항과 환경조건을 모니터링하고 관리하기 위한 절차를 문서화하여야 한다.

다. 조직은 품질관리시스템 운영에 필요한 다음 요구사항을 수행하여야 한다.

- 1) 작업원의 건강, 청결 및 복장에 대한 요구사항 정의 및 문서화(작업원이 제품 또는 작업환경과 접촉하여 소프트웨어의 안전성 및 성능에 영향을 미칠 수 있는 경우)
- 2) 특별한 환경조건에서 임시로 작업하는 모든 인원은 역량을 갖추고 있거나, 역량을 갖춘 인원에 의해 감독되도록 보장

3.2 소프트웨어

3.2.1 프로젝트

3.2.1.1 프로젝트 계획

가. 조직은 프로젝트 목표에 따라 작업 범위를 결정하고 주어진 예산과 일정에 맞춰 프로젝트를 수행하기 위한 단계별 활동에 대한 전략 및 성공적 프로젝트 수행을 위한 관리 계획을 수립하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 프로젝트의 목표 및 접근 방식 식별
- 2) 프로젝트의 제약사항 식별
- 3) 프로젝트의 규모 및 작업 범위 결정
- 4) 프로젝트에 적용할 수명주기 모델과 이를 구성하는 주요 프로세스 정의
- 5) 프로젝트에 필요한 인프라와 자원 식별 및 목록화
- 6) 공수와 비용을 산정하고, 근거 기록
- 7) 일정과 예산을 결정하고, 근거 기록
- 8) 프로젝트 계획 수립
- 9) 프로젝트 계획서를 작성하고, 이해관계자의 승인 획득

3.2.1.2 프로젝트 통제

가. 프로젝트 계획서를 기반으로 프로젝트 진척 사항을 모니터링하고 문제 발생에 대한 시정조치를 통해 프로젝트 진행을 관리하고 통제하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 담당 팀 또는 개인을 지정하여 작업 할당
- 2) 프로젝트 계획서를 기반으로, 계획 대비 진척도 모니터링 및 기록
- 3) 주요 프로세스별 산출물 검토
- 4) 발견되거나, 보고된 문제를 문제해결 프로세스로 이관

3.2.1.3 문제 분석 및 시정조치

가. 발생한 문제들을 분석하여 시정조치 방안을 선정하고 수행하며, 그 결과를 프로세스 개선에 반영하여 품질목표를 달성하기 위한 성과 관리 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 문제 분석 범위 및 우선순위 결정
- 2) 문제 분석 및 시정조치 가이드라인을 작성하고, 이해관계자의 승인 획득
- 3) 모니터링 중 발견된 문제 또는 보고된 문제를 해결하기 위한 책임 할당
- 4) 모니터링 중 발견된 문제 또는 보고된 문제에 대한 원인 및 인과관계, 종속성 등을 분석
- 5) 모니터링 중 발견된 문제 또는 보고된 문제에 대한 해결 방안 도출
- 6) 도출한 해결 방안이 미치는 영향을 평가한다.
- 7) 도출한 해결 방안을 반영하여, 기한 내 시정조치 활동 수행
- 8) 문제 및 시정조치 내용 기록 및 관리

3.2.1.4 협력 업체 관리

가. 프로젝트에 참여하는 협력 업체의 선정 및 계약 체결과 이행에 관한 확인 및 관리를 수행하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 협력 업체의 업무 범위 및 접근 권한 결정
- 2) 협력 업체 선정
- 3) 협력 업체와 보안 서약을 포함한 계약 체결
- 4) 협력 업체의 계약 이행 여부 확인

5) 제품 및 서비스 검수

3.2.2 소프트웨어 개발

3.2.2.1 분석 프로세스

가. 고객의 요구사항, 기대사항 등을 파악하여 조직과 고객 간의 공통적인 이해관계를 형성하고, 개발 과정 동안 변경되는 요구사항을 추적 및 관리하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 고객 요구사항 확인
- 2) 고객 요구사항에 대한 수용 기준 결정
- 3) 고객 요구사항을 기반으로 계약 조건 협의
- 4) 고객 요구사항에 대한 변경 관리
- 5) 고객 요구사항과 산출물 간 양방향 추적성 유지
- 6) 해당되는 경우, 분석 프로세스 개선 활동 수행

3.2.2.2 설계 프로세스

가. 고객 요구사항을 바탕으로 소프트웨어 개발에 필요한 하위 수준의 요구사항을 식별하고 상세화하며, 이를 검토하여 정확한 소프트웨어를 개발하기 위해 요구사항을 분석하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 고객 요구사항을 기술 용어로 변환
- 2) 소프트웨어 요구사항 분석 및 검토
- 3) 소프트웨어 요구사항 명세서를 작성하고, 이해관계자의 승인 획득
- 4) 소프트웨어 요구사항과 산출물 간 양방향 추적성 유지
- 5) 소프트웨어 요구사항의 출처를 관리하고, 추적성 불일치 문제를 문제해결 프로세스로 이관
- 6) 해당되는 경우, 설계 프로세스 개선 활동 수행

나. 설계 프로세스에서 식별된 요구사항을 바탕으로 소프트웨어에 대한 단위 및 상세 설계 등 개발 프로세스를 위한 준비적인 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 소프트웨어 모듈화, 설계 절차 및 방법 등을 포함하여, 단위 설계 계획 수립
- 2) 소프트웨어 모듈 내부 알고리즘 및 데이터 명세화, 설계 절차 및 방법 등을 포함한 상세 설계 계획 수립
- 3) 소프트웨어 설계 명세서를 작성하고, 이해관계자의 승인 획득
- 4) 소프트웨어 요구사항과 설계 항목 간 양방향 추적성 유지
- 5) 추적성 불일치 문제를 문제해결 프로세스로 이관
- 6) 해당되는 경우, 설계 프로세스 개선 활동 수행

다. 소프트웨어 설계 명세서의 단위 설계 내용을 바탕으로 단위 테스트 계획을 수립하여 구현 프로세스를 준비하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 소프트웨어 단위 테스트 계획 수립
- 2) 소프트웨어 테스트 계획서를 작성하고, 이해관계자의 승인 획득
- 3) 소프트웨어 단위별 테스트케이스를 작성하고, 요구사항과의 양방향 추적성 유지
- 4) 추적성 불일치 문제를 문제해결 프로세스로 이관
- 5) 해당되는 경우, 설계 프로세스 개선 활동 수행

3.2.2.3 구현 프로세스

가. 소프트웨어 설계 명세서 상 단위 설계 내용을 바탕으로 소프트웨어를 단위별로 구현하고, 요구사항 반영 여부를 확인한 후 이를 통합하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 소프트웨어 단위 구현
- 2) 소프트웨어 단위 테스트 수행
- 3) 동료 검토를 통해, 발견된 결함에 대한 위험도, 영향 등을 분석하여 개선 여부 및 우선순위 결정
- 4) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 5) 각 담당자가 배포된 개선 사항 적용

6) 배포 과정에서의 문제를 문제해결 프로세스로 이관

7) 소프트웨어 통합

8) 해당되는 경우, 구현 프로세스 개선 활동 수행

3.2.2.4 시험 프로세스

가. 소프트웨어 설계 명세서 상 상세 설계 내용을 바탕으로 통합 및 시스템 테스트를 수행하고, 요구사항 반영 여부를 확인하는 활동으로 다음 내용을 포함하고 있어야 한다.

1) 소프트웨어 테스트케이스를 작성하고, 요구사항과의 양방향 추적성 유지

2) 소프트웨어 통합 테스트 수행

3) 동료 검토를 통해, 발견된 결함에 대한 위험도, 영향 등을 분석하여 개선 여부 및 우선순위 결정

4) 이해관계자의 승인을 획득한 후, 개선 사항 배포

5) 각 담당자가 배포된 개선 사항 적용

6) 배포 과정에서의 문제를 문제해결 프로세스로 이관

7) 소프트웨어 시스템 테스트 수행

8) 동료 검토를 통해, 발견된 결함에 대한 위험도, 영향 등을 분석하여 개선 여부 및 우선순위 결정

9) 이해관계자의 승인을 획득한 후, 개선 사항 배포

10) 각 담당자가 배포된 개선 사항 적용

11) 배포 과정에서의 문제를 문제해결 프로세스로 이관

12) 해당되는 경우, 시험 프로세스 개선 활동 수행

3.2.2.5 배포 프로세스

가. 소프트웨어 인수 테스트를 수행하여 최종적으로 소프트웨어가 주어진 환경에서 제대로 동작하는지 확인한 후, 고객 요구사항이 만족하는 소프트웨어를 제공하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 소프트웨어 인수 테스트 수행
- 2) 소프트웨어 테스트 결과서를 이해관계자에게 공유
- 3) 고객의 의사결정에 따라 개선 여부 또는 기능 확정
- 4) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 5) 각 담당자가 배포된 개선 사항 적용
- 6) 배포 과정에서의 문제를 문제해결 프로세스로 이관
- 7) 조직은 고객사에 소프트웨어를 인도
- 8) 해당되는 경우, 배포 프로세스 개선 활동 수행

3.2.2.6 유지보수 프로세스

가. 의도된 용도에 따라 시판 후 소프트웨어를 모니터링하고, 피드백을 수집 및 관리하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 의도된 용도에 따라 시판 후 소프트웨어에 대한 피드백 모니터링
- 2) 시판 후 소프트웨어에 대한 피드백 기록 및 관리
- 3) 해당되는 경우, 피드백을 문제해결 프로세스로 이관
- 4) 유지보수 관련 보고 매커니즘 이행

나. 조직이 피드백을 통해 시판 후 소프트웨어에 대한 개선 요구를 식별하고, 식별된 개선 요청에 대한 분석 및 피드백 반영 활동을 시행하며, 활동의 결과를 기록 및 관리하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 피드백 반영 계획 수립
- 2) 소프트웨어 개선 계획서를 작성하고, 이해관계자의 승인 획득
- 3) 피드백 반영에 대한 위험도, 영향도를 분석하여 우선순위 결정
- 4) 피드백 반영에 대한 내부 테스트 수행
- 5) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 6) 관련 담당자는 배포된 개선 사항 적용
- 7) 피드백 반영 활동 기록 및 관리
- 8) 피드백을 반영한 소프트웨어 재배포

9) 유지보수 관련 보고 매커니즘 이행

다. 조직이 피드백 반영 후, 소프트웨어 재배포에 대해 사용자 및 규제 기관에 보고하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

1) 배포한 소프트웨어에 존재하는 모든 문제와 변경하지 않고 계속해서 사용했을 때의 결과

2) 배포한 소프트웨어의 가능한 모든 변경과 그러한 변경 사항을 입수 및 설치하는 방법

3.2.3 소프트웨어 지원

3.2.3.1 품질 보증 체계

가. 프로젝트 전 과정의 활동이 정의된 프로세스와 적합성을 유지하고 있는지와 산출물이 요구사항을 만족시키고 있는지에 대해 확인하여 프로젝트를 관리하는 활동으로 다음 내용을 포함하고 있어야 한다.

1) 품질 보증 영역 식별

2) 품질 보증에 대한 평가 방식 및 계획 수립

3) 필요에 따라 과거 품질 데이터를 품질 보증 접근 방식 및 계획에 반영

4) 품질 보증 계획서를 작성하고, 이해관계자의 승인 획득

5) 품질 보증 계획서를 기반으로 평가에 대한 베이스라인 설정 및 통제

6) 품질 및 규정 위반에 대한 문제 보고

7) 품질 보증 활동 기록 및 관리

8) 주기적으로 품질 보증 활동의 감사를 시행하여 개선 기회 식별

9) 해당되는 경우, 품질 보증 체계 개선

3.2.3.2 형상 관리 체계

가. 프로젝트 수명주기 동안 개발되는 작업산출물에 대한 베이스라인을 수립하고 작업산출물의 변경을 주요 단계별로 추적하고 통제하여

관리하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 형상 항목 식별 및 고유 식별자 할당
- 2) 형상 관리 계획 수립
- 3) 형상 관리 계획서를 작성하고, 이해관계자의 승인 획득
- 4) 형상 관리 계획서를 기반으로 형상 항목에 대한 베이스라인 설정 및 통제
- 5) 형상 변경 요청에 대한 영향도를 분석하여 우선순위 결정
- 6) 형상 변경 요청에 대한 검토 및 테스트 수행
- 7) 이해관계자의 승인을 획득한 후, 변경 사항 배포
- 8) 형상 관리 활동 기록 및 관리
- 9) 주기적으로 형상 감사(무결성 유지, 추적성 확보 등) 실시
- 10) 해당되는 경우, 형상 관리 체계 개선

3.2.3.3 자원 관리 체계

가. 프로젝트에서 사용되는 자원에 대한 계획을 수립하고, 자원을 통제 및 관리하는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 자원 식별 및 고유 식별자 할당
- 2) 자원 관리 계획 수립
- 3) 자원 관리 계획서를 작성하고, 이해관계자의 승인 획득
- 4) 자원 관리 계획서를 기반으로 자원 구매, 사용 및 폐기 통제
- 5) 프로젝트별 규모 및 가용성 요구에 따라 필요한 자원 검토 및 제공
- 6) 제공된 자원에 대한 담당자 배정
- 7) 자원 관리 작업 기록 및 관리
- 8) 프로젝트 종료에 따른 자원 회수 시행
- 9) 주기적으로 자원 감사 실시
- 10) 해당되는 경우, 자원 관리 체계 개선

3.2.4 프로세스 관리

3.2.4.1 표준 프로세스 관리

가. 조직의 표준 프로세스의 요구 및 목표를 식별하여 가이드라인을 수립하고 확산하며, 향후 조직 표준 프로세스 개선에 활용하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 조직의 표준 프로세스에 대한 요구 및 목표 식별
- 2) 표준 프로세스의 잠재적 위험 분석
- 3) 표준 프로세스 관리 가이드라인 수립
- 4) 표준 프로세스 관리 가이드라인을 작성하고, 이해관계자의 승인 획득
- 5) 프로세스별 담당자 배정
- 6) 프로세스별 담당자에게 역할 및 책임 할당
- 7) 표준 프로세스 관리 가이드라인을 기반으로 프로세스에 대한 베이스라인 설정 및 통제
- 8) 프로세스별 주기적인 감사 수행
- 9) 프로세스 관련 보고 매커니즘 설정 및 이행

3.2.4.2 프로세스 개선 관리

가. 조직의 프로세스 개선에 관한 요구를 식별하고, 식별된 프로세스 개선 요청에 대한 분석 및 개선 활동을 시행하며, 프로세스 개선 활동의 결과를 기록 및 관리하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 프로세스 개선 계획 수립
- 2) 프로세스 개선 계획서를 작성하고, 이해관계자의 승인 획득
- 3) 프로세스 개선 요청에 대한 영향도를 분석하여 우선순위 결정
- 4) 프로세스 개선 요청에 대한 검토 수행
- 5) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 6) 프로세스별 담당자가 배포된 개선 사항 적용
- 7) 프로세스 개선 활동 기록 및 관리
- 8) 프로세스 관련 보고 매커니즘 이행

3.2.4.3 표준 작업환경 관리

가. 조직의 표준 작업환경의 요구 및 목표를 식별하여 안전·보안 가이드라인을 수립하고 확산하며, 향후 조직 표준 작업환경 개선에 활용하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 조직의 표준 작업환경에 대한 요구 및 목표 식별
- 2) 표준 작업환경의 잠재적 위험 분석
- 3) 표준 작업환경 관리 가이드라인 수립
- 4) 표준 작업환경 관리 가이드라인을 작성하고, 이해관계자의 승인 획득
- 5) 작업환경별 담당자 배정
- 6) 작업환경별 담당자에게 역할 및 책임 할당
- 7) 표준 작업환경 관리 가이드라인을 기반으로 작업환경에 대한 베이스라인 설정 및 통제
- 8) 작업환경별 현장 조사 및 설문조사를 통한 주기적인 감사 수행
- 9) 작업환경 관련 보고 매커니즘 설정 및 이행
- 10) 해당되는 경우, 작업환경에 대한 안전·보안 훈련 시행

3.2.4.4 작업환경 개선 관리

가. 조직의 작업환경 개선에 관한 요구를 식별하고, 식별된 작업환경 개선 요청에 대한 분석 및 개선 활동을 시행하며, 개선 활동의 결과를 기록 및 관리하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 작업환경 개선 계획 수립
- 2) 작업환경 개선 계획서를 작성하고, 이해관계자의 승인 획득
- 3) 작업환경 개선 요청에 대한 영향도를 분석하여 우선순위 결정
- 4) 작업환경 개선 요청에 대한 검토 수행
- 5) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 6) 작업환경별 담당자가 배포된 개선 사항 적용
- 7) 작업환경 개선 활동 기록 및 관리

8) 작업환경 관련 보고 매커니즘 이행

3.2.5 조직 관리

3.2.5.1 조직 성과 관리

가. 조직의 성과 목표를 조직 차원에서 일관되게 관리하는 것으로, 조직은 프로젝트별 성과를 주기적으로 수집하여 조직 성과 목표에 대한 달성 여부를 파악하고, 향후 문제점의 시정 및 개선 활동에 이용하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 조직의 비즈니스 목표를 기반으로 성과 목표 식별
- 2) 우선순위를 포함한 조직의 성과 관리 계획 수립
- 3) 조직 성과 관리 계획서를 작성하고, 이해관계자의 승인 획득
- 4) 조직 성과 관리 계획서를 기반으로 조직 성과를 측정할 수 있는 통계 및 기타 정량적 기법과 도구 결정
- 5) 주기적으로 프로젝트별 성과 수집
- 6) 수집된 프로젝트별 성과를 기반으로 조직의 성과 목표 측정 및 분석
- 7) 분기별 조직 성과 기록 및 관리
- 8) 조직 성과 보고 매커니즘 이행
- 9) 필요에 따라, 달성하지 못한 목표를 문제해결 프로세스로 이관

3.2.5.2 조직 성과 개선 관리

가. 조직의 성과 목표 개선에 관한 요구를 식별하고, 식별된 성과 목표 개선 요청에 대한 분석 및 개선 활동을 시행하며, 개선 활동의 결과를 기록 및 관리하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 조직 성과 목표 개선 계획 수립
- 2) 조직 성과 목표 개선 계획서를 작성하고, 이해관계자의 승인 획득
- 3) 조직 성과 목표 개선 사항의 비용, 이점, 위험도 등을 분석하여 우선순위 결정

- 4) 조직 성과 목표 개선 사항을 기반으로 성과 예측
- 5) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 6) 각 담당자가 배포된 개선 사항 적용
- 7) 조직 성과 목표 개선 활동 기록 및 관리
- 8) 조직 성과 보고 매커니즘 이행한다.

3.2.5.3 프로젝트 성과 관리

가. 조직의 성과 목표를 달성하기 위하여 프로젝트의 성과 목표를 조직 차원에서 일관되게 관리하는 것으로, 조직은 프로젝트별 성과를 주기적으로 측정 및 수집, 분석하여 프로젝트 성과 목표에 대한 달성 여부를 파악하고, 향후 문제점의 시정 및 개선 활동에 이용하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 프로젝트별 성과 목표 식별
- 2) 우선순위를 포함한 프로젝트별 성과 관리 계획 수립
- 3) 프로젝트별 성과 관리 계획서를 작성하고, 이해관계자의 승인 획득
- 4) 프로젝트 성과 관리 계획서를 기반으로 프로젝트 성과를 측정할 수 있는 통계 및 기타 정량적 기법과 도구 결정
- 5) 프로젝트 성과를 주기적으로 측정 및 수집, 분석
- 6) 분기별 프로젝트 성과 기록 및 관리
- 7) 프로젝트 성과 보고 매커니즘 이행
- 8) 해당되는 경우, 달성하지 못한 목표를 문제해결 프로세스로 이관

3.2.5.4 프로세스 성과 개선 관리

가. 프로세스 성과 목표 개선에 관한 요구를 식별하고, 식별된 성과 목표 개선 요청에 대한 분석 및 개선 활동을 시행하며, 개선 활동의 결과를 기록 및 관리하기 위한 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 프로세스 성과 목표 개선 계획 수립
- 2) 프로세스 성과 목표 개선 계획서를 작성하고, 이해관계자의 승인

획득

- 3) 프로세스 성과 목표 개선 사항의 비용, 이점, 위험도 등을 분석하여 우선순위 결정
- 4) 프로세스 성과 목표 개선 사항을 기반으로 성과 예측
- 5) 이해관계자의 승인을 획득한 후, 개선 사항 배포
- 6) 프로세스별 담당자가 배포된 개선 사항 적용
- 7) 프로세스 성과 목표 개선 활동 기록 및 관리
- 8) 프로세스 성과 보고 매커니즘 이행

3.2.5.5 조직 구성원 관리

가. 조직 목표에 맞추어 구성원의 교육 및 훈련의 수요를 식별하며 교육 계획 수립, 교육 시행 및 평가 등 구성원의 역량을 강화시키는 활동으로 다음 내용을 포함하고 있어야 한다.

- 1) 프로젝트 수행 시 필요한 기술과 현재 구성원이 보유한 지식 간의 격차 식별
- 2) 교육 및 훈련 계획 수립
- 3) 교육 및 훈련 시행
- 4) 교육 및 훈련의 효과 평가
- 5) 교육 및 훈련의 결과 기록, 관리
- 6) 해당되는 경우, 프로젝트 계획에 인력 교육 및 훈련 계획 포함

3.3 위험관리

3.3.1 위험 허용 기준

가. 최고 경영자는 위험 허용 기준을 수립하기 위한 방침을 결정하고 이를 문서화하여야 한다.

3.3.2 위험관리 프로세스

가. 최고 경영자는 위험관리 프로세스의 지속적인 효과성을 보장하기 위해 계획된 주기로 위험관리 프로세스의 적절성을 검토하여야 하며

모든 결정과 수행된 조치를 문서화하여야 한다.

3.3.3 위험관리 계획

가. 위험관리 활동을 계획하여야 하며 고려하고 있는 제품에 대해 위험관리 프로세스에 따라 위험관리 계획을 수립하고 이를 문서화하여야 한다.

나. 위험관리 계획은 다음 내용을 포함하여야 한다.

- 1) 계획된 위험관리 활동의 범위, 계획의 각 요소를 적용할 수 있는 제품과 수명 주기 단계를 식별하고 설명
- 2) 책임과 권한의 할당
- 3) 위험관리 활동의 검토에 대한 요구사항
- 4) 위해 발생 가능성을 산정할 수 없는 경우 위험을 수용하기 위한 기준을 포함하여 허용 가능 위험을 결정하기 위한 조직의 방침에 기반한 위험 허용 가능성에 대한 기준
- 5) 전체 잔여 위험을 평가하기 위한 방법 및 허용 가능한 위험을 결정하기 위한 조직의 방침에 근거한 전체 잔여 위험의 허용 가능성에 대한 기준
- 6) 위험 통제 조치의 이행 및 효과성 검증을 위한 활동
- 7) 관련 생산 및 생산 후의 정보를 수집하고 검토하는 것과 관련된 활동

4. 안전관리

4.1 소비자 정보 제공

4.1.1 소비자 정보 제공 의무

가. 조직은 제품을 사용하는 소비자에게 제품의 안전한 사용을 위해 필요한 정보를 제공하여야 하며, 다음 사항이 포함되어야 한다.

- 1) 제품 사용 방법 및 주의 사항

2) 제품의 기능 및 성능 사항

3) 예상되는 오용 사례, 부작용 등 위험 요인 사항

4) 제품 업데이트 및 유지보수 관련 사항

나. 조직은 제품의 안전한 사용을 위한 정보 제공 방법과 절차에 대한 사항을 문서화하여야 한다.

4.1.2 정보 제공 방법

가. 조직은 제품 설명서 또는 웹사이트, 모바일 애플리케이션 등의 방법을 통해 소비자에게 필요한 정보를 제공하여야 한다.

나. 정보 제공 방법이 전자적 방식으로 제공되는 경우 최신의 정보를 제공하여야 하며 변경 사항이 있을 경우 소비자에게 바로 알려야 한다.

다. 조직은 제품 사용 정보에 대해 소비자에게 제공하기 위한 방안과 그 활동 기록에 대해 문서화하여야 한다.

4.1.3 교육 및 인식 제고

가. 조직은 소비자 및 필요한 경우 의료서비스제공자를 대상으로 제품의 안전하고 효과적인 사용에 대한 교육을 제공하여야 한다.

나. 교육에 필요한 사항은 조직에서 우선적으로 정하며, 협의에 따라 교육 방식 및 주기를 정하여 교육을 진행하여야 한다.

다. 조직은 교육에 필요한 제반 사항과 교육 지원 방식에 대한 절차에 대해 문서화하여야 한다.

4.2 부작용 발생 시 대응체계

4.2.1 부작용 신고

가. 조직은 부작용으로 인해 신고된 제품에 대해 신고 방법 및 절차에 대한 사항을 제품 설명서, 홈페이지 등을 통해 명확히 안내하여야 하며 관련 절차를 문서화하여야 한다.

나. 조직은 부작용으로 의심되거나 확인되어 신고된 제품에 대해 대응

하기 위한 방안을 마련하여야 하며 관련 절차를 문서화하여야 한다.

4.2.2 부작용 모니터링 및 보고

가. 조직은 제품 부작용 신고 모니터링 체계를 구축하여야 하며 소비자로부터 접수된 부작용 신고 사항을 수집, 분석 및 평가하여야 한다.

나. 조직은 평가가 완료된 부작용에 대해 부작용 사례로 분류하고 위험 및 심각도에 따라 식품의약품안전처와 협의를 통해 그 보고 시점을 정하여야 한다.

다. 조직은 부작용 모니터링 및 보고를 위한 절차와 그 활동 기록에 대해 문서화하여야 한다.

4.2.3 부작용 대응 및 조치

가. 조직은 부작용 발생 시, 정해진 절차에 따라 즉각적인 대응 조치를 취해야 하며 제품의 수정, 보완 및 회수 등의 조치를 신속히 수행하여야 한다.

나. 조직은 제품에서 매우 심각한 부작용이 발생된 경우 사용을 즉각 중지하여야 하며, 정해진 절차에 따라 회수 및 폐기를 즉시 시행하여야 한다.

다. 조직은 제품의 부작용 발생 시 대응 및 조치 방안 등의 절차와 그 활동 기록에 대해 문서화하여야 한다.

4.2.4 사후 관리 및 개선

가. 조직은 부작용 발생 이력 및 대응 조치에 대해 문서화하고 식품의약품안전처에서 요구하는 경우 이를 제출하여야 한다.

나. 조직은 수집된 부작용에 대한 분석을 통해 원인, 개선 사항 조치, 조치 결과 등에 대해 문서화하여야 하며, 개선 조치가 완료된 경우 이에 대한 결과에 대해 투명하게 공개하여야 한다.

5. 전자적 침해행위의 예방 및 대응체계

5.1 일반 사항

가. 조직은 소프트웨어 품질관리시스템 내 소프트웨어 수명 전 주기에 걸쳐 전자적 침해행위를 예방 및 대응하기 위한 체계를 구축하여야 하며 체계별 활동에 대해서는 「전자적 침해행위 보안지침」에 명시된 지침을 준수하여야 한다.

나. 조직은 품질책임자 또는 별도의 보안 업무를 수행하는 자를 보안 업무 담당자로 지정하며, 보안 업무 수행에 필요한 자격 및 역량 등을 확인하는데 필요한 자격 조건 등을 문서화하여야 한다.

다. 보안 업무를 담당하는 자는 다음과 같은 활동들을 수행하여야 한다.

- 1) 물리적·기술적·관리적 보안 체계 수립
- 2) 전자적 침해행위 대응
- 3) 위험관리, 개발 및 검증, 레거시 관리 등 보안 활동
- 4) 침해사고 대응 및 취약점 감시

5.2 보안 체계 수립

가. 조직은 제품과 그 운영 환경에서의 설치 및 운용 환경, 네트워크, 제품 관련 장비 및 자료 보호 등을 위한 물리적 보안 구성을 고려하여야 하며, 제품이 운용되는 물리적 보안 환경 분석 및 각종 물리적 위협으로부터 보호할 수 있는 대책을 마련하여야 한다.

나. 조직은 제품이 운용되는 기술적 보안 환경을 분석하고 각종 기술적 위협으로부터 보호할 수 있는 대책을 마련하여야 한다.

다. 조직은 물리적·기술적 관리 체계 구성에 필요한 인원 및 활동 등에 대한 전반적 사항에 대해 조직화하고 이를 문서화하여야 한다.

라. 조직은 보안 전자적 침해행위 발생 시, 전자적 침해행위 발생 여부, 보안 점검 결과, 취약점 분석 결과 등이 포함된 보안 정책 중점 사항에 대해 점검 보고서를 작성하여야 한다.

5.3 전자적 침해행위 대응

가. 조직은 「전자적 침해행위 보안지침」 제4조 및 제5조, 제7조 내지 제12조에 대한 보안을 강구하고 방안을 마련하여야 한다.

나. 조직은 보안을 강구하기 위해 해당되는 경우 각 고려사항에 대해 유효성 확보 계획과 확보 결과에 대해 문서화하여야 한다.

5.4 보안 활동

5.4.1 위험관리 활동

가. 조직은 다음과 같은 사항을 포함하여 제품 개발 전주기에 걸쳐 위험관리 활동을 수행하여야 한다.

- 1) 제품 수명 주기 전반적인 위협 모델링
- 2) 위협 및 취약점에 대한 식별 및 위협 평가
- 3) 보안 위협 완화를 위한 위협 통제 조치 설계, 구현 및 검증
- 4) 잔여 위협 평가 및 평가 보고서 작성
- 5) 시판 후 위협 및 취약점 모니터링

나. 조직은 위험관리 활동에 대해 절차를 문서화하여야 한다.

5.4.2 개발 및 검증 활동

가. 조직은 보안 코딩, 보안 설계 및 보안 테스트 등을 고려하여 제품을 개발 및 검증하여야 하고 검증 결과를 문서화하여야 한다.

나. 조직은 검증 활동에 사용하는 테스트 도구에 대해 유효성을 확인하여야 하며 확인 결과를 문서화하여야 한다.

5.4.3 레거시 관리 활동

가. 조직은 제품을 개발하는 과정에서 지원 종료 이후의 보안 위협을 최소화하도록 제품을 설계 및 구현하여야 한다.

나. 조직은 제품 수명 종료 단계 내에서 위협 및 취약점이 발견되는 경우 이를 해결하기 위한 방안을 다음과 같이 마련하여야 한다.

1) 위험 식별, 분석, 평가 등 위험 관리 방안

2) 제품 또는 컴포넌트 패치

3) 제품 보안 문서

다. 조직은 제품의 지원 종료 단계에 진입한 이후 안전한 제품 사용을 위한 계획을 수립하고 이를 문서화하여야 한다.

5.4.4 소프트웨어 구성 요소 명세서 관리 활동

가. 조직은 제품에 대해 소프트웨어 구성 요소 명세서 작성을 위한 절차와 실행 계획, 실행 결과 등에 대해 문서화하여야 한다.

나. 조직은 소프트웨어 구성 요소 명세서 정보에 대해 보안 조치 등을 강구하여야 하며 이를 적용하여야 한다.

5.5 전자적 침해행위 대응 및 취약점 감시

5.5.1 전자적 침해행위 대응

가. 조직은 해킹, DDoS 공격 등 전자적 침해행위가 발생하는 것을 고려하여 이를 대응하기 위한 계획을 수립하여야 한다.

나. 조직은 대응 계획에 대해 다음과 같은 항목을 포함하여야 한다.

1) 침해행위 신고 방안

2) 침해행위 조치 방안

3) 침해행위 식별, 분석, 평가 등 위험 관리 방안

4) 침해사고 대응 팀 구성

5) 제품 사용의 연속성을 보장하기 위한 계획

6) 침해행위 대응을 위한 테스트 및 훈련 방안

다. 조직은 침해사고 대응을 위해 필요한 관련 보안 교육에 대해 파악하여야 하며, 관련 업무를 수행하는 자는 해당 교육을 이수하여야 한다.

라. 조직은 교육 계획, 이수 등의 교육 관리에 대해 문서화하여야 한다.

마. 조직은 침해사고 대응 계획, 신고 및 조치 절차에 대해 문서화하

여야 한다.

바. 조직은 침해행위가 발생한 경우 발생한 원인과 분석, 조치, 재발 방지 대책 등 조치에 대해 기록하기 위한 절차를 문서화하여야 한다.

5.5.2 취약점 감시

가. 조직은 제품의 취약점 감시를 위한 정기적 보안 모니터링, 로그 분석 등의 감시 활동을 계획하고 감시, 공개 및 조치 결과에 대해 문서화하여야 한다.

나. 조직은 취약점이 발견되어 보고할 경우 취약점에 대한 상세 내용, 심각도, 영향, 대응 방안 등 조치에 대해 기록하기 위한 절차를 문서화하여야 한다.

다. 조직은 취약점 공개 및 조치에 대한 절차에 대해 문서화하여야 한다.

6. AI/ML 제어 조치

6.1 일반사항

가. 조직은 AI/ML 소프트웨어 시스템의 품질관리를 위하여 다음과 같은 제어 조치 들을 정의하고 조직 전반에 해당 조치를 적용하여야 한다.

- 1) 경영진 참여, 정책 수립 및 적용 등 경영책임
- 2) 운영 필요 인력 확보, 교육·훈련 제공 등 자원 관리
- 3) AI/ML 소프트웨어의 잠재적인 위험 식별, 평가, 완화 등 위험관리
- 4) 책임, 의사결정 및 승인 절차 등 거버넌스 체계
- 5) 학습용 데이터 품질 관리, 데이터 비식별화 조치 등 데이터 처리
- 6) 인공지능 모델 설계 및 구현
- 7) 학습용 데이터 및 인공지능 모델을 결합한 AI/ML 소프트웨어 시스템 개발
- 8) AI/ML 소프트웨어의 주기적인 정확도 확인 등 운영 및 모니터링

나. 조직이 정의하는 AI 제어 조치는 다음 내용을 포함하여야 한다.

- 1) 해당되는 경우, 프로세스 입력 이전에 수행된 프로세스의 산출물, 품질관리시스템 내의 문서관리시스템에 기록된 기타 자료 등 프로세스 입력 사항
- 2) 프로세스 내 활동 수행 절차
- 3) 수행된 프로세스의 산출물 등 프로세스 출력 사항

다. AI/ML 제어 조치들은 기존 품질관리시스템의 소프트웨어 수명주기 프로세스 내 활동 또는 독립적인 소프트웨어 수명 주기 프로세스로 정의되어 문서화하여야 한다.

라. AI/ML 제어 조치의 실행 및 산출물은 기록되어야 한다.

6.2 경영책임

가. 최고 경영자는 AI 제어 조치의 개발 및 실행, 그리고 AI 제어 조치의 효과성을 유지하기 위한 의지의 증거를 다음을 통하여 제시하여야 한다.

- 1) AI 방침(AI Policy) 수립
- 2) AI 목표(AI Objective) 수립
- 3) 검토 수행

나. 최고 경영자는 AI 방침이 다음과 같음을 보장하여야 한다.

- 1) 조직의 목적에 적절할 것
- 2) 요구사항을 준수하고 AI/ML 소프트웨어 시스템의 효과성을 유지하려는 의지를 포함할 것
- 3) AI 목표를 수립하고 검토하기 위한 기반을 제공할 것
- 4) 조직 내에서 의사소통이 이루어질 것
- 5) 지속적인 적절성을 위하여 검토될 것

다. 최고 경영자는 AI 목표가 적용되는 법적 요구사항과 제품에 대한 요구사항을 충족시키는데 필요한 사항을 포함하고, 조직 내의 관련 기능 및 계층에서 수립됨을 보장하여야 한다.

라. AI 목표는 측정 가능하여야하고 품질방침과 일관성이 있어야 한다.

마. 경영검토

- 1) 조직은 AI 제어 조치 경영검토에 대한 절차를 문서화하여야 한다.
- 2) 최고 경영자는 문서화된 계획된 주기로 AI 제어 조치를 검토하여, AI 제어 조치의 지속적인 적합성, 적절성 및 효과성을 보장하여야 한다.
- 3) 경영검토에서는 AI 방침 및 AI 목표를 포함하여 AI 제어 조치의 변경 필요성 및 개선 가능성에 대한 평가가 이루어져야 한다.
- 4) 경영검토에 관한 기록은 문서화 되어 유지하여야 한다.

6.3 자원 관리

가. 조직은 다음에 필요한 자원을 결정하고 확보하여야 한다.

- 1) AI 제어 조치의 실행 및 그 효과성 유지
- 2) 적용되는 법적 요구사항 및 고객 요구사항의 충족

나. AI 제어 조치 업무를 수행하는 인원은 적절한 교육, 훈련, 숙련도 및 경험을 바탕으로 능력을 갖추어야 한다.

다. 조직은 AI 제어 조치 운영에 필요한 인원이 갖추어야 할 역량을 확립하고, 인원에게 필요한 훈련을 제공하며, 인원의 인식을 보장하기 위한 프로세스를 문서화하여야 한다.

라. 조직은 AI 제어 조치 운영에 필요한 다음의 사항들을 실행하여야 한다.

- 1) 제품 품질에 영향을 미치는 업무를 수행하는 인원에게 필요한 역량을 결정
- 2) 필요한 역량을 갖추거나 유지하기 위해 훈련을 제공하거나 그 밖의 조치 실시
- 3) 취해진 조치의 효과성 평가
- 4) 조직의 인원들이 자신의 활동에 대한 관련성 및 중요성을 인식하고 있으며, 이들이 어떻게 품질목표의 달성에 기여하는지 인식함을 보장

5) 교육, 훈련, 숙련도 및 경험에 대한 적절한 기록을 유지

6.4 위험관리

가. AI/ML 소프트웨어 시스템에 대한 위험관리 계획을 세우고 이를 실행하여야 한다.

나. AI/ML 소프트웨어 시스템에 대한 위험관리는 본 기준 3.3호의 요구사항을 만족하여야 한다.

6.5 거버넌스 체계

가. 조직은 내부적으로 이행해야 할 윤리 원칙 및 규정을 다음과 같이 수립하여야 한다.

- 1) 의료 인공지능 관련 법, 규제, 정책, 표준 및 지침을 채택·정리하여 내부적으로 이행해야 할 지침 및 규정을 수립
- 2) 인공지능 시스템 생명주기에 따른 조직의 역할과 책임을 명확하게 문서화

나. 조직은 조직의 규모 및 AI/ML 시스템에 적합한 인공지능 거버넌스 체계를 구축하여야 한다.

- 1) 조직의 윤리 원칙 및 규정을 실행할 수 있도록 관리하는 조직 구성
- 2) 해당되는 경우, 외부 전문가(예 : 의사, 간호사 등 의료인, 데이터 과학자, 임상, 품질 및 관련 교수진 등)를 포함하는 조직 구성

다. 조직은 인공지능 거버넌스 체계의 올바른 이행을 위해 다음과 같은 항목을 관리 및 감독하여야 한다.

- 1) 내부적으로 이행해야 할 윤리 원칙 및 규정 준수 여부
- 2) AI/ML 시스템의 목표 성능 모니터링
- 3) AI/ML 시스템의 폐기 의사 결정
- 4) 인공지능 거버넌스 체계 이행 기록 문서화

6.6 신뢰성 확보 계획

조직은 AI/ML 시스템 출력 결과의 불확실성을 줄이기 위해 해당되는 경우, 다음과 같이 필요한 활동을 강구하여야 한다.

가. 시뮬레이터 등을 통한 가상 시험 환경 구축

나. AI/ML 시스템의 기대 출력을 결정하기 위한 협의 체계 구성

다. AI/ML 시스템의 기대 출력 설명 또는 해석 확인을 위한 사용자 평가단 구성

6.7 AI/ML 기능 관련 학습용 데이터 관리

가. 조직은 안전하고 신뢰할 수 있는 AI/ML 기능을 제공하기 위해 다음과 같이 필요한 데이터 수집 및 처리 활동을 강구하여야 한다.

1) 데이터의 명확한 이해와 활용을 지원하는 상세한 정보 관리

2) 데이터의 출처 기록 및 관리

3) 해당되는 경우, 데이터의 이상 여부 식별 및 점검

나. 조직은 학습용 데이터의 안전과 보안을 위해 다음과 같이 필요한 활동을 강구하여야 한다.

1) 해당되는 경우, 학습용 데이터 중독, 유출 등의 공격에 대한 방어

2) 해당되는 경우, 학습용 데이터의 편향성 완화

6.8 AI/ML 기능 관련 인공지능 모델 개발

가. 오픈소스 라이브러리를 활용하는 경우 라이브러리 사용에 따른 위험 관리를 실행하고 그 결과를 문서화하여야 한다.

1) 활성화된 오픈소스 라이브러리 사용 등 오픈소스 라이브러리의 안정성 확인

2) 사용중인 오픈소스 라이브러리의 라이선스 준수사항 확인

3) 사용중인 오픈소스 라이브러리의 호환성 및 보안취약점 확인

나. 조직은 AI/ML 기능 관련 인공지능 모델의 안전성 및 신뢰성을 제공

하기 위해 다음과 같이 필요한 활동을 강구하여야 한다.

- 1) 인공지능 모델의 매커니즘, 성능, 주의사항 등의 정보에 대한 모델 명세서
- 2) 해당되는 경우, 인공지능 모델의 편향성 분석 및 완화
- 3) 해당되는 경우, 모델 추출, 모델 회피 등 인공지능 모델의 공격에 대한 방어 대책 수립
- 4) 해당되는 경우, 인공지능 모델의 추론 결과에 대한 설명 제공

6.9 AI/ML 기능 관련 시스템 개발

조직은 AI/ML 기능 관련 시스템의 안전성 및 신뢰성을 제공하기 위해 다음과 같이 필요한 활동을 강구하여야 한다.

가. 인공지능 시스템의 문제 발생 알림 기능 제공

나. 인공지능 시스템의 보안 강화를 위한 보안 기법 적용

다. 해당되는 경우, 소스 코드 및 사용자 인터페이스로 인한 편향 완화

라. 해당되는 경우, 인공지능 시스템의 성능 저하 평가 지표 수립 및 알림

6.10 AI/ML 기능 관련 운영 및 모니터링

조직은 AI/ML 기능 관련 운영 및 모니터링 시 안전성 및 신뢰성을 제공하기 위해 다음과 같이 필요한 활동을 강구하여야 한다.

가. 인공지능 시스템의 올바른 사용을 유도하기 위한 목적, 범위, 제약사항, 면책조항 등 설명 제공

나. 해당되는 경우, 시스템 로그 등 인공지능 시스템의 의사결정에 대한 추적 방안 수립