TTA Standard

정보통신단체표준(국문표준) 제정일: 20xx년 xx월 xx일

TTAx.xx-xx.xxxx/R1

효과적인 정보보호 거버넌스를 위한 금융보안 조직체계

Financial Security Organization for Effective Information Security Governance

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 응용보안 및 평가인증 프로젝트그룹(PG505)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	최지선	금융보안원	대리	-	
표준 초안 작성자	강은성	금융보안표준 화협의회 (블록체인OS)	CISO	-	
	김건우	금융보안표준 화협의회 (중앙대학교)	박사	-	
	임형진	금융보안표준 화협의회 (금융보안원)	팀장	-	
	최지선	금융보안표준 화협의회 (금융보안원)	대리	-	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임	-	

이 표준 발간 이전에 접수된 지식재산권 확약서 정보는 이 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
이 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx.

서 문

1 표준의 목적

이 표준의 목적은 국내 금융회사의 조직체계가 업권이나 개별 회사별로 구성·운영하는데 차이가 있을 수 있다는 점을 고려하여 금융회사가 효율적인 거버넌스 구현을 위한 정보보호조직체계 수립 시 참고할 수 있는 정보를 제공한다.

2 주요 내용 요약

금융회사의 거버넌스를 위한 정보보호 조직체계를 위하여 아래의 내용을 포함한다.

- CISO 조직의 구성
- CISO의 직급과 권한
- 정보보호 협업체계의 수립 및 운영

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당 사항 없음

3.2 인용 표준과 이 표준의 비교표

해당 사항 없음

Preface

1 Purpose

The standard refers to the establishment of an information protection organization for efficient governance implementation by financial institutions considering that there may be differences in the organization system of domestic financial institutions in each business or individual company.

2 Summary

The standard includes the information protection organization system for governance of financial institutions.

- Composition of the CISO Organization
- Position and Authority of CISO
- Establishment and operation of a cooperative system for information protection

3 Relationship to Reference Standards

NONE

목 차

효과적인 정보보호 거버넌스를 위한 금융보안 조직체계 (Financial Security Organization for Effective Information Security Governance)

1 적용 범위

이 표준에서는 정보보호 조직체계가 업권이나 규모에 따라 차이가 있을 수 있다는 점을 고려하여 세부적인 조직체계보다는 거버넌스 측면에서의 조직체계를 다룬다. 즉, 국내 금융권 CISO의 보고대상 및 정보보호 전담조직의 편제를 고려하여 정보보호 조직체계를 아래와 같이 유형화하였다.

o CEO 직속 조직
o IT조직 산하
o 경영지원(재경, 인사, 총무 등) 조직 산하
o 내부통제(준법감시, 감사 등) 조직 산하

2 인용 표준

해당 사항 없음

3 용어 정의 및 약어

3.1 CEO (Chief Executive Officer)

최고경영자

3.2 CFO(Chief Financial Officer)

최고재무관리자

3.3 CISO(Chief Information Security Officer)

정보보호최고책임자

3.4 CIO(Chief Information Officer)

최고정보기술책임자

3.5 CPO(Chief Privacy Officer)

개인정보보호책임자

4 정보보호 조직체계 요구사항

이 표준은 국내 개별 금융회사의 효과적인 정보보호 거버넌스 구현 및 운영을 목적으로 한다.

5 CISO의 지정

금융회사는 전자금융거래법 제21조의2제1항에 의거하여 CISO를 지정하여야 하며, 업권 및 규모에 따라 CISO의 직급과 요건을 만족해야 한다.

5.1 CISO의 직급

전자금융거래법 시행령 제11조의3제1항에 의거하여 직전 사업연도 말을 기준으로 총자산이 2조원 이상, 상시 종업원 수가 300명 이상인 금융회사는 CISO를 임원으로 지정하여야 한다. 임원이라 함은 이사(은행권의 경우 본부장) 이상의 직급을 의미하며, CISO가 정보보호 업무에 대한 의사결정 권한을 갖고 CIO 등 타 임원들과 협업하기 위해서는 CISO는 C레벨의 임원으로 지정할 것을 권고한다.

<표 6-1> 금융회사 직급체계

<table>
<tr><th>구분</th><th>일반</th><th>은행</th><th>증권</th><th>카드</th><th>보험</th><th>제2금융</th><th>비고</th></tr>
<tr><td rowspan="5">임원</td><td>사장</td><td rowspan="2">은행장</td><td>사장</td><td>사장</td><td>사장</td><td>사장</td><td rowspan="3">C레벨</td></tr>
<tr><td>부사장</td><td>부사장</td><td>부사장</td><td>부사장</td><td>부사장</td></tr>
<tr><td>전무</td><td rowspan="4">부행장
상무
본부장
부장</td><td>전무</td><td>전무</td><td>전무</td><td>전무</td></tr>
<tr><td>상무</td><td>상무</td><td>상무</td><td>상무</td><td>상무</td><td rowspan="3">-</td></tr>
<tr><td>이사</td><td>상무보
이사</td><td>이사</td><td>이사</td><td>상무보
이사</td></tr>
<tr><td>직원</td><td>부장</td><td>부부장</td><td>부장</td><td>부장</td><td>부장</td><td>부장</td></tr>
</table>

5.2 CISO의 요건

전자금융거래법 시행령 제11조의3제4항에 의거하여 CISO는 정보보호 또는 IT 분야의 학력 및 자격을 만족해야 한다. CISO가 CEO를 비롯하여 타 임원들에게 정보보호의 중요성 설명하고 이해상충 시 이를 조정하기 위해서는 정보보호 및 실무적 지식을 겸비해야 한다. 또한, 정보보호 이슈에 대한 신속하고 정확한 의사결정을 내리고, 정보보호 조직을 효율적으로 운영하기 위한 리더십을 갖춰야 한다. 그리고 비 정보보호 및 비 IT(이하 현업) 임원 및 직원들을 포함한 전사적 정보보호를 위해서는 위험 관리 기반의 접근방법을

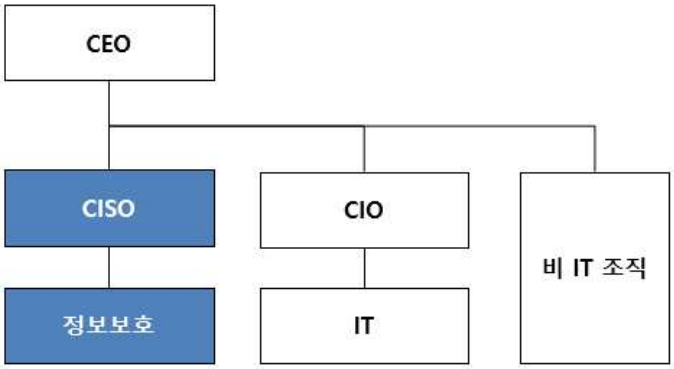
통해 소통하고 업무를 조정할 필요가 있다.

6 CISO 조직의 구성

CISO의 소속은 금융회사의 조직 및 사업, CISO의 직급과 정보보호조직의 규모에 따라 다를 수 있다. 이 표준에서는 전형적인 네 가지 유형을 제시하고 각 유형의 특징과 개별 회사가 자신의 조건에 맞는 유형을 참고하여 채택할 수 있도록 하였다.

6.1 CEO 직속

CISO의 조직이 (그림 7-1)과 같이 다른 조직에 속하지 않고 CEO에게 직접 보고하는 별도의 조직으로 구성될 수 있다.



(그림 7-1) CEO 직속의 CISO 조직

6.1.1 특징

o CEO와의 원활한 의사소통을 통해 신속한 의사결정 및 실행권한 확보
o 비즈니스 요구사항의 반영 및 사업전략과 정보보호 전략의 연계
o IT조직 및 비IT조직과의 원활한 소통 및 협업을 통한 전사적 정보보호 업무 이행
o CISO의 역량이 부족할 경우 IT조직 및 비IT조직과의 갈등 발생
o CISO의 직급이 낮을 경우 타 임원들의 견제를 받아 신속한 의사결정에 제약

6.1.2 고려사항

o CISO는 정보보호 전략 수립, 조직 구성 및 운영, 위험관리 등 거버넌스 업무 대부분의 최종 책임과 수행 책임이 있으므로, CEO의 전폭적인 지지 및 타 임원들과의 원활한 의사소통을 통해 해당 업무 수행의 효과성을 극대화할 수 있다.
o CISO는 중복투자 및 타 조직과의 갈등을 최소화하기 위하여 정보보호 전략 및 계획, 정책 수립, 취약점 진단 및 위험평가 결과와 대책 수립, 정보보호 사고 대응 시 CEO

보고 전에 타 임원들과의 사전 협의를 통해 보고 내용을 조정할 필요가 있다.

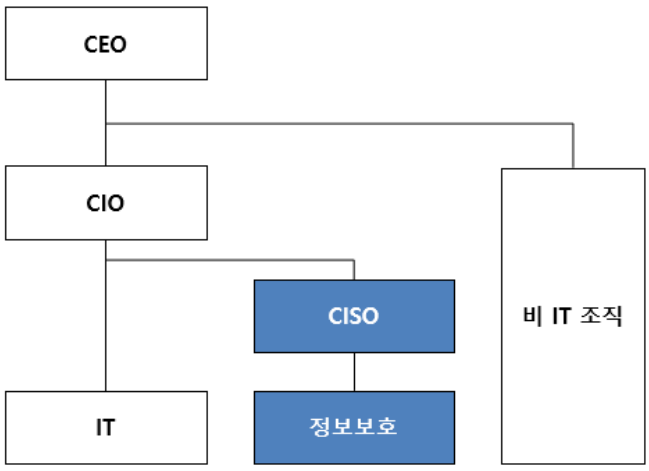
- o CISO는 정보보호 예산 확보, 정보보호 감사, 정보보호 대책 구현 등 업무에 대한 수행 책임을 공유하므로, 타 임원과의 원활한 소통 및 협업을 위해서 CISO의 직급은 C레벨의 임원으로 지정하는 것이 바람직하다.
- o CEO 및 C레벨 임원들과의 소통 시에는 법규준수 측면보다는 위험 관리 기반의 소통 역량이 필요하다. 즉, 단순히 법규준수를 위한 정보보호 활동이 아닌 정보보호 대책이 미흡할 시 회사에 재무적, 운영적으로 어떠한 위험이 존재하며, 어느 정도의 부정적인 영향을 미치는지 설명할 수 있어야 한다.
- o 취약점 분석평가는 부분적인 위험관리 활동으로, 전사적 정보보호를 위해서는 비즈니스를 고려한 전사적 정보보호 위험 식별 및 평가를 기반으로 정보보호 대책을 선정하는 업무가 수행될 필요가 있다.

6.1.3 중소 금융회사 참고사항

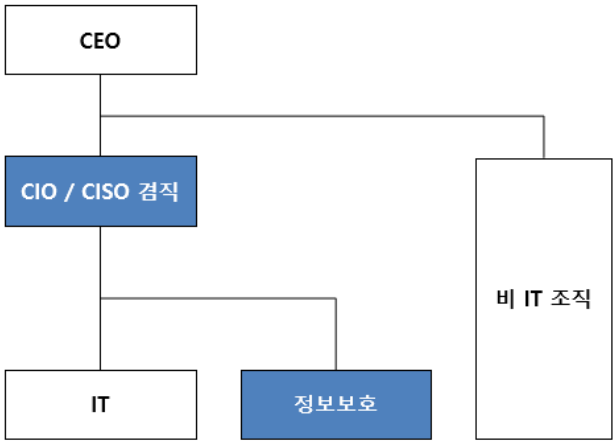
정보보호 수준이 상대적으로 낮은 중소 금융회사의 경우 단편적인 정보보호 대책 수립보다는 CEO의 적극적인 지원 하에 정보보호 위협, 취약점, 위험을 고려한 중장기 정보보호 전략을 우선 수립하여 단계적으로 정보보호 수준을 향상 시킬 필요가 있다.

6.2 IT조직 산하

전자금융거래법 시행령 제11조의3제2항에서는 직전 사업연도 말을 기준으로 총자산이 10조원 이상, 상시 종업원 수가 1,000명 이상인 금융회사에서는 CISO가 CIO를 겸직할 수 없도록 규정하고 있다. 하지만 (그림 7-2)와 (그림 7-3)과 같이 CISO가 IT 조직 산하에 존재하거나 중소규모 금융회사의 경우 CISO가 CIO를 겸직하여 정보보호 업무와 IT 업무를 담당하는 조직의 구성이 존재한다.



(그림 7-2) IT 조직 내 CISO 조직



(그림 7-3) IT 조직 내 CIO/CISO 겸직

6.2.1 특징

o 기술적 침해사고(디도스, 악성코드 감염, 해킹 등) 대응 등 비상대응 업무의 신속한 처리 가능
o 인프라, PC 보안 등 정보보호 대책구현 및 운영 업무의 원만한 수행이 가능
o CEO에게 보고 시 정보보호 이슈 중 일부 사안이 누락될 수 있음
o IT 운영 업무에 대한 점검 또는 감사가 제한되며, 발견된 문제의 축소 또는 은폐가 가능함
o 정보보호 업무가 IT 업무보다 우선순위에 밀려 정보보호 활동 제한
o 기술적 대책 중심의 정보보호 대책 수립으로 관리적, 물리적 정보보호 대책 수립 및 운영에 제약

6.2.2 고려사항

o CISO는 CIO와 정보보호 대책구현 및 운영 업무에 대한 최종 책임 또는 수행 책임을 공유하므로, IT 조직과의 갈등을 최소화하기 위해서는 정보보호 업무와 IT 업무를 명확히 구분할 필요가 있다.
o 정보보호 업무의 우선순위가 IT 업무의 우선순위보다 낮아질 수 있으므로, CEO 및 CFO는 정보보호 위협, 취약점, 위험 등을 고려하여 요구되는 정보보호 대책과 예산의 적절성을 객관적으로 검토해야 한다.
o 정보보호 전략, 계획 및 정책 수립, 취약점 진단 및 위험평가 결과와 대책 선정, 침해사고 대응 등의 업무는 CISO가 CIO에게 보고한 후 CIO가 CEO에게 보고하는 체계 보다는 CISO가 CIO와 검토 후 CISO가 CEO에게 직접 보고할 수 있는 체계를 구축할 필요가 있다.
o IT 운영 업무에 대한 점검 또는 감사가 제한되며, 발견된 문제의 축소 또는 은폐가 가능하므로, 감사조직은 주기적으로(연 1회 이상) 정보보호 및 IT 업무에 대한 감사를 수

행하여 투명성을 보증할 필요가 있다.

o CISO는 조직의 정보보호 위험 대비 구현된 대책 수준을 검토하여 전담조직 구성 및 CIO 조직과의 분리를 위한 객관적인 평가자료를 작성할 필요가 있다.

o CISO가 CIO 겸직 시 개인정보보호 정책 및 대책은 CISO가 CPO 등 타 임원 및 조직과 협의하여 수립하고, 통제의 운영은 관련 부서에서 수행한다.

6.2.3 중소 금융회사 참고사항

o 정보보호 조직이 파트로 존재하는 경우, 정보보호 전담인원을 최소 2명(기획, 운영)이상 편성하고, IT 업무 직원만으로 구성하지 않는다. (단, 예산 부족 시 단기간 동안 IT 조직의 임직원이 정보보호 업무를 병행할 수 있다.)

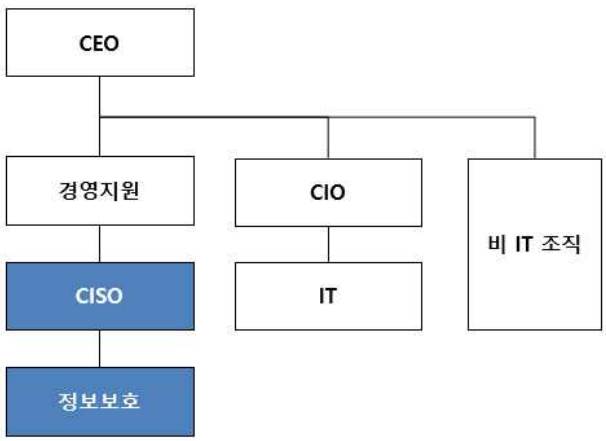
o CISO가 CIO 겸직 시 개인정보보호 정책 및 대책은 CISO가 CPO 등 타 임원 및 조직과 협의하여 수립하고, 통제의 운영은 관련 부서에서 수행한다.

o 규모가 작은 금융회사의 경우 정보보호 전담인력과 IT 인력의 직무순환 등을 통해 정보보호 및 IT 운영 역량을 향상시키고, 상황에 따라 탄력적으로 인력을 배치 및 운용할 수 있다.

o 규모가 작은 금융회사의 경우 CISO가 CIO 겸직 시, 정보보호 대책 수립 및 운영에 집중할 수 있도록 CPO 겸직을 제한할 필요가 있다.

6.3 경영지원 조직 산하

경영지원 조직은 재경, 전략 및 기획, 인사, 총무, 홍보 등 금융회사의 원활한 운영을 위한 지원 업무를 수행하는 조직을 포괄하며, (그림 7-4)와 같이 CISO가 경영지원 조직의 장이거나 경영지원 조직에 소속되어 조직장에게 보고하는 형태를 구성할 수 있다.



(그림 7-4) 경영지원 조직 내 CISO 조직

6.3.1 특징

o 비즈니스 요구사항의 반영 및 사업전략과 정보보호 전략의 연계
o 정보보호 예산 확보 및 집행이 용이함
o 정보보호 규정 위반자에 대한 징계조치가 용이함
o 인적보안, 출입통제 등 비IT 정보보호 통제의 운영 업무가 용이함
o 침해사고 대응 훈련 시 인사, 총무, 홍보 등 비IT 부서의 참여율 향상 가능
o IT 부서와의 협업 및 기술적 침해사고 대응이 어려울 수 있음
o 정보보호 업무가 단순 지원업무에 그칠 수 있음

6.3.2 고려사항

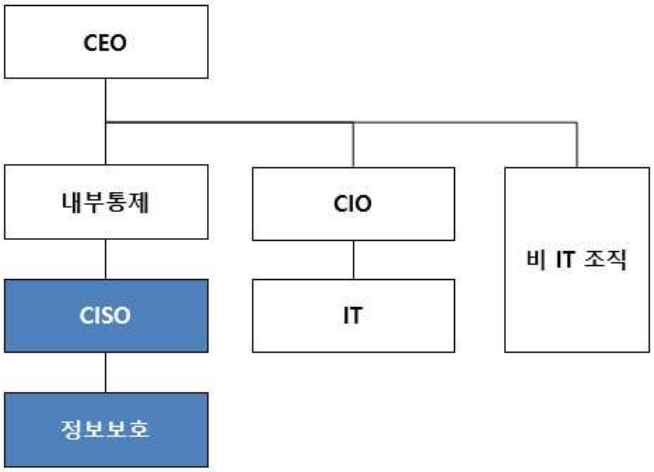
o CISO는 정보보호 관련 법규 및 정책 위반자에 대한 징계 요구를 위하여 위반의 고의성, 파급효과 등 객관적인 기준을 마련할 필요가 있다.
o CISO는 중장기 정보보호 전략 및 계획 수립, 취약점 진단 및 위험평가 결과와 대책 선정, 침해사고 대응 등의 업무와 관련하여 경영지원 조직장 또는 CEO에게 보고 전 CIO와의 사전 협의를 통해 보고 내용을 조정할 필요가 있다.
o CISO는 정보보호 정책 수립 시 CIO와의 충분한 협의가 필요하며, 정책 이행을 위한 명확한 역할 및 책임을 정의해야 한다.
o IT 조직과의 업무 분장 시 정보보호 시스템 도입 및 운용은 CISO 조직에서 담당하고, 정보보호 시스템의 운영(장애조치, 성능관리, 백업 등)은 IT 조직에서 담당할 수 있다.
o CISO는 CIO와 협의를 통해 서버, 네트워크 등 단말기 및 인프라와 관련된 기술적 정보보호 대책을 수립하고, 통제의 구현 및 운영은 IT 조직에서 담당할 수 있다.
o 정보보호 업무가 단순 지원업무라고 인식될 수 있으므로, 정보보호 전략이 비즈니스 전략에 포함될 수 있도록 전략 및 기획, 홍보 부서 등과의 유기적인 협업이 중요하다.
o 출입통제시스템 운영 등 출입통제 업무를 총무부서에서 수행하는 경우, 정보보호 부서와 총무부서 간 탄력적 인력 운용을 고려할 수 있다.

6.3.3 중소금융회사 참고사항

o 규모가 작아 정보보호 전담조직 구성에 제한이 있는 경우, 정보보호 기획 및 운영 업무를 위한 최소 2명 이상의 전담인력을 배치하고, 인적보안은 인사부서, 물리적 보안은 총무부서, 기술적 보안은 IT 부서의 파트에 소속된 인원이 수행할 수 있다.

6.4 내부통제 조직 산하

(그림 7-5)와 같이 CISO가 감사, 준법감시, 법무 등 내부통제 기능을 수행하는 조직의 장이거나 해당 조직에 소속되어 정보보호 조직을 구성할 수 있다.



(그림 7-5) 내부통제 조직 내 CISO 조직

6.4.1 특징

o 정보보호 감사 등 내부통제 관련 업무의 원활한 이행
o 법적 문제에 신속하게 대응 가능
o CISO와 CPO 겸직 시 정보보호 및 개인(신용)정보보호 업무의 시너지 효과 발생
o IT 부서와의 협업 및 기술적 침해사고 대응이 어려울 수 있음
o 임직원의 정보보호에 대한 부정적 인식 발생 및 확산 가능

6.4.2 고려사항

o 법규 준수를 위한 정보보호 대책 수립이 아닌 정보보호 위험 관리 기반의 대책이 수립될 수 있도록 인식을 전환한다.
o CISO는 정보보호 정책 수립, 정보보호 위험관리, 정보보호 대책구현 시 정보보호 업무와 개인(신용)정보보호 업무 중 중복되는 업무를 식별하여 비용 효과적으로 대책을 수립하고 운영한다.
o CISO가 CPO를 겸직하는 경우, 정보보호 정책 수립, 개인(신용)정보보호 대책구현 및 운영 업무와 관련하여 CIO와의 충분한 협의가 필요하며, 정책 이행을 위한 명확한 역할 및 책임을 정의해야 한다.
o CISO가 정보보호 감사 계획을 수립하여 정보보호 조직이 이를 이행하거나 감사조직의 정보보호 감사 수행 시 CISO가 정보보호 인력을 파견할 수 있다.
o 임직원의 정보보호에 대한 부정적 인식을 전환하기 위하여 긍정적인 정보보호 문화 형성 및 유지와 관련된 업무를 수행할 필요가 있다.

6.4.3 중소금융회사 참고사항

o 정보보호 인력 부족에 따라 CISO가 자체적으로 정보보호 감사가 어려울 경우 외부 기관에 의뢰하여 정보보호 감사를 수행할 수 있다.
o 규모가 작은 금융회사의 경우 CISO가 CPO 겸직 시 정보보호 및 개인(신용)정보보호 업무에 집중할 수 있도록 CIO를 겸직을 제한할 필요가 있다.

7 정보보호 협력체계

전사적 정보보호를 위해서는 정보보호 전담조직 뿐만 아니라 전사의 각 조직에서 정보보호 업무를 수행해야 하므로, 소통 및 협업이 필수적이라 할 수 있다. 따라서 원활한 의사결정을 위한 위원회와 협의체의 수립 및 운영이 요구되어지며, 업무상 발생하는 갈등을 최소화할 필요가 있다.

7.1 정보보호위원회

전자금융감독규정 제8조의2제1항에 의거하여 금융회사는 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.

7.1.1 구성 및 역할

전자금융감독규정 제8조의2제2항에 의거하여 정보보호위원회는 아래의 사항을 만족해야 한다.
o 정보보호위원회의 장은 CISO로 임명한다.
o 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.

또한 정보보호 위원회는 전자금융감독규정 제8조의2제3항에 의거하여 아래의 사항을 심의·의결하여야 한다.
o 전자금융거래법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항
o 전자금융거래법 제21조의2제4항제1호에 관한 사항(전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립)
o 전자금융거래법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항
o 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항
o 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항

7.1.2 고려사항

정보보호가 발달되어 있는 국가의 경우 전사적인 주요 보안 이슈에 관해 신속하고 정확한 의사결정, 결정한 사항에 대한 실행력 강화, 실행 결과에 대한 지속적인 후속 조치를 위하여 정보보호위원회의 장은 CEO가 맡고 CISO는 간사역할을 수행하며 CIO, CPO 등 C레벨의 임원들이 위원으로 구성되는 경우가 다수이다. 전자금융감독규정은 최소한의 요건이며, 규정의 취지에 맞게 정보보호 위원회를 운영하기 위해서는 아래와 같은 방안을 권고한다.

- o 위원장은 CEO, 안건 상정 등 위원회 운영은 CISO가 맡고, CIO, 준법관리인, 신용정보관리인, 현업 임원 등 C레벨 이상의 임원이 참석한다.
- o 위와 같은 운영에 제한일 있을 경우, CEO 등 C레벨 임원들이 참석한 위원회에 CISO가 정보보호 관련 안건을 상정하고 임원들이 심의·의결한다.
- o 정보보호위원회의 안건은, 참여한 임원들이 의견을 개진할 수 있도록 기술적인 내용보다는 경영적 측면에서 전사적인 정보보호 의제를 다룬다.

7.2 정보보호실무협의체

정보보호위원회의 하부 조직이자, 실무책임자급의 소통과 협업을 위한 기제 역할을 하는 실무조직이 필요하다. 또한 정보보호 관련 주요 이슈가 발생하였을 때 상시적으로 전사적 대응을 위해 정보보호실무협의체 운영이 요구된다.

7.2.1 구성 및 역할

정보보호실무협의체의 장은 정보보호 전담부서장이 맡고, 과·차장급 전담인력이 간사 역할을 수행한다. 협의체의 구성은 IT, 인사/총무 등 경영지원, 준법, 현업 부서의 팀장급으로 구성한다. 회사에 따라 부서장(팀장)을 대신하여 과·차장의 관리자가 참여할 수 있으며, 안건에 대한 전문성 및 권한을 갖고 있어서 실무적인 결정을 할 수 있는 실무책임자가 참여하는 것이 중요하다. 또한, 정보보호실무협의체는 아래와 같은 역할을 수행한다.

- o 정보보호 정책 수립, 정보보호시스템 도입, 정보보호 인증 등 전사적 정보보호 업무에 대한 의견 제시 및 조정
- o 침해사고 등 정보보호 이슈에 대한 대응
- o 정보보호위원회 의제에 대한 최종 점검 및 의결사항에 대한 전파 및 이행

7.2.2 고려사항

정보보호위원회는 주기적으로 개최하는 반면 정보보호 실무협의체는 이슈 발생 시 상시 개최가 필요하다. 또한, 최고경영층의 합리적인 의사결정을 위해서는 현업의 의견이 적극적으로 반영되어야하기 때문에 실무적인 소통과 협업이 중요하다.

7.3 갈등 조정

비즈니스의 복잡성 증가, 새로운 기술의 등장 등 비즈니스 및 정보보호 환경 변화에 따른 전사적 정보보호 활동은 조직 또는 부서 간 갈등을 수반한다. 갈등 조정은 정보보호 거버넌스의 주요 업무 중 하나이며, 갈등 및 업무 조정을 통해 정보보호 활동의 효율성 및 효과성을 보장할 필요가 있다.

갈등 조정을 위해서는 관련 조직 또는 부서 간 업무에 대한 이해와 사전 협의를 전제로 하고, 법규 제·개정, 신기술 및 신규 위협 등장 등 주요 변경사항과 요구되는 대책을 주기적으로 공유하고 논의할 필요가 있다. 정보보호 업무와 관련된 갈등 해소를 위해 업무 조정이 필요한 경우(실무자 간 협의를 통해 갈등 해결이 불가능한 경우 포함), 정보보호 실무협의체에서 역할 및 책임을 논의한 후 정보보호위원회에 안건을 상정하여 심의·의결하는 것을 권고한다. 이 표준에서는 해외 정보보호 거버넌스 가이드 및 국내 금융회사의 갈등 조정 사례에 대한 설문조사를 기반으로 <표 8-1>과 같이 정보보호 업무 관련 갈등 조정 방안을 제시한다.

<표 8-1> 정보보호 업무 관련 갈등 조정 방안

구분	주요 내용
정보보호와 IT	정보보호 정책의 제·개정 전 IT 인프라 및 운영 현황을 이해하고 일방적인 통제·대책의 적용을 요구하지 않는다.
	정보보호시스템 관련하여 운영 업무와 운용 업무를 명확히 구분한다.
	정보보호 인력과 IT 인력의 직무순환을 통해 정보보호 및 IT 역량을 강화하고 탄력적으로 인력을 운용한다.
	정보보호 및 IT 목표가 아닌 비즈니스 목표 달성을 접점으로 인식하여 갈등을 조정한다.
	필요에 따라 조직 통합 시 내부감사를 통해 정보보호 대책의 수립 및 운영에 대한 투명성을 보장한다.
정보보호와 개인(신용)정보보호	정보보호 업무와 개인(신용)정보보호 업무를 명확히 구분한다.
	정보보호 정책의 제·개정 시 개인(신용)정보보호 요구사항을 고려하여 중복투자를 예방하고 갈등 발생을 최소화 한다.
	개인(신용)정보보호 시스템의 운영 업무와 운용 업무를 명확히 구분한다.
	필요시 CISO가 CPO를 겸직하여 통합적인 관점에서 업무를 조정한다.
정보보호와 감사	정보보호 감사의 범위와 대상을 명확히 정의한다.
	CISO 조직이 감사 권한을 보유한 경우, 감사 조직의 일정을 참고하여 정보보호 감사 계획을 수립·이행한다.
	CISO 조직에 감사 권한이 없는 경우, 감사 조직의 계획에 정보보호 감사를 추가하거나 감사 시행 시 정보보호 인력을 파견할 수 있다.
정보보호와 현업	정보보호 정책의 제·개정, 신규 정보보호 시스템의 도입 등 협업부서의 불만이 예상되는 경우, 사전 공지 및 교육을 통해 변경사항의 필요성과 적정성을 인지할 수 있도록 한다.
	단순히 법규 준수뿐만 아니라 관련 위험이 비즈니스에 미치는 영향을 충분히 설명해야 하며, 대책 수립 시 업무 효율성과 보안수준의 균형을 고려하였음을 제시한다.

부 록 Ⅰ-1
지식재산권 확약서 정보

- 해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 이 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2
시험인증 관련 사항

- 해당 사항 없음

부 록 Ⅰ-3
이 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4
참고 문헌

[1] ISO/IEC 27014:2013, Information technology-Security techniques-Governance of information security
[2] 강현식, 김정덕, 정보보호 전담조직 편성모델에 관한 연구, 한국전자거래학회지 20(2), pp.167~174, 2015.
[3] 금융보안연구원, 해외 정보보호 거버넌스 우수 구축 사례 조사, 2011.
[4] Carnegie Mellon CyLab, Governance of Enterprise Security: CyLab 2012 Report, 2012.
[5] Gartner, Information Security and Risk Governance: Functions and Processes, 2011
[6] Gartner, Managing Risk and Security at the Speed of Digital Business, 2016.
[7] Georgia Tech Information Security Center, Governance of Cyber security: 2015 Report, 2015.

부 록 Ⅰ-5
영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6
표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12		효과적인 정보보호거버넌스를 위한 금융보안 조직체계	PG504