정보화경영체제 인증규격

2013년

중소기업기술정보진흥원

목 차

0. 서 문 ····· 1

1. 적용범위 ····· 4

2. 용어정의 ····· 5

3. 정보화경영체제 요구사항 ····· 9

3.1 일반 요구사항 ····· 9

3.2 문서화 요구사항 ····· 9

3.3. 정보화 방침 ····· 10

3.4 계 획 ····· 10
3.4.1 목표 ····· 10
3.4.2 추진계획 ····· 11

3.5 실행 ····· 11
3.5.1 자원, 역할, 책임과 권한 ····· 11
3.5.2 교육훈련 ····· 12
3.5.3 프로젝트 관리 ····· 13
3.5.4 업무분석 ····· 13
3.5.5 공급자 선정 ····· 14
3.5.6 개발 ····· 14
3.5.7 검수 ····· 14

3.6 운 영 ····· 15
3.6.1 의사소통 ····· 15
3.6.2 문서 및 기록관리 ····· 15
3.6.3 운영관리 ····· 16
3.6.4 유지보수 ····· 16
3.6.5 보안 및 대응 ····· 17

3.7 점검 ····· 18
3.7.1 측정 및 내부심사 ····· 18
3.7.2 경영검토 ····· 19

A. 부속서 ····· 21

0. 서 문

정보기술의 발달로 인하여 사회가 지식기반사회로 전이됨에 따라 조직의 정보화를 통한 생산성 향상과 효율성 증진에 대한 관심이 점차 높아지고 있다.

과거 정보화는 주로 부문별로 도입한 정보시스템에 대한 감리와 통제를 통하여 적합성을 검토하는 방식이었으나, 조직의 경영에서 정보화가 차지하는 비중이 증대됨에 따라 단위 정보시스템 각각에 대한 감리와 통제만으로 조직의 경영목표에 적합하도록 전체 정보시스템을 일관되게 유지하는 것이 어려운 과제가 되고 있다.

따라서 전체 경영활동과 통합되고 융화되는 정보화 방식의 도입이 필요하며, 이를 통하여 조직의 전략적 측면이나 사회·경제적 요구들을 포함하는 포괄적인 문제를 고려하여 정보화를 추진하는 것이 바람직하다.

정보화경영체제는 조직의 정보화에 필요한 요구사항 즉, 기본 요건을 정의하고 있으며, 정보화를 추진하는 조직은 이 요구사항을 만족할 수 있도록 지속적이고 체계적으로 관리함으로써 효율적으로 조직의 정보화 수준을 향상시키고 유지할 수 있게 된다.

정보화경영체제의 규격은 기본적으로 특정한 조직의 형태나 크기, 업무처리형태 및 의사결정 방법에 제약을 받지 않는다. 예를 들어 유사한 성격의 활동을 행하는 두 조직의 정보화 수준과 성과가 서로 차이가 있음에도 불구하고 두 조직 모두가 규격의 요구사항을 만족할 수 있는 것이다.

정보화경영체제의 도입과 운영을 위한 기본모형은 그림1과 같다.

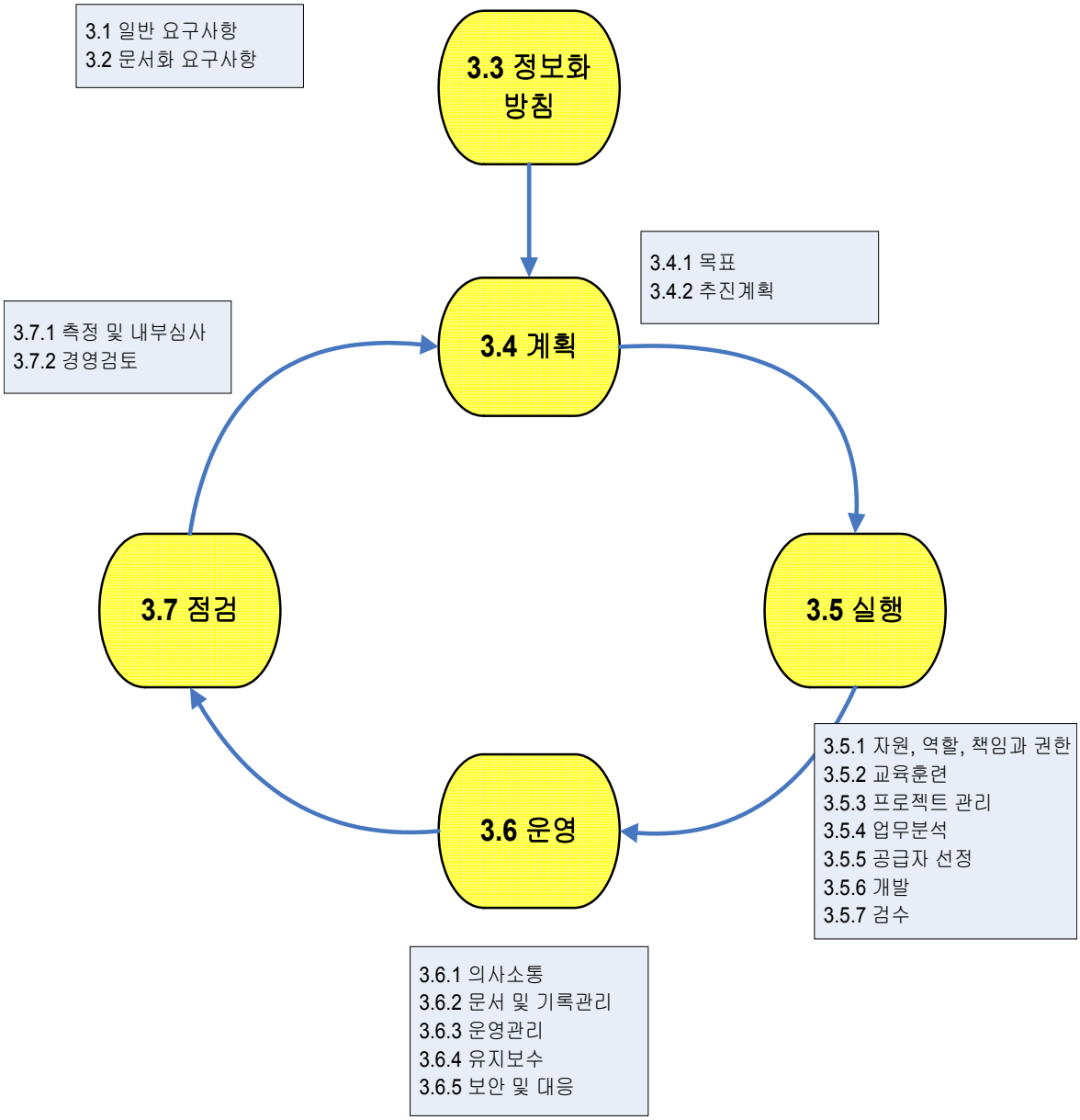

그림 1 정보화경영체제(IMS) 기본모형

이 규격은 인증이나 자체선언의 목적으로 객관적 심사가 가능한 요구사항들만을 포함하고 있으므로 조직은 규격의 성공적인 이행을 통하여 적절한 정보화경영체제를 유지하고 있다는 사실을 이해관계자들에게 보증할 수 있다.

이 규격에 기반하여 체계적인 방법으로 정보기술을 채택하여 정보화를 시행하는 경우 조직과 이해관계자에게 최대의 이익을 가져다 줄 수 있으나 이 규격의 채택 그 자체가 최적의 정보화 수준과 경영혁신을 보증하지는 않는다. 따라서 조직은 정보화경영체제의 채택과 함께 정보화목표를 달성하기 위하여 경제적으로 이용 가능한 최적의 정보기술을 사용하도록 노력하여야 하며 기술투자에 따른 비용측면의 효과성도 고려하여야 한다.

이 규격은 품질경영시스템 규격인 ISO 9000 및 환경경영시스템 규격인 ISO 14000과 동일하게 일반적인 경영체제의 원칙을 준수한다. 그러나 조직이 여러 가지 경영체제들을 동시에 운영할 때에는 상이한 규격 목적과 이해관계자로 인하여 적용에 약간의 조정 작업이 필요할 수도 있다는 점에 유의하여야 한다.

또한 품질경영시스템 및 환경경영시스템이 각각 품질과 환경 측면의 경영목적 달성을 다루는 것에 비하여, 정보화경영체제는 정보화의 측면에서 이해관계자 요구와 경영목적 달성을 위한 효율적인 사항을 다룬다는 점을 고려하여야 한다.

정보화경영체제의 도입을 위하여 조직이 기 운영 중인 타 경영시스템의 일부를 채택함으로써 관련 요구사항을 충족시킬 수도 있다.

1. 적용범위

이 규격은 조직에 영향을 미치는 경영환경을 고려하면서 정보화방침 및 목표를 설정하고 정보화를 체계적으로 추진할 수 있도록 정보화경영체제의 요구사항을 규정함을 목적으로 한다.

이 규격은 조직에서 관리가 가능하며 조직에 어떤 영향을 줄 수 있다고 예측되는 정보화 방침과 목표, 인적자원, 하드웨어, 소프트웨어, 운영 인프라 등과 같은 정보화 요소들에 적용된다.

이 규격은 다음과 같은 경우에 적용한다.

가. 정보화경영체제의 도입, 유지 및 개선을 하고자 할 때

나. 조직이 설정한 정보화경영체제의 적합성을 스스로 확인하거나 적합성을 다른 사람에게 증명하고자 할 때

다. 외부기관이나 제3자로부터 정보화경영체제에 대한 인증을 획득하려고 할 때

라. 이 규격에 대한 적합성을 자체 확인하고 선언하고자 할 때

이 규격에 규정된 모든 요구사항들은 조직의 수준과 범위에 관계없이 적용할 수 있으나 적용의 정도는 조직의 방침, 활동내용 및 경영여건 등의 여러 가지 요건에 의해 좌우된다. 예를 들어 정보화경영체제를 개선 또는 확장하는 경우 등에는 규격의 모든 요구사항을 순차적으로 적용하지 않아도 된다.

따라서 이 규격의 적용을 위한 범위를 사전에 분명하게 설정하여야 하며, 이 규격의 요구사항 적용에 대한 참고지침은 부속서 A에 나타나 있다.

2. 용어정의

이 규격에 사용된 용어들을 다음과 같이 정의한다.

2.1 기록(record)

달성된 결과 또는 수행된 활동의 증거를 명시하는 문서(2.3)를 의미한다.

2.2 내부심사(internal audit)

조직(2.18)이 설정한 정보화경영체제(2.13) 심사기준에 충족되는 정도를 결정하기 위하여 조직 자체에 의하여 수행되는 심사 증거를 수집하고 객관적으로 평가하기 위한 체계적이고 독립적이며 문서화된 프로세스이다.

비고 많은 경우, 특히 소규모 조직에서, 심사 대상 업무에 대하여 책임이 없다는 것으로 심사원의 독립성이 입증될 수 있다.

2.3 문서(document)

정보 및 정보지원 매체

비고1 매체는 종이, 자기, 전자 또는 광학 컴퓨터 디스크, 사진, 견본이나 그 조합이 될 수 있다.

비고2 정보화매뉴얼(manual)은 조직의 정보화경영체제를 규정한 문서로써 개별 조직의 규모 및 특성에 맞도록 세부 사항 및 형식이 다를 수 있다.

2.4 부적합(nonconformity)

요구사항의 불충족을 의미한다.

2.5 시정조치(corrective action)

발견된 부적합(2.4)의 원인을 제거하기 위한 조치이다.

비고1 부적합에는 하나 이상의 원인이 있을 수 있다.

비고2 시정조치는 재발을 방지하기 위하여 취해지나, 예방조치는 발생을 방지하기 위하여 취해진다.

2.6 심사원(auditor)

심사를 수행하기 위한 능력을 갖춘 사람을 말한다. 심사(audit)란 심사의 기준으로 활용되는 방침, 절차 또는 요구사항의 집합인 심사기준에 충족되는 정도를 결정하기 위하여, 심사기준에 관련된 검증할 수 있는 기록, 사실의 진술 또는 기타 정보인 심사증거를 수집하고 객관적으로 평가하기 위한 체계적이고 독립적인 문서화된 프로세스이다.

2.7 이해관계자(interested party 또는 stakeholder)

조직(2.18)의 정보화(2.11)에 의해 영향을 받거나 관련된 인원 또는 단체를 말한다.

2.8 절차(procedure)

활동 또는 프로세스를 수행하기 위하여 규정된 방식을 말한다.

비고 절차는 문서화될 수도 있고 문서화되지 않을 수도 있다.

2.9 정보기술(information technology)

다양한 형태로 정보의 생성, 저장, 교환 및 사용에 필요한 모든 형태의 기술을 말한다.

2.10 정보시스템(information system)

조직(2.18)이 수행하는 업무, 지식 및 관련 정보를 정보기술(2.9)을 활용하여 처리하는 체계로 소프트웨어, 하드웨어 및 통신망, 데이터베이스 및 관련 인력 등 일체를 포괄한다.

2.11 정보화(information)

정보기술(2.9)을 활용하여 조직(2.18)의 경영 효율화를 달성하도록 경영요소를 전환 또는 개선하는 활동을 말한다.

2.12 정보화경영(information management)

정보화(2.11)에 관하여 조직(2.18)을 지휘하고 관리하기 위하여 조장되는 활동을 의미한다.

비고 정보화(2.11)와 관련한 지휘 및 관리는 일반적으로 정보화방침(2.14) 및 정보화목표(2.15)의 수립, 정보시스템(2.10)의 운영과 개선 등을 포함한다.

2.13 정보화경영체제(information management system)

정보화방침(2.14)과 목표(2.15)를 정하고 이의 달성을 위한 조직(2.18), 책임 및 절차의 마련과 인적·물적 자원을 배분한 후 전사적으로 체계 있게 관리하는 조직의 경영체제의 일부를 말한다.

비고1 경영체제는 방침과 목표를 설정하고 그 목표를 달성하는데 활용하기 위한 상호 관련되는 요소들의 조합이다.

비고2 경영체제에는 조직 구조, 기획 활동, 책임, 관행, 절차(2.8), 프로세스 및 자원 등을 포함한다.

비고3 경영체제의 유형으로 정보화경영체제, 품질경영시스템, 환경경영시스템 등이 있다.

2.14 정보화방침(information policy)

최고경영자에 의해 공식적으로 제시된 정보화성과(2.16)와 관련된 조직(2.18)의 전반적인 의도 및 방향을 의미한다.

비고 정보화방침은 정보화목표(2.15)의 설정 및 실행을 위한 틀을 제공한다.

2.15 정보화목표(information objective)

정보화방침(2.14)과 일관성을 가지며 조직(2.18)이 정보화를 통하여 달성하고자 스스로 설정한 전반적인 목표를 의미한다.

2.16 정보화성과(information performance)

조직의 정보화에 대한 측정 가능한 결과를 의미한다.

비고 정보화경영체제(2.13)의 관점에서, 결과란 조직(2.18)의 정보화방침(2.14), 정보화목표(2.15) 및 기타 정보화성과(2.16) 요구사항에 대하여 측정한 것이 될 수 있다.

2.17 정보화 책임자(Chief Information Officer)

조직(2.18)의 정보화(2.11) 추진을 위한 경영자 대리인 즉 총괄책임자를 말한다.

2.18 조직(organization)

법인, 비법인, 공공 기관, 민간 기관이든에 관계없이 자체적인 기능과 행정을 갖춘 회사, 법인, 업체, 기업, 정부당국 또는 협회, 또는 이러한 집단의 일부분이나 연합체를 의미한다.

비고 1 개 이상의 운영 단위로 이루어진 조직(2.18)에 대해서는 단일 운영 단위가 1 개의 조직으로 규정될 수 있다.

2.19 지속적 개선(continual improvement)

조직(2.18)의 정보화방침(2.14)과 일관성이 있는 전반적인 정보화성과(2.16)의 개선을 달성하기 위하여 정보화경영체제(2.13)의 강화를 반복하는 프로세스이다.

비고 이 프로세스가 모든 활동 분야에서 동시에 이루어질 필요는 없다.

2.20 프로젝트(project)

조직(2.18)의 정보화목표(2.15)를 달성하기 위한 구체적인 정보화사업을 말한다.

비고 프로젝트는 착수일과 종료일, 비용 및 자원 등에 있어 제약이 있으며 특정 요구사항에 적합한 목표를 달성하기 위하여 수행된다.

3. 정보화경영체제 요구사항

3.1 일반 요구사항

조직은 이 규격의 요구사항에 따라 정보화경영체제의 수립, 문서화, 실행 및 운영과 지속적 개선을 하여야 하며, 어떻게 이 요구사항을 충족시킬 것인지를 결정하여야 한다.

3.2 문서화 요구사항

문서화는 정보화와 관련된 활동의 의도 및 일관성에 대한 의사 소통을 가능하게 하는 것으로 다음에 기여한다.

가. 요구사항과의 적합성 및 정보화목표 달성
나. 적절한 교육훈련 제공
다. 반복성 및 추적성
라. 객관적 증거 제공
마. 정보화경영체제의 유효성 및 지속적인 적절성 평가

정보화경영체제 문서화는 다음 사항을 포함하여야 한다.

가. 정보화방침 및 정보화목표 기술
나. 정보화경영체제의 범위 기술
다. 정보화경영체제의 주요 구성 요소, 그들 간의 상호관계 및 관련 문서의 참조에 대한 기술
라. 기록을 포함한 규격에서 요구하는 문서
마. 정보화 관련 주요 프로세스들의 효과적인 계획, 운영 및 관리를 보장하기 위하여 기록을 포함한 조직에서 필요하다고 결정한 문서

비고1 이 규격에서 “문서화된 절차”라는 용어의 사용은 그 절차의 수립, 문

서화, 실시 및 유지를 의미한다.

비고2 정보화경영체제 문서화의 정도는 다음의 이유로 인하여 조직에 따라 다를 수 있다.
가. 조직의 규모 및 활동의 종류
나. 도입 정보기술과 운영환경의 특성
다. 조직구성원의 능력

비고3 문서의 양식 및 매체의 종류는 어떠한 것이라도 가능하다.

3.3. 정보화방침

최고경영자는 다음 사항을 보장하는 조직의 정보화방침을 설정하여야 한다.

가. 조직의 규모와 활동, 제품 및 서비스의 특성에 적합할 것
나. 정보보호를 포함하여, 정보기술의 발전방향 및 환경의 변화가 반영되어 있을 것
다. 정보화목표를 설정하고 검토하기 위한 틀을 제공할 것
라. 정보화경영체제에 대한 지속적인 지원, 개선 및 확장에 대한 의지가 포함될 것
마. 조직을 통하여 문서화되어 전달되고, 이해되며, 실행될 것
바. 필요시 이해관계자에게 이용 가능하게 하고 지속적으로 적합성에 대하여 검토할 것

3.4. 계 획

3.4.1 목표

조직은 정보화방침에 따른 측정 가능한 정보화목표를 수립하고 이의 달

성을 위한 관련 활동을 이행하여야 하며, 이 목표는 정보화경영체제 운영에 따른 성과 및 목표에 대한 기여를 평가하는 척도로 관리되어야 한다.

조직이 정보화목표를 수립할 때에는 조직의 경영 환경, 기술적 대안, 재정, 생산 및 영업상의 여건과 이해관계자의 견해를 고려하여야 한다.

조직은 정보화방침을 충족할 수 있도록 정보화목표를 설정하여야 하며 정보화경영체제 운영을 통한 경영혁신에 대한 의지를 포함하여야 한다.

3.4.2 추진계획

조직은 정보화목표를 달성하기 위하여 정보화추진계획을 수립하고 이행하여야 한다.

정보화추진계획에는 정보화방침과 목표를 달성하기 위한 방법과 하부조직별 책임이 명시되며, 이를 위하여 조직은 현재 운용 중인 정보시스템들의 운영계획 뿐 아니라 정보시스템의 변경 및 확장 등을 포함한 신규로 추진해야 하는 주요 정보화 프로젝트에 대한 세부계획을 수립하여야 한다.

정보화추진계획은 문서화되어야 하며 주기적으로 검토, 보완 및 승인이 되어야 한다.

3.5 실행

3.5.1 자원, 역할, 책임과 권한

조직은 정보화경영체제를 효과적으로 수립, 실행, 유지 및 개선하기 위하여 정보화와 관련된 조직 및 구성원에 대한 역할, 권한 및 책임을 규정하고

문서화하여야 한다.

조직의 최고경영자는 정보화경영체제의 실행과 운영에 필요한 자원제공을 보장하여야 한다.

최고경영자는 다음 사항을 이행하는 정보화 책임자를 지정하여야 한다.

가. 정보화경영체제가 이 규격에 따라 수립, 실행되고 유지됨을 보장

나. 정보화경영체제의 개선을 위한 의사결정자료로 활용할 수 있도록 최고경영자에게 정보화성과를 보고

다. 경영자를 포함하여 조직 내부 및 외부와의 의사소통

3.5.2 교육훈련

조직은 정보화경영체제와 관련한 교육훈련의 필요성을 인식하고 정보화경영체제에 영향을 미칠 수 있는 업무를 담당하는 모든 조직구성원에 대하여 교육훈련을 제공하여야 한다.

정보화경영체제에 중대한 영향을 야기할 수 있는 업무를 수행하는 인원은 관련된 교육훈련, 경력 및 숙련도 등의 측면에서 일정 수준의 자격을 갖추어야 한다.

교육훈련과 관련된 조직구성원은 정보화경영체제를 운영하기 위한 역할, 이점 및 이로 인한 영향을 인식하여야 한다.

조직의 교육훈련 계획에는 다음 사항을 포함시켜야 하며, 교육훈련의 계획 및 이행결과에 대한 기록을 유지하여야 한다.

가. 교육훈련 요구사항

나. 교육훈련의 인원, 시기 및 방법

다. 교육훈련 이행 및 평가

3.5.3 프로젝트 관리

조직은 정보화추진계획에 명시된 정보시스템의 운영을 위한 개별 프로젝트의 추진을 위하여 문서화된 프로젝트 계획을 수립하고 이행하여야 한다.

프로젝트 계획에는 다음 사항이 포함되어야 한다.

가. 세부목표, 추진일정, 소요자원, 의사소통 및 구매 관리

나. 프로젝트 수행에 대한 책임 지정

다. 프로젝트 결과에 대한 품질확보 방안

프로젝트의 전체 또는 일부는 외부로부터의 구매 또는 용역 방식으로 추진할 수 있으며, 필요한 경우 외부 전문가의 기술자문을 이용할 수 있다.

3.5.4 업무분석

조직은 정보화 대상 업무에 대한 분석을 실시하여야 하며 이때 사용자의 문서화된 요구사항을 추진 프로젝트에 반영할 수 있도록 고려하여야 한다.

업무분석 결과에는 다음 사항이 포함되어야 한다.

가. 정보화를 추진하고자 하는 업무의 내용 및 범위

나. 현재 수행업무의 분석

다. 사용자 측면의 요구기능 및 입출력 양식 등의 요구사항

라. 관련 표준 및 운영환경

업무분석 결과의 적절성은 검토되어야 하며 관련 기록을 유지하여야 한다.

3.5.5 공급자 선정

조직은 정보시스템의 도입 또는 확장 및 운영을 위한 계약, 구매 및 용역 관리에 대한 적합성을 보장하여야 한다.

조직은 업무분석 결과를 정보시스템으로 적절하게 구현할 수 있는 적합한 공급자를 평가하고 선정하기 위한 기준과 방법을 설정하고 문서화하여야 한다.

계약 및 구매문서는 정보시스템의 개발 및 운영 특성이 고려된 요구사항 이행의 적합성을 검증하기 위한 관련 정보를 포함하여야 한다.

3.5.6 개발

조직은 정보시스템의 자체개발 또는 용역개발을 위하여 문서화된 절차를 수립하고 이행하여야 한다.

정보시스템의 개발절차에는 다음 사항이 포함되어야 한다.

가. 분석·설계·구현 및/또는 설치·시험·운영에 대한 관리·통제방법

나. 개발 단계별 검증과 개발결과에 대한 품질보증 방안

조직은 개발 절차에 따라 진행되는 각 단계에서 생성되는 주요 결과들에 대한 기록을 유지하여야 한다.

3.5.7 검수

조직은 개발의 최종 결과물인 정보시스템의 시험가동, 운영시험 및 인수 등에 대한 문서화된 절차를 수립하여 이행하고, 각 단계별 시나리오를 작성

하여야 하며, 관련 결과에 대한 기록을 유지하여야 한다.

검수절차와 계획을 수립할 때에는 다음 사항을 고려하여야 한다.

가. 시험가동 및 운영자 교육방법

나. 시험가동기간

다. 최종 결과물의 종류

라. 시험 방법 및 적합성 판정기준

마. 운영의 실현가능성 및 효율성

3.6 운 영

3.6.1 의사소통

조직은 효율적인 정보화경영체제 운영을 위하여 조직 내의 여러 기능과 계층 간의 의사소통을 보장하여야 한다.

조직은 정보화경영체제 운영에 대한 중요한 의사소통 과정 및 조직의 결정 사항들에 대하여 기록을 유지하여야 한다.

3.6.2 문서 및 기록관리

조직은 정보화경영체제 운영과 관련된 주요 기록, 기술동향, 조사평가 및 의사소통 결과 등에 대한 중요한 정보의 수집·보관 및 공유를 통하여 신속한 의사결정에 활용할 수 있도록 필요한 절차를 마련하여야 한다.

조직은 정보를 정형화하여 체계적으로 관리하기 위한 각종 문서의 개발, 작성, 식별, 유지 및 조회가 가능하도록 문서화된 절차를 수립하고 이행하여야 한다.

조직은 컴퓨터의 보조기억장치 등에 저장되는 정보의 보관 및 활용을 위한 문서화된 절차를 수립하고 이행하여야 한다.

조직은 정보화경영체제의 적합성과 달성된 결과를 실증하기 위하여 필요한 기록을 유지하여야 한다.

조직은 기록의 식별, 보관, 보호, 검색, 보유 및 폐기에 대한 문서화된 절차의 수립, 실행 및 유지를 하여야 한다.

기록은 읽기 쉽고, 식별 및 추적이 가능하여야 한다.

3.6.3 운영관리

조직은 정보화방침 및 목표와 관련된 정보화경영체제의 운영과 활동을 파악하고 수행하기 위한 세부운영 절차 및 관련 운영 기준을 포함한 문서화된 운영관리 절차를 수립하여야 한다.

정보화 업무에 대한 운영절차와 정보시스템에 대한 운영절차를 별도로 문서화하여야 한다.

조직은 주기적으로 운영관리에 대한 관련 기록을 유지하여야 한다.

3.6.4 유지보수

조직은 정보시스템의 안정된 운영을 위하여 문서화된 절차를 수립하고 이행하여야 한다.

조직은 유지보수를 위하여 다음 사항을 조치하여야 한다.

가. 책임 및 권한의 지정
나. 정기적인 예방점검 및 문제에 대한 복구조치
다. 유지보수 요청에 대한 접수 및 처리 방법
라. 외부 위탁관리 절차
마. 운영 자료의 백업 관리

조직은 정보시스템의 유지보수 관련 기록을 유지하여야 한다.

3.6.5 보안 및 대응

조직은 정보보호에 대한 정보화방침을 근간으로 내·외부로부터의 정보시스템에 대한 통제를 위하여 보안담당자를 지명하여야 하며, 다음과 같은 보안 대책을 수립하고 이행하여야 한다.

가. 정보 및 업무별 접근 권한과 범위의 제한
나. 통신망 불법침입에 따른 자료유출 및 훼손
다. 정보시스템의 직접 접근을 통한 자료유출 및 훼손
라. 보안체계 붕괴 시의 긴급복구 및 처리대책

조직은 천재지변, 예기치 않은 사고 또는 돌발상황의 발생으로 인한 정보시스템의 피해를 최소화하기 위하여 문서화된 비상계획을 수립하여야 하며, 비상계획에는 다음 사항이 포함되어야 한다.

가. 비상사태 유형 및 조치방안
나. 화재와 정전 등 정보시스템의 정상적인 운영에 지장을 주는 사고 발생에 대한 대책
다. 시설, 시스템, 자료의 파괴 또는 손상 시의 복구대책
라. 정보시스템이 집중 설치된 장소에 대한 필요 시 통제구역 설치 및 출입자 통제
마. 비상조치 및 안전관리에 대한 주기적 예방교육 실시

조직은 사고 혹은 비상사태 발생 후 그 조치 결과를 기반으로 비상계획을 검토하고 필요한 경우 개정하여야 한다.

사고 및 비상조치 관련 기록을 유지하여야 한다.

3.7 점검

3.7.1 측정 및 내부심사

조직은 정보화경영체제의 지속적 개선을 위하여 주기적으로 수행하여야 하는 정보화경영체제에 대한 측정 및 내부심사를 위한 문서화된 절차를 수립하고 이행하여야 한다. 측정 및 내부심사의 주요 사항은 다음과 같다.

가. 정보화 성과의 측정 여부와 결과
나. 부적합 사항의 확인과 조치
다. 정보화경영체제가 다음 사항을 만족하는지의 결정
  1) 이 규격의 요구사항을 포함한 정보화 추진계획과의 적합성 여부
  2) 정보화경영체제의 적절한 이행 및 유지 여부
라. 최고경영자에게 심사결과에 대한 결과보고

조직은 정보화목표 및 추진계획에 대한 적합성, 운영관리상태 및 정보화 성과 등을 추적, 측정 및 확인하여야 하며, 그 결과에 대한 기록을 유지하여야 한다.

조직의 실제 또는 잠재적인 부적합사항의 원인을 제거하기 위하여 취해지는 모든 시정조치는 해당 문제의 수준에 적절하여야 하고 발생한 부적합으로부터의 영향에 상응하여야 한다.

조직은 부적합 사항에 대한 시정조치 및 개선내용을 토대로 모든 절차상의 변경 및 이행 사항에 대한 기록을 유지하여야 하며 그 유효성을 확인하여야 한다.

측정 및 내부심사 결과는 해당 부서에 전달되어야 하며, 심사대상 부서의 책임자는 심사 중 발견된 부적합 사항에 대하여는 적기에 시정조치를 취하여야 한다.

측정 및 내부심사 절차는 측정 및 심사 대상 주요 사항들을 중심으로 실시와 결과보고에 대한 요건 및 책임, 측정 및 심사의 범위·주기 및 방법을 포함하여야 한다.

내부심사 계획은 일정을 포함하여 관련 활동의 중요성 및 과거의 심사결과를 바탕으로 수립되어야 한다.

조직은 측정 및 내부심사 결과와 관련된 기록을 유지하여야 한다.

3.7.2 경영검토

조직의 최고경영자는 정보화경영체제의 지속적인 적합성 및 효과성을 보장하기 위하여 계획된 주기로 정보화경영체제를 검토하고 그 결과를 문서화하여야 한다.

경영검토에 포함될 사항은 다음과 같다.
가. 목표 및 추진계획의 달성정도
나. 내부심사결과
다. 경영환경 및 정보기술의 변화에 따른 정보화경영체제의 지속적 적합성
라. 관련된 이해관계자의 관심사

조직은 경영검토에서 논의된 관찰, 결론 및 권고에 대한 기록을 유지하여야 하며, 필요시 개선을 실시하고 그 효과성을 점검하여야 한다.

경영검토 결과에는 정보화경영체제에 대한 지속적 개선 의지와 일관성이 있도록 정보화방침, 목표 및 정보화경영체제의 관련 요소들의 변경에 관련된 결정과 조치가 포함되어야 한다.

A. 부속서 정보화경영체제 - 참고지침

정보화경영체제에 관한 이 부속서는 정보화경영체제의 요구사항에 관한 추가 정보를 제공함으로써 규격의 해석상 오해를 피하고 정보화경영체제 실행이 용이하도록 지원하기 위하여 작성되었다.

이 규격은 정보화성과의 증진방안을 계획하고 실행하기 위하여 조직이 정기적으로 그들의 정보화경영체제를 검토하고 평가한다는 개념에 입각한 것이다. 조직은 규격에서 기술한 정보화경영체제의 실행을 통하여 정보화성과를 개선할 수 있으며, 나아가 정보시스템의 개선으로 부가적인 경영의 성과도 얻을 수 있다.

정보화경영체제는 정보화의 지속적 개선을 달성할 수 있도록 체계적 과정을 제공하며, 개선에 따른 성과 및 개선의 정도는 기업의 제반 경영여건과 경제성 등을 토대로 조직에 의하여 결정된다. 특히 조직은 이 규격의 요구사항을 만족시키기 위하여 수행한 노력에 대한 결과가 현재의 정보화경영체제의 부분적 운영개선으로 나타날 수 있으나, 새로운 정보시스템 도입을 병행할 때 획기적인 성과로 나타날 수 있음을 인식하여야 한다.

이 규격은 “정보화방침, 계획, 실행, 운영, 점검” 단계의 동적 순환 과정에 기초한 정보화경영체제의 요구사항들을 포함한다. 따라서 조직은 각 단계가 포함하는 개별적 요구사항을 충실히 만족시키면서 단계를 순환시킬 때 지속적인 정보화 수준의 향상과 궁극적인 정보화목표의 달성을 이룩할 수 있음을 인식하여야 한다.

또한, 이 규격은 여러 경영시스템의 원칙을 준수하고 있다.

A.1 적용범위

정보화가 조직의 경영방침 및 목표와 일치되어 추진되는 것을 전제로 하므로, 정보화경영체제는 전체 경영시스템의 한 부분이다.

따라서 이 규격에서 제시하는 요구사항은 조직이 현재 운영 중이거나 향후 도입예정인 정보시스템뿐만 아니라 정보화에 영향을 주거나 정보화를 통하여 영향을 받을 수 있는 모든 경영환경에 적용되어야 한다.

이 규격은 조직의 규모나 유형에 관계없이 적용될 수 있도록 설계되었다. 따라서 조직은 조직의 제반 여건에 적합하도록 규격을 해석하여 조직의 능력이나 자원의 낭비없이 절차와 문서 등을 마련하고 조직의 정보화목표를 효과적으로 달성함과 동시에, 사용자에게는 만족성을 제공하도록 조직 형편에 적합한 정보기술을 선택하여 이행하는 것이 중요하다.

또한 조직은 필요에 따라 정보화경영체제를 적용하는 조직단위를 융통성 있게 설정할 수 있으며, 전체 조직, 특정 운영단위 또는 조직의 활동에 대해서도 이 규격의 이행을 검토할 수 있다. 이 규격이 특정 운영단위나 활동에서만 실행되는 경우 조직이 운영하는 다른 경영체제에서 수립한 방침과 절차들을 이 규격 요구사항의 충족에 사용할 수 있다.

조직은 이 규격을 외부 기관으로부터의 심사 목적으로 활용할 수 있을 뿐 아니라 조직 내부적으로 자체 인증 또는 선언을 위하여도 활용할 수 있다. 또한 조직은 이 규격에서 기술된 요구사항들을 기반으로 정보화경영체제를 설정하고 유지하여야 한다.

A.2 용어정의

별도 해설 없음.

A.3 정보화경영체제 요구사항

A.3.1 일반요구사항

조직은 이 규격의 요구사항을 기본으로 조직의 경영여건과 특성을 고려하여 조직에 적합한 정보화경영체제를 수립하여야 한다. 정보화와 관련한 주요 지침 및 절차 등의 문서화, 정보시스템의 도입 또는 개발과 운영 및 지속적 개선 등이 추진되어야 한다.

이 규격에서 규정된 정보화경영체제의 요구사항은 궁극적으로 정보화성과의 개선을 의도한다. 따라서 이 규격은 개선기회를 파악하고 실행하기 위하여 조직이 주기적으로 조직의 정보화경영체제를 검토하고 평가한다는 전제에 기초를 두고 있다. 지속적인 개선의 일정과 정도는 조직의 여건과 경제성에 따라 조직이 결정한다.

A.3.2 문서화 요구사항

정보화경영체제에 있어 문서화의 중요한 의도는 정보화방침을 표현하고 정보화경영체제의 운영 및 관리를 위한 절차와 방법을 표준화하기 위함이다.

정보화경영체제를 위한 문서는 이 규격을 적합하게 이행하기 위하여 작성하는 것으로 정보화방침 및 목표, 정보화업무 표준 및 운영절차, 조직, 정보화와 관련된 각종 문서의 종류와 관리방향을 정의하는 등 보다 구체적인 정보

를 어디서 어떻게 취득할 수 있는가에 대한 방향을 제공하기에 충분하여야 한다.

또한 문서화는 다음과 같은 사항을 포함할 수 있다.

가. 정보화방침 및 목표의 문서화된 결과

나. 정보화경영체제 매뉴얼

다. 이 규격이 요구하는 문서화된 절차

라. 정보화경영체제의 효과적인 기획, 운영 및 관리를 보장하기 위하여 조직이 필요로 하는 문서

이미 관련 문서가 조직에 존재하는 경우 조직 차원의 효율적 경영을 위하여 별도로 해당 문서를 작성할 필요는 없다. 또한 이러한 문서는 조직에 의해서 실행되는 다른 경영시스템의 문서와 통합될 수 있다. 단, 이 경우 해당 절차서 등에 언급하여야 한다.

A.3.3. 정보화 방침

정보화방침은 조직의 정보화성과 유지 및 지속적 개선을 위하여 조직의 정보화경영체제의 실행 및 개선을 유도하는 핵심요소이다. 또한 정보화방침은 조직의 정보화목표 설정 시 그 근거를 제공하는 중요한 수단이며, 방침 결정에 앞서 조직의 경영방침과 정보화 수준을 포함한 정보화 환경에 대하여 고려할 필요가 있다.

정보화방침에서 무엇보다 중요한 사항은 최고경영자의 의지이며, 정보화경영체제 운영을 위한 최고경영자의 중요한 역할과 책임은 다음과 같다.

가. 정보화방침 및 목표, 추진계획의 승인 및 이행의 보장

나. 종업원 참여를 위한 내부 환경의 조성 및 인센티브제 실시

다. 정보화경영체제 운영을 위한 조직, 인원 및 책임과 권한의 할당

라. 소요자원에 대한 가용성 보장
마. 경영검토의 수행 및 중요 의사결정을 위한 검토회의 참여
바. 최고경영자를 위한 정보화 교육 참가

이러한 최고경영자의 의지는 확고한 결의와 함께 실무현장에서 이행되고 확인될 수 있어야 한다.

A.3.4 계획

A.3.4.1 목표

조직은 정보화방침을 추진하기 위한 정보화목표를 설정하여야 한다. 정보화 추진에 대한 정기적인 성과측정 등을 통하여 설정된 정보화목표에 대한 달성여부가 확인되어야 하며, 필요시 정보화목표를 수정할 수 있다.

목표는 정보화성과를 판단할 수 있도록 구체적이고 정량적으로 설정하여야 한다. 따라서 조직은 조직의 생산성 향상, 지식·정보 등 자원의 최적활용, 서비스 만족도의 개선 및 조직구성원의 정보화 능력제고 등의 관점에서도 긍정적인 효과와 부정적인 효과를 동시에 분석할 수 있도록 목표를 설정하여야 한다.

정보화목표를 실행하기 위한 기술적인 방안을 검토할 때 조직은 향후의 기술발전 방향과 조직의 운영기준에 적합한 경우, 경제적으로 실현 가능한 최적의 정보기술 사용을 검토할 수 있다.

A.3.4.2 추진계획

정보화추진계획을 체계적으로 수립하고 활용하는 것은 정보화경영체제를

성공적으로 이행하기 위한 핵심적 요소 중의 하나이다.

정보화추진계획에는 주요 프로젝트, 목표, 일정, 소요자원 및 책임 등이 포함되어야 한다.

정보화추진계획의 수립을 위하여 경영 전략적 측면이나, 정보보안을 포함한 기술적 측면 및 경제적 측면에서의 타당성 분석이 선행되어야 하며 아울러 소요예산이나 일정계획, 프로젝트간의 관련성 및 추진 우선 순위 등 종합적인 관점에서의 검토가 이루어져야 한다.

또한, 정보보호 측면에서는 정보화추진에 있어 보호되어야 할 자산과 범위 설정을 한 후 위험을 평가하여 관리할 수 있도록 계획을 수립하여야 한다.

A.3.5 실행

A.3.5.1 자원, 역할, 책임과 권한

정보화경영체제의 성공적인 실행을 위하여 조직의 모든 구성원의 의지가 뒷받침되어야 한다. 따라서 정보화 책임에는 정보화 기능 뿐 아니라 관련된 기타 기능도 포함될 수 있다. 이러한 정보화경영체제의 실행의지는 최고 경영층으로부터 표명되어야 하고 조직의 최고경영자는 정보화경영체제가 실행되도록 보장하여야 한다.

최고경영자는 정보화경영체제를 주관하는 조직 및/또는 구성원에게 정보화경영체제의 전반적 활동에 필요한 적절한 책임과 권한을 보장하여야 한다.

또한 최고경영자는 정보화가 성공적으로 추진될 수 있도록 적극적인 지원을 하여야 하며, 중요한 지원요소에는 인적자원, 제도, 기술, 설비, 시스

템, 재정자원, 지식 및 정보보호 등이 있다.

이를 위하여 최고경영자는 정보화경영체제의 이행을 보장하는 책임과 권한을 갖는 특정 경영자 대리인을 정보화 책임자로 지정할 수 있다. 중소기업의 경우는 한 명의 정보화책임자가 이러한 임무를 수행할 수 있으나, 조직의 규모에 따라서 최고경영자를 포함하여 두 명 이상의 정보화 책임자를 둘 수 있다.

A.3.5.2 교육훈련

정보화목표를 달성하기 위하여 조직 구성원의 정보화 능력과 수준을 파악하고 개발하는 것이 중요하다.

교육훈련은 반드시 최고경영자를 포함하여 계층별로 적합하게 실시되어야 한다. 교육훈련을 위하여 조직자체의 교육과정이나 외부전문교육과정을 활용할 수 있다. 교육훈련과정은 그 성과평가와 함께 관련 기록을 유지하여야 한다.

또한 조직은 정보화 관련 조직 구성원에 대한 경험, 능력 및 훈련수준 등과 같은 자격 조건을 규정하여 정보화를 효율적으로 수행할 수 있도록 하고 아울러 이러한 자격을 유지하는 데 필요한 교육훈련의 기회도 보장하여야 한다.

교육훈련을 통하여 조직 구성원이 다음과 같은 인식을 갖도록 하여야 한다.

가. 정보화방침 및 절차와 정보화경영체제 요구사항을 준수하는 일의 중요성

나. 정보화가 자신들의 업무활동에 미치는 중대한 영향과 개인적인 역

량의 향상에 따른 정보화 추진 상 이득

다. 정보화방침, 정보화목표와 관련 절차들, 긴급사태의 대비와 처리요건을 포함한 정보화경영체제 요구사항을 준수하기 위하여 필요한 역할과 책임

라. 규정된 운영절차들을 준수하지 않음으로 인하여 발생할 수 있는 결과

교육훈련은 조직 구성원이 수행하는 기본업무 외에도 다음과 같은 추가적인 요구 사유가 있을 경우 실시할 수 있다.

가. 정보화추진계획 수립에 필요한 미래 지향적 요구

나. 정의된 활동을 수행할 인력에 대한 능력 평가의 결과

다. 관련 법률 및 규정과 표준 등 조직의 정보화에 직접적 영향을 주는 활동 및 자원

라. 정보보호를 포함하여 정보화를 추진하는데 중요한 논점

필요한 경우 조직은 협력회사나 외주회사의 관계자에 대한 교육훈련계획을 수립하여야 한다.

아울러 조직 구성원의 교육효과를 높이기 위하여 조직 자체적으로 동기부여 방안을 마련하는 것이 바람직하다.

A.3.5.3 프로젝트 관리

프로젝트 계획은 정보화추진계획의 하부로서 수립되며, 정보화 대상에 대한 업무분석, 공급자선정, 정보시스템 개발 및 검수 등의 절차를 포함한다.

프로젝트 관리는 영속성 있게 수행되는 것이 아니라 일정기간 즉, 프로젝트의 수명주기 동안 계획, 실행 및 점검 등 자체적인 관리절차로 운영된다.

프로젝트 관리는 범위관리, 일정관리, 비용관리 및 품질관리 등을 포함할 수 있다.

조직은 품질관리를 위한 방안으로 개발공정의 적합성을 확인하기 위한 품질보증계획을 수립할 수 있으며, 품질보증에 대한 계획수립과 품질평가, 품질통제 및 검토회의 개최 등의 절차를 거칠 수 있다.

프로젝트를 외주용역으로 진행할 경우 프로젝트 관리방안을 제안요청사항으로 사전에 용역 수행 회사에 요청하여 해당 내용을 검토하는 것이 바람직하며, 용역회사의 프로젝트진행을 단계별로 통제하여야 한다.

A.3.5.4 업무분석

업무분석은 정보화 대상 업무를 명확히 정의한 후 최종 결과물이 사용부서의 용도와 의도에 적합하게 구축되도록 하기 위하여 필요하다.

업무분석 결과는 조직의 내부 정보화 인력에 의한 자체 개발 또는 외부인력에 의한 위탁개발을 위한 요구사항으로 기술되며, 이 요구사항에는 기능적 요구사항과 비기능적 요구사항이 포함된다.

기능적 요구사항은 업무를 정보화로 전환한 후 현업 사용자가 이용하는 세부 기능을 포함한다.

비기능적 요구사항은 목표 시스템의 성능 및 용량, 활용 컴퓨터 및 통신망의 성능, 시스템 자체 또는 외부 인터페이스를 위하여 적용되는 표준, 시스템 구축 및 설치환경, 시스템 시험방법, 시스템 보안, 시스템 운영 및 유지보수 대책과 시스템 교육훈련에 관한 사항 등을 포함한다. 비기능적 요구사항으로 시스템의 신뢰성, 안정성, 확장성, 병용성 및 실용성 등을 추가로 고

려할 수 있다.

특히 업무분석결과 작성 시 업무와 관련된 모든 부서의 의견이 충분히 반영될 수 있도록 주요 업무담당자들의 참여가 보장되어야 하며, 작성된 업무분석 결과는 확정하기에 앞서 검토회의를 통하여 관련업무담당자의 협의와 최종적으로 검증 및 확인할 수 있는 절차를 거쳐야 한다.

A.3.5.5 공급자선정

조직이 정보시스템을 개발, 확장 또는 보완하려고 할 때, 자체 정보화 인력이 충분하지 못한 경우 효율적으로 정보화를 추진하기 위하여 외부 전문인력 활용을 통하여 즉, 아웃소싱을 의뢰할 수 있다.

아웃소싱은 대상 업무의 선정, 서비스 공급자의 선정, 계약, 개발과 검수 등의 절차로 수행된다. 서비스 공급자의 선정을 위하여 잠재적 서비스 공급자의 파악, 제안요구사항(RFP: Requirement For Proposal)의 작성 및 배포, 설명회 개최, 제안서 접수 및 평가와 서비스 공급자 선정 등의 절차를 거칠 수 있다.

정보화추진조직은 프로젝트 요구사항, 품질 목표, 계약 협상점, 이행기관의 예산과 공급자 선정기준 등을 포함한 제안요구사항을 작성하고 배포할 수 있다.

정보시스템에 대한 아웃소싱은 개발 측면뿐만 아니라 운영적 측면에서도 추진할 수 있으며, 이때 정보시스템의 보안에 대한 사항에 주의를 기울여야 한다.

A.3.5.6 개발

조직은 자체개발 혹은 외부 위탁을 통한 개발에 관계없이 최종 결과물의 적합성 여부의 판단에서, 결과물 그 자체의 확인을 포함하여 결과물 개발 주요과정의 적합성에 대하여도 확인하여야 한다.

시스템 개발 시 조직에서 별도로 정의한 절차 즉, 시스템 요구사항 정의, 시스템 설계, 모듈 설계와 구현 및 시험 등의 활동을 위하여 필요한 문서와 이러한 활동을 수행하였음을 확인할 수 있는 관련 문서들이 작성되어야 한다.

설계과정에서 작성된 문서들은 추후 개발 결과물의 확인을 위한 근거가 될 수 있다. 예를 들어 업무분석 과정에서 정의한 요구사항은 개발 결과물에 대한 검증조건이 된다.

아웃소싱 결과물에 대한 적합성 판단은 업무분석결과에 따른 요구사항과 시스템 설계서, 그리고 사용자와 서비스 공급자간에 작성한 계약서 등을 기초로 이루어진다.

A.3.5.7 검수

검수 단계에서는 시스템 설치와 일정기간 운영시험 후의 최종 승인 및 인수 등의 절차가 수행되며, 이 단계에서의 중요한 시험결과를 반드시 유지하여야 한다.

규정된 운영환경에 시스템을 설치할 때, 정상적인 운영이 보장되어야 한다. 이때 조직은 개발자가 요구하는 필요한 지원활동을 제공하여야 한다.

시스템 설치 후에는 일정기간 동안 사용 부서 또는 사용자가 기존의 업무와

병행하면서 실제 업무에의 적용 가능 여부를 확인하고 문제점을 보완하여 최종적인 안정화를 성취하여야 한다.

운영시험은 시스템 개발을 완료한 후, 시스템을 실제 업무에 적용하였을 때의 문제점을 보완하기 위하여 시험적으로 시스템을 운영하는 과정이다.

일정기간 동안의 시험가동으로 안정성이 확인된 후 공식적인 인수시험을 실시하며 이때 이전 단계에서 도출되었던 성능, 기능, 장애복구 및 보안 등과 같은 전반적인 요구사항에 대한 만족도를 점검하여 최종적인 인수여부를 결정한다.

검수를 위하여 별도의 팀을 구성하는 것이 바람직하며, 이 팀에는 사용자와 내부 또는 외부로부터 적합한 능력을 갖춘 전문가를 포함시켜야 한다.

A.3.6 운영

A.3.6.1 의사소통

정보화경영체제 운영을 위한 의사소통에는 정보화 업무 담당자간의 의사소통, 정보시스템 운영자와 정보화 업무 담당자간의 의사소통 및 조직의 내부 인원과 외부이해 관계자 사이의 의사소통 등이 있다. 각 유형의 의사소통을 위한 절차를 마련하여야 하며 각종 정보의 처리 및 공유절차 등도 확립하여야 한다.

또한 이러한 절차에는 비상시 의사소통계획도 포함되어야 한다. 조직은 특히 쇼핑몰, 인터넷 홈페이지 및 전자상거래 등에 대한 외부 이용자의 불만사항에 대한 의사소통절차를 마련하고 중대한 사항에 대한 처리 및 회신절차를 수립하여야 한다.

효율적인 의사소통을 위하여 관계자의 역할과 책임이 명확히 규정되어야 하며, 다양한 각종 매체를 적극적으로 활용하여야 한다.

A.3.6.2 문서 및 기록관리

정보화경영체제의 모든 단계에서 필요한 문서와 기록은 작성되고 관리되어야 한다.

조직은 문서가 다음과 같은 요구사항을 만족하도록 보장하여야 한다.

가. 문서는 읽기 쉽고, 쉽게 식별되어야 한다.

나. 문서는 이용 가능하여야 한다.

다. 문서는 수시 또는 정기적으로 검토하여 항상 최신의 것으로 유지될 수 있도록 개정, 승인, 전파하여야 한다.

라. 문서는 파손·훼손 및 손실로부터 보호되어야 한다.

마. 적정 승인권자에 대한 검토, 개정 및 승인 등의 책임 설정이 되어야 한다.

정보시스템에 관련한 문서의 예는 다음과 같다.

가. 정보화추진계획서

나. 정보시스템 운영에 필요한 각종 절차서 및 지침서

다. 업무분석서 및 정보시스템 설계서

라. 각종 계약서

마. 유지보수 계획서

정보화경영체제에 관한 기록의 예는 다음과 같다.

가. 정보시스템 운영 기록

나. 정보화업무 운영 기록

다. 교육훈련 기록

다. 시스템 장애 및 유지보수 기록
라. 성과 및 만족도 측정 결과 기록
마. 유지보수 계획 및 조치 기록
바. 성과측정 기록
사. 내부심사 기록 및 경영검토 기록
아. 기타 중요한 정보화 영향 기록

기밀이 유지되어야 할 문서와 기록에 대해서는 별도의 관리절차가 마련되어야 한다.

A.3.6.3 운영관리

조직은 정보시스템 운영기능과 활동들을 체계있게 수행하기 위한 운영절차를 문서화하여야 한다.

이때 수립되는 운영절차 내에 운영기준들을 설정하여 정보시스템 운영관리가 표준화되도록 하고, 업무운용에 대한 현황을 지속적으로 평가하고 개선하는 방안도 포함하여야 한다.

정보화업무에 대한 운영절차를 설정하는 주 목적은 사용자들이 정보시스템을 적극적이며 효율적으로 사용하도록 유도하기 위한 체제를 마련하고 운영함으로써 정보화성과를 향상시키는 것이다.

정보시스템에 대한 운영절차에는 정보화업무에서 처리하는 데이터와 데이터를 수록한 전자매체, 소프트웨어, 전산시스템, 통신망 자원, 안전 및 보안시스템과 시설 등을 운영하기 위한 절차와 운영현황의 기록, 평가 및 개선 등에 대한 절차가 기술되어야 한다.

A.3.6.4 유지보수

유지보수의 주요 활동에는 유지보수 계획수립, 서비스 공급자 선정 및 계약, 정기 및 수시 점검과 오류 및 변경요청에 대한 조치 등이 있다. 오류 및 변경요청에 대한 처리절차에는 접수, 검토 및 분석, 시험, 기록, 승인, 변경, 병행운영 및 백업과 폐기 등이 있다.

유지보수 계약을 체결할 경우 “3.5.5 공급자 선정”의 요구사항에 근거하여 계약서의 대상 및 기간 등과 같은 중요 계약정보를 관리하여야 한다.

유지보수 계획은 목적, 범위, 주관조직 및 책임자, 절차와 방법, 기록 및 보고 방법과 유지보수시스템의 환경 등을 포함한다.

유지보수의 범주에는 구성 및 변경관리, 성능관리, 보안관리, 사용자 자원관리, 운영아웃소싱관리, 운영상태관리, 전산실관리 및 예산관리가 포함된다.

유지보수 대상에 대한 종합적 변경관리를 위하여 형상관리 계획을 수립할 수 있다.

A.3.6.5 보안 및 대응

조직은 외부로부터의 정보도용 및 남용, 내부사용자의 정보유출, 해킹, 바이러스 및 자연재해 등과 같은 각종 위험과 위협으로부터 정보시스템, 관리정보 등에 대한 보안대책을 강구하여야 한다.

조직은 보안대상을 분야별, 계층별 및 공개 또는 비공개 등으로 분류하고 보안의 요구수준에 따라 적합한 대책을 강구하여야 한다.

또한 대상별로 소유와 사용에 대한 권리를 설정하고 보안 책임자 및 실무자를 지정함과 아울러, 책임 및 권한과 관련하여 인사규정이나 보안사고 시의 비상복구 조치절차도 마련하여야 한다.

보안을 위한 방법에는 정보시스템 및 정보자원에 대한 접근통제와 권한통제, 그리고 컴퓨터를 이용하는 각종 활동에 대한 추적 및 탐지 등이 있다.

장애관리는 소프트웨어, 하드웨어, 데이터베이스 및 네트워크 등의 운영관리 대상의 고장, 장애 및 서비스 불능 등과 같은 장애 여부의 관찰, 진단, 보고, 제어 및 처리하는 일련의 과정을 말하며, 장애원인 분석 및 조치를 통하여 장애시간을 단축하는데 그 목적이 있다. 장애의 근본원인을 사전에 차단하기 위하여 장애의 발생 통계 및 관리를 하며, 장애 발생을 예측하고 분석하여 중단없는 서비스를 제공하여야 한다.

따라서 정보시스템 관리자는 장애관리를 통하여 장애의 예방에 최선을 다하여야 한다.

비상사태란 발생된 장애의 업무파급 영향범위가 넓고, 신속한 복구가 필요한 시스템에 발생된 장애가 허용 시간 내에 복구가 불가능하여 통제 불가능한 재해가 예상되는 상태를 의미하며, 이러한 비상사태를 효과적으로 해결하기 위하여 비상사태 발생 시 대처방안을 미리 수립하여야 한다.

비상조치 방안에는 비상사태의 판단을 위한 의사결정 방법, 비상사태 선언 및 보고 방법, 비상 운영 및 복구 방법 및 필요 조직체계 구성 등에 대한 지침이 포함되어야 한다.

A.3.7 점검

A.3.7.1 측정 및 내부심사

조직은 정보화경영체제 운영을 통한 정보화 수준 향상 정도와 정보화성과 달성 정도를 주기적으로 비교 분석하기 위하여 단위업무별 활동 또는 업무전반에 걸쳐 성과를 측정하여야 한다. 조직은 부적합의 조사와 시정조치를 통하여 정보화경영체제의 적합성, 정보시스템의 안정성과 신뢰도 및 고객 만족도 등을 점검하고 개선하여야 한다. 또한 조직은 정보화경영체제에서의 계획수립과 그에 따른 이행 여부 등을 확인하고 필요 시 개선하여야 한다. 이를 위하여 조직은 성과 측정 절차, 부적합 조사 및 시정조치와 이행 적합성 심사에 관한 절차를 마련하고 그 절차에 따라 관련 업무를 수행하여야 한다.

측정 활동은 정보화의 효과성과 만족성을 나타낼 수 있는 중요한 판별 수단으로 인식되어야 한다.

정보화경영체제를 통한 성과는 효과성과 만족성 등으로 측정할 수 있다. 효과성은 달성하고자 하는 정보화목표에 대한 충족의 정도이며, 만족성은 고객의 제공받은 가치에 대한 만족하는 정도를 표현한 것이다.

조직은 다양한 방법으로 정보화성과를 측정하는 방안을 고려하는 것이 바람직하다.

조직은 내부심사를 통하여 운영 중인 정보화경영체제의 규격의 요구사항에 대한 부적합 사항을 조사하고 시정조치 하여야하며, 다음과 같은 요소들을 고려하여야 한다.

가. 부적합 원인의 규명

나. 필요한 시정조치의 규명 및 실행
다. 부적합 사항의 반복을 피하기 위하여 필요한 관리절차들의 실행 및 수정
라. 조치 후 결과에 대한 확인
마. 시정조치로 인하여 발생한 모든 변경사항의 기록

부적합 사항에 대한 시정조치에서는 잠재적 부적합의 예방조치를 포함하도록 고려하여야 한다.

내부심사를 통하여 조직은 정보화경영체제에서의 계획수립과 그에 따른 이행의 적절성 여부 등을 확인하고 필요 시 개선하여야 한다.

내부심사에는 다음 사항이 고려되어야 한다.
가. 심사 시 검토되어야 할 활동 및 분야
나. 심사 주기
다. 심사 관리 및 실행과 관련된 책임
라. 심사 결과의 전달 방안
마. 심사를 담당하는 심사원의 자격
바. 심사수행 방법

조직이 내부심사 계획을 수립할 때에는 과거 내부심사를 통하여 수집된 정보를 기반으로, 중요한 개선의 유도 및 효과적인 자원의 사용방안이 도출될 수 있도록 고려하여야 한다.

내부심사는 조직이 선정한 조직 내부인 및/또는 외부인에 의해 실시될 수 있다. 어느 경우든 심사를 수행하는 사람은 공정하고 객관적으로 심사를 실시할 수 있는 위치에 있어야 한다.

A.3.7.2 경영검토

정보화경영체제의 지속적인 개선, 적합성 및 효과성을 향상시키기 위하여, 그리고 그 결과 정보화목표를 달성하기 위하여 조직의 최고경영자는 정보화경영체제에 대한 정기적인 검토와 평가를 하여야 한다. 경영검토에서 모든 정보화경영체제의 요소를 한 번에 검토할 필요는 없으나 검토범위는 포괄적이어야 하고 검토과정은 일정주기에 걸쳐 발생될 수 있다.

경영검토는 반드시 최고경영자가 참석한 가운데 1년에 최소 1회 이상 이루어져야 한다.

관련된 경영관리자는 경영검토에 참여하여야 하며, 필요 시 다른 부문 및 기능이 검증된 인력을 포함시키는 것도 바람직하다.

경영검토의 입력 자료에는 다음 사항이 포함되어야 한다.

가. 정보화방침 및 목표의 달성 정도
나. 프로젝트 추진 결과
다. 부적합 시정조치 내용
라. 정보화경영체제 요소의 변경 사항
마. 개선을 위한 제언
바. 이전 경영검토의 후속 조치

또한 경영검토에서는 경영자가 이러한 평가를 수행하는데 필요한 정보가 수집·전달되는지를 확인하여야 하며 경영 검토결과에 대한 관련 기록을 유지하여야 한다.