AGR-VII-2019-②-142

금융보안 거버넌스 가이드

2019. 12.

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

◩ 가이드 제·개정 이력

버전	발행연월	주요내용	비고
Ver 1.0	2015.4월	- 최초 제정	
Ver 2.0	2017.3월	- 법규 개정 내용 반영	가이드 통합본 제작
Ver 3.0	2019.12월	- 법규 개정 내용 반영	

AGR-VII-2019-②-142

금융보안 거버넌스 가이드

2019. 12.

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

목 차

금융보안 거버넌스 가이드

금융보안 거버넌스 7대 기본원칙

❶ 정보보호 활동을 수행하는 핵심 플레이어들에 대한 명확한 역할 정의와 그에 따른 권한 및 책임 부여

❷ CEO의 올바른 의사결정을 위해 정보보호 활동 결과가 누락 없이 전달될 수 있는 보고체계 수립

❸ 조직의 위험 감소 및 완화를 위해 특정 영역이 아닌 전사적 위험 관리 체계 확립

❹ 현재 정보보호 활동 수준과 앞으로 나아갈 방향에 대해 최고경영층의 이해를 돕기 위한 방법 제시

❺ 정보보호 활동의 시너지를 극대화하기 위한 최고경영층 간, 실무조직 및 현업조직과의 수평적·수직적 소통 강화

❻ 계획적이며 안정적인 정보보호 활동을 위한 정보보호 예산 수립·집행 및 적절한 전담인력 배치

❼ 조직의 평판과 정보보호의 선순환 구조를 위한 정보보호 문화 확립

역할 매트릭스

구분	CEO	CISO(실무조직)	CIO(실무조직)	CPO	준법감시인, 감사
정보보호 거버넌스	• 정보보호 전담 조직 구성 보장 • CISO(정보보호 최고책임자) 지정 • 사업계획 승인 및 성과 평가 • 최고경영층의 소통 지원	• 정보보호 사업 계획 수립 및 평가 • 정보보호위원회의 위원장 역할 수행 • 최고경영층과의 소통을 통해 타 부서의 정보보호 활동 지원	• 최고경영층과의 소통 적극 참여 • 정보보호 조직의 구성 및 사업 계획에 대해 협조	• 최고경영층과의 소통 적극 참여 • 정보보호 사업 계획 중 개인정보 보호 계획에 대한 협조	• 최고경영층과의 소통 적극 참여
정보보호 관리	• 정보보호 정책 승인 • 전사적 위험관리 승인	• 정보보호 정책 수립 및 평가 • 전사적 위험관리 수립 및 평가 • 정보보호 교육 및 훈련	• 정보보호 역할 및 책임 규정을 관련 부서와 협력 • 전사적 위험관리 방안 관련부서와 협력	• 정보보호, 위험관리 등의 개인정보 관리를 위한 협력	• 정보보호 정책 협력 • 전사적 위험관리 방안 협력
정보보호 보증	• 법규, 내규 준수 및 감사 활동 보장	• 규제 대응 및 관련 부서와 협력 • 보안감사 수행 지원	• 규제 대응 협조 • 보안감사 협조	• 규제, 감사 대응 및 협조	• 규제 대응 및 협력 • 보안감사 계획 및 수행
정보보호 대책 구현 및 운영	• 정보보호 대책 구현 및 운영될 수 있도록 보장	• 물리적·환경적 보안, 접근통제, 운영보안, 전자금융거래 보안, 외부주문 보안, IT 도입·개발·유지보수시 정보보호 대책 구현 및 운영	• 통제(접근, 서버, SW, 외주개발 등), 전자금융거래 기록관리, 정보보호 대책을 반영한 IT·정보보호시스템 운영	• 정보보호 대책 중 개인정보 관련 협조 • 개인정보영향평가 결과에 대한 평가	-
정보보호 비상대응 및 대비	• 서비스의 비상대응 및 대비가 될 수 있도록 보장	• 위험에 대한 업무 연속성 확보 방안 수립 및 평가 • 사고 대응 및 협력	• 위험에 대한 업무 연속성 확보 방안 수립 협력 • 사고 대응 및 협력	• 개인정보 사고 관련 대응 및 대비에 대한 협조	-

제1장 금융보안 거버넌스 개요

1 배경 및 목적

❐ **최근 금융 IT 환경의 변화 및 국내·외 금융 보안사고가 지속적으로 발생함에 따라 금융보안 위험에 대한 효과적인 관리가 필요**

○ 지난 금융전산망 마비사고, 카드사 고객정보 유출사고 등에서 알 수 있듯이, 보안이 전제되지 않고서는 그 어떤 편의성과 효율성도 담보할 수 없음

○ 뿐만 아니라, 보안사고가 발생하는 경우 집단 소송으로 인한 금전적 피해와 고객 이탈, 평판 실추, 대외 신뢰도 하락 등 무형의 피해도 발생할 수 있음

○ 보안사고 발생 시 신속한 복원력(Resilience) 향상을 위한 전사적인 정보보호 거버넌스 구축도 요구되고 있음

❐ **국내 금융권의 보안 수준은 전자금융거래법, 전자금융감독규정 등에 대한 최소한의 법규 준수 활동에 머물러 있으며, 그 이상의 수준을 향상시키기 위한 노력은 다소 부족한 것이 현실**

○ 이는 금융회사 전반에 걸쳐 보안에 대한 인식이 여전히 비용의 관점에서 바라보는 경향이 많고, 보안은 보안 전담부서 또는 정보보호최고책임자(CISO)만의 역할로 인식하는 것이 근본 원인

○ 최소한의 법규 준수 활동만으로는 날로 지능화·고도화되는 보안위협에 대한 효과적인 대응이 어려우며, 금융회사별로 보안수준이 차별화되기 보다는 하향 평준화될 가능성이 높음

❐ **이러한 이유로, 이미 해외에서는 보안 문제를 더 이상 정보보호(보안) 부서 또는 기술적 관점이 아닌 기업 거버넌스 관점에서 전사적 차원의 보안 강화를 추진**

○ 이를 통해 최고경영층을 중심으로 Top-Down 방식의 강력한 보안 강화 추진이 가능하며, 보안사고 발생 시 신속한 사이버 복원력(Resilience)이 향상되어 이용자 보호 및 금융회사의 피해 최소화에 효과적임

▶ 금융회사의 보안위험을 완화하기 위해 금융권 업무 특성을 반영한 효과적인 금융보안 거버넌스의 도입을 권고

2 금융보안 거버넌스 개념

❒ **거버넌스(Governance)란, 통상적으로 정부가 주도하는 통치(Government)가 아닌 다양한 이해관계자들의 파트너십에 의한 협치(協治)를 말하며, 사용되는 분야에 따라 조금씩 다른 의미를 내포**

거버넌스

▶ 경영학
- 주주, 종업원, 거래 기업, 지역사회 등 회사 관련 이해관계자들의 이해를 조정하여 의사결정, 결정된 사항의 집행 및 감시 감독

※ 기업 거버넌스(Corporate Governance)

▶ 행정학
- 정보의 의사결정 과정에 모든 민간 이해 당사자들이 참여하는 새로운 국가 통치 및 관리방식

❒ **금융보안 거버넌스란, 금융권의 업무 특성을 반영한 정보보호 거버넌스를 의미하며, 정보보호 거버넌스 개념은 현재 국제표준(ISO 27014)에서 규정**

정보보호 거버넌스

▶ 정보보호 거버넌스(ISO 27014) : 2013년 제정
- 정보보호에 대한 최고경영층의 의사결정 권한과 책임, 비즈니스와의 전략적 연계, 컴플라이언스 보장을 위해 지켜야 할 원칙과 수행해야 할 활동 및 과제를 정의한 문서

○ 정보보호 거버넌스란, 조직 전반에 걸친 정보보호 목표를 달성하기 위해 전략 및 정책을 통한 지시(Direct)와 성과 모니터링을 통한 통제(Control) 활동을 수행하기 위한 “이사회와 최고경영층의 역할 및 책임”으로 정의

- 즉, 금융회사의 전사적인 금융보안을 위해 최고경영층과 실무조직, 현업조직 간의 상호 협력을 통한 적극적인 정보보호 활동
- 또한, 적절한 역할 정의를 통해 책임을 분배하고 권한을 부여하여 해당 역할에 충실히 수행할 수 있게 해야 함

○ 이러한 정보보호 거버넌스가 궁극적으로 추구하는 목표는 다음과 같음

- (첫째) 정보보호의 목표를 조직의 목표와 전략적 연계
- (둘째) 최고경영층과 정보보호 관련 이해관계자들에게 정보보호의 비즈니스 가치를 전달
- (셋째) 정보보호 관련 위험이 조직 내 적절한 수준으로 관리되고 있으며, 정보자산에 대한 책임추적성을 보장

❐ 금융권에 정보보호 거버넌스가 구축되는 경우, 가질 수 있는 기대 효과는 다음과 같음

○ 금융회사의 정보보호 효과성 확보로 정보보호 인력 및 예산 등에 대한 자발적인 보안 투자 유도

- ❍ 중복과 불필요한 보안 프로세스 통합으로 정보보호 업무 효율성 개선
- ❍ 전사적으로 정보보호 거버넌스를 문화로 인식하여 업무 수행시 자연스럽게 정보보호 활동을 위해 노력
- ❍ 비즈니스 연속성 확보를 통한 투자자와 이해관계자 등의 신뢰 확보

제2장 금융보안 거버넌스 환경 변화

1 금융보안 패러다임 변화

❒ **전세계적으로 정보보호 패러다임은 기술적 관점에서 관리, 제도화 단계를 지나 정보보호 거버넌스 단계로 진입**

〈 정보보호 패러다임의 변화 〉

Step 01 Wave : **Technology**	[50년대 후반 ~ 80년대 초반]
Technical issues by techies	Built in facilities of mainframe OS
Step 02 Wave : **Management**	[80년대 초반 ~ 90년대 중반]
Distr. Computing, Internet, WWW, Ec	Top Mgmt involvement, ISSO, Organization
Step 03 Wave : **Institutionalization**	[90년대 후반 ~ 2002년]
Corporate wide effort	Int'l std, certification, culture, measurement
Step 04 Wave : **Infosec Governance**	[2002년 ~ 현재]
Corporate governance, Legal & regulatory compliance	Mgmt and leadership of the Board and Top Mgmt

〈자료출처 : Computers and Security, 2006〉

❒ **금융보안 정책이 사전규제 중심에서 금융회사가 스스로 보안을 책임지는 자율보안체계 확립에 중점**

○ 최근 금융당국은 금융회사의 기술 자율성 제고를 위해 반드시 필요한 조치만 규율하는 방향으로 법률 개정

- 기존 기술적 조치 의무를 세세하게 규율하던 태도는 지양

○ 관련 규제의 변경 추이를 살펴보면, 금융회사의 자율성 제고를 위한 개정사항이 포함

- 전자금융거래와 단말기 보호를 위해 금융회사가 자율적으로 보호 대책을 마련하도록 규정
- 금융회사의 IT·정보보호 부문의 인력 및 예산에 대한 규제(일명 557 규제)의 효력 일몰(`20.1.1.)

○ 한편, 금융회사의 자율성을 보장하는 대신 보안사고 발생시, 금융회사에 엄정한 책임을 부과

- 금융회사에 대한 징벌적 과징금, 양벌규정 책임주의 원칙, 안전조치 미조치 시 과태료, 데이터 유출시 형사처벌 등 도입

❐ 금융권 디지털 전환이 가속화됨에 따라 금융산업의 패러다임이 변화하고 있으며, 금융혁신 서비스에 대한 안전성 확보 요구도 증가

○ 금융 결제 인프라 개방에 따라 ICT 기업 등도 금융업에 진출하여 전자금융서비스 제공자가 확대

○ IT 新기술을 악용하는 공격 기법이 등장하고 금융권에 대한 사이버 위협이 지속됨에 따라 안전한 전자금융서비스 환경 구축 필요

○ 과거와 같은 인식 즉, 보안 업무가 IT 부서 또는 보안부서의 전담업무로 인식하는 것은 이러한 변화의 흐름을 역행

- 즉, 보안 문제는 기술적 해결책만으로는 한계가 있기 때문에 거버넌스 차원의 접근이 필요하고, 이사회, 최고경영층 별로 역할 및 책임 배분이 중요

❐ CISO 임원 지정 및 겸직금지, IT·정보보호 인력 및 예산 책정 등의 거버넌스 이슈는 규제가 아닌 금융회사의 자율적인 방식으로 진행될 필요

○ 금융회사는 법규에서 규정한 거버넌스 이슈에 대해 단기적 관점이 아닌 중장기 관점에서 본질적인 체질 개선이 필요

- 주요 거버넌스 이슈로 직급별·부서별 보안 역할 및 책임 배분, IT·정보보호 인력 및 예산 책정, 보안전담부서 구성 및 CISO 지정, 보안위험 관리, 보안 문화 및 교육 등이 존재

[참고]

관련 법규(제재) 현황

❒ **금융회사 최고경영자의 보안 업무(전자금융감독규정 2014.1.1.)**

- 임직원들의 정보보안 법규 준수여부에 대한 정기점검 결과를 정보보호최고책임자로부터 보고 받음
- 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영
- 정보보호위원회 심의·의결사항을 정보보호최고책임자로부터 보고 받음
- 전자금융거래법 제21조제4항에 따라 매년 금융위원회에 제출해야 하는 정보기술부문에 대한 계획에 확인·서명
- 정보보호교육을 실시한 이후 대상 임직원에 대해 평가 실시
- 취약점 분석·평가에서 도출된 보안 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우 위험수용 여부 승인
- 취약점 분석·평가 결과에 따른 이행계획 실시 결과를 정보보호최고책임자로부터 보고 받음

❒ **정보보호최고책임자 지정 요구(전자금융거래법 2012.5.15.)**

- 전자금융업무 및 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자 지정 의무화(총자산이 2조원 이상이고, 상시 종업원 수가 300명 이상이면 임원으로 지정)

❒ **양벌규정 책임주의 원칙 반영(전자금융거래법 2012.5.15.)**

- 위반 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형 부과 (상당한 주의와 감독을 게을리하지 않은 경우에는 제외)

❒ 금융보안 규제 강화 현황(전자금융거래법 2015.4.16.)

• 징벌적 과징금 제도 도입

구분	과거	현행
제21조(안전성의 확보의무) 제1~2항 위반시	6개월 이내의 업무정지 또는 5천만원 이하의 과징금	동일
제21조(안전성의 확보의무) 제1~2항 위반 및 전자금융거래 정보 타인 제공 또는 누설, 업무상 목적 외 사용시	-	(신설) 50억원 이하의 과징금 부과

• 정보보호최고책임자의 겸직 제한

구분	과거	현행
제21조의2(정보보호 최고책임자 지정)	-	(3항 신설) 총자산, 종업원 수 등을 감안 정보보호최고책임자의 정보기술부문 업무 겸직 제한

• 데이터 유출 행위 등에 대한 벌칙 강화

구분	과거	현행
제21조의4(전자적 침해행위 등의 금지) 위반자	7년 이하의 징역 또는 5천만원 이하의 벌금	10년 이하의 징역 또는 1억원 이하의 벌금
26조(전자금융거래정보의 제공 등) 위반자	5년 이하의 징역 또는 3천만원 이하의 벌금	10년 이하의 징역 또는 1억원 이하의 벌금

• 안전성 확보 의무 불이행시 과태료 부과

구분	과거	현행
제21조(안전성의 확보의무) 위반시	-	(제1항 또는 제2항) 5천만원 이하의 과태료 (제4항) 1천만원 이하의 과태료

대규모 금융보안사고 발생 사례

• 신용카드 3개사 손실 및 제재 현황

구분		A사	B사	C사
유출건수		5,419만건	2,677만건	2,688만건
영업수익 손실(추정)		445억7천만 원	338억 원	289억5천만 원
소송자수 현황		108,433명 ('14.10 기준)	69,849명 ('14.10 기준)	70,933명 ('14.10 기준)
임직원 제재 조치	임원	해임권고 상당 1명, 주의적경고(상당) 2명, 주의 상당 1명	주의적경고(상당) 2명	해임권고 상당 1명, 문책경고 1명, 주의적경고 상당 2명
	직원	면직 상당 1명, 정직 3월 1명, 감봉 3월(상당) 6명, 견책(상당) 4명, 주의 1명, 퇴직자 위법사실통지 2명, 기타 관련직원 조치의뢰	정직 1명, 정직(상당) 1명, 감봉 2명, 감봉(상당) 3명, 기타 관련직원 조치의뢰	면직 상당 1명, 정직 3월 4명, 감봉 3월 5명, 감봉 3월 상당 2명, 견책 3명, 견책 상당 1명, 기타 관련직원 조치의뢰
기관 제재조치		업무일부정지 3개월 및 과태료 600만원 부과	업무일부정지 3개월 및 과태료 600만원 부과	업무일부정지 3개월 및 과태료 600만원 부과
카드재발급 비용		약 68억원 (약 223만건)	약 70억원 (약 199만건)	약 76억원 (약 160만건)
고객통보 우편발송		약 101억원	-	약 18억원
콜센터 추가운영		약 11억원	약 39억원	약 14억원

[전자공시시스템], [국감 보도자료, 김상민의원실]

2 금융보안 거버넌스 주요 이슈

❒ **금융보안의 패러다임이 변화하고 있지만 언론, 금융회사 인터뷰 등의 조사를 통해 이러한 변화에 모든 금융회사가 적절하게 대응하고 있지 못한 것으로 나타남**

❒ **금융회사는 변화에 따른 금융보안 거버넌스 확립을 위해 거버넌스 주요 이슈 현황에 대한 고민이 필요**

1) 최고경영층 및 CISO의 역할과 책임이 명확하게 정의되어 있지 않으며, 직책에 맞는 권한도 부족함

- 일부 금융회사는 내규에 각각의 직무에 대해 설명하고 있지만 이마저 정확히 인지하고 있지는 못하는 경우가 다수

- 전자금융거래법에서 CISO가 CIO 업무를 겸직할 수 없도록 규율* 하고 있으나 각각의 역할 및 책임이 명시적으로 구분되어 있지 않을 경우 부서 간 충돌로 갈등이 발생할 가능성도 존재

* 총자산 10조원 이상, 상시 종업원 수 1,000명 이상인 기업 대상

2) 보고체계에 따라 정보보호와 관련한 보고가 최고경영자에게 누락되는 경우가 발생

- 위험관리 결과, 보안사고 등 조직에서 발생하는 중요 이슈가 최고경영자에게 보고되지 않아 부적절한 대응 발생

3) 디지털금융 확산 등으로 정보보호의 중요성이 더욱 강조되고 있으나 정보보호 투자에 대한 실질 예산 집행이 쉽지 않음

- 비즈니스가 정보보호보다 우선시 되는 경우가 많기 때문에 정보보호 예산 집행이 다음으로 미뤄지는 경우가 발생

- 정보보호에 대한 효과성, 효율성 등을 정량적으로 제시하기가 쉽지 않고, 가시적이지 못 한 부분들로 인한 최고경영층과의 공감대 형성이 어려움

4) 위험관리가 전사적으로 이뤄지지 않고 특정 영역에 대해서만 관리되고 있는 경우가 존재

- 전사적 위험관리가 되고 있지 않다는 것은 조직이 위험에 대해 적절하게 예방하고 대응하지 못하고 있음을 의미함

5) 최고경영층 간의 소통이 활발하지 않아 업무 진행시 어려움 발생

- 중요 정보보호에 관한 사항을 심의·의결하고 소통의 장이 될 수 있는 정보보호위원회를 운영하도록 하고 있으나 회의 개최 주기도 길고 형식적으로 운영

- 또한, 정보보호위원회 위원들이 IT·보안 부서의 부서장 등으로 구성되어 이사회에 보고되지 않는 경우가 많고 최고경영층간 소통도 미흡

6) 법규 및 내규가 관리되고 있으나 실질적으로 임직원이 인지하지 못함

- 정보보호 인식 고취를 위한 임직원 대상 정보보호 교육이 체계적이지 않아 교육의 효과성이 다소 부족함

- 정보보호에 대한 임직원의 인식 제고를 위해 상벌조항을 마련하거나 규정 위반자에 대한 인사상 조치 등을 내규화할 필요가 있으나 현실적으로 곤란

7) 법규에서 규정하고 있는 정보보호 활동만 수행하려는 경향이 여전

- 법규에서 규제하지 않은 정보보호 활동을 추진하기 위해서는 자율적인 정보보호 문화가 형성될 필요가 있으나 아직 미흡

- 효과적인 정보보호 활동을 위해 적절한 비율의 정보보호 인력 및 예산을 확보해야 하나 557 규제를 최소가 아닌 적정 기준으로 오해하고 정보보호 투자에 소극적

제3장 금융보안 거버넌스 전략

1 정보보호 활동을 위한 명확한 역할 정의, 권한 및 책임 확립

❒ **디지털 금융확대로 정보보호 리스크가 금융회사의 핵심 리스크로 부각되면서 최고경영자와 CISO 등의 역할 및 책임을 명확히 정의하고 그에 따른 합당한 권한 부여가 필요**

❒ **본 가이드는 RACI 차트를 통해 금융보안 거버넌스 핵심 플레이어들의 역할 및 책임 정의**

RACI 차트

▶ **RACI 차트란**

- 업무 프로세스 상의 부서/개인 간 업무에 대한 역할 및 책임 그리고 권한을 명확히 설명하는 차트
- 표로 누가(Who), 어떤 일(What)을 하는지를 명확히 규명함으로써 구성원간의 유기적 협력체계를 구축하여 효율적 업무 수행 가능
- 업무별로 누가 실제 수행 책임(Responsible)을 지는지, 누가 해당 업무에 대해 최종 책임(Accountable)을 지는지, 업무수행과 관련하여 협업·협의(Consulted)가 필요한 주체는 누구인지, 그리고 해당 업무 수행결과를 보고(Informed)받는 주체는 누구인지 명확히 함

구분	CEO	CISO	CIO	CPO	준법감시인/감사
정보보호 거버넌스	A/I	R	R	R	R
정보보호 관리	A/I	R	C	C	C
정보보호 보증	A/I	R	C	C	C
정보보호 대책 구현 및 운영	A/I	R	R	C(R*)	-
정보보호 비상 대응 및 대비	A/I	R	R	C	-

* 개인정보와 관련된 구현 및 운영시 R

※ 자세한 사항은 부록 참고

❒ 최고경영자의 역할 및 책임

1) 최고경영자와 CISO 등 최고경영층 간 소통의 장을 마련

- 소통의 장으로 정보보호위원회 등을 활용 가능

- 최고경영층 간의 원활한 소통을 통해 도출된 의견을 의사결정에 반영하며, 조직의 자율적 정보보호 문화 조성을 선도

2) 비즈니스를 고려한 현재와 미래의 정보보호 목표에 대한 승인 및 보장

- 이사회와의 소통을 통해 전략적인 중장기 정보보호 정책을 승인하고 동 정책이 임직원들에게 효과적으로 전달되어 달성되도록 지원

- 목표 달성을 위한 정보보호 활동 결과가 최고경영자에게 정확하게 보고될 수 있도록 정책을 마련하고 보고체계를 보장

- 효과적인 정보보호 활동을 위한 전담 조직과 인력 구성은 물론, 정보보호 예산을 검토·승인하고 동 예산이 모두 집행될 수 있도록 보장

- 전사적인 위험관리 결과를 토대로 조직이 수용할 수 있는 위험범위, 위험 대응 우선순위 등을 최고경영층의 의견을 수렴해 승인하고 관리

3) 임직원들이 관련 법규, 내규에 따라 행동할 수 있도록 격려 및 감독

4) 임직원들에게 최고경영자의 정보보호 활동에 대한 관심을 지속적으로 피력

5) 최고경영자의 정보보호 활동 등을 외부 전문가(조직)을 통해 주기적 평가

❒ CISO의 역할 및 책임

1) 원활한 정보보호 활동을 위한 최고경영자 등과 소통 강화

- 정보보호위원회 운영을 통해 소통의 장을 활성화

- IT·정보보호에만 치우치지 않고 비즈니스 또한 고려하여 이사회, 최고경영층 간의 지속적·정기적인 대화를 통해 적정한 정보보호 인력 안배와 예산 확보 및 집행에 대한 공감대 형성

- 고객 정보 자산 등을 소유하고 있는 현업 부서(장)와의 소통을 통해 정보보호의 중요성을 고취시키고 타 부서에 조력할 수 있도록 지원

- 정보보호 관련 핵심 이슈나 사고 발생 등의 사실을 최고경영층에게 신속히 공유하고 이를 해결할 수 있도록 지원

- 최고경영자가 조직의 자율적 정보보호 문화 조성을 선도할 수 있도록 지원

2) 비즈니스를 고려한 현재와 미래의 정보보호 목표 제시 및 평가

- 정보보호 목표 달성을 위해 기 수립한 중장기 정보보호 정책에 대한 적정성을 평가

정보보호 정책

▶ IT 관련

- 물리적·환경적 보안, 접근통제, 운영보안, 전자금융거래 보안, 외부주문 보안, IT도입·개발·유지보수 관리, 사업연속성·재해복구 등

▶ 기타

- 임직원 정보보호 교육, 전사적 위험관리, 정보보호 인증 취득 및 유지관리 등

- 관련 법규, 내규 등 조직과 관계사 적용 및 대응 전략 평가

- 보안 기술적용 시기와 보안 제품 도입 시기를 결정하고 항상 신기술 트렌드에 대해 파악

3) 정보보호 정책 등을 정보보호(보안)부서에 지시

- 정보보호 목표와 목표 달성을 위해 구현 필요성이 있는 정책을 정보보호(보안) 부서에 지시

4) 정보보호(보안)부서에 대한 관리 감독

- 정보보호(보안) 부서의 정보보호 활동에 대해 주기적으로 관리 감독

5) CISO의 정보보호 활동 등을 외부 전문가(조직)에 의해 주기적 평가

❒ 정보보호(보안) 부서의 역할 및 책임

1) CISO의 정보보호 활동 지원 및 정책 수행

- 중장기 정보보호 계획 수립

- 전사적인 정보보호 정책 수립·운영 및 유지 관리
  . 물리적·환경적 보안
  . 정보보호시스템, 정보처리시스템들의 계정 및 권한 관리, 데이터베이스 접근제어 관리
  . 영역별(단말기, 전산자료, 정보보호시스템, 무선통신망, 악성코드 등) 보안
  . 안전한 전자금융거래를 위한 보안

. 외부주문 관련 보안
. IT도입·개발·유지보수 관리(사업추진시 보안성 검토, 프로그램 통제, 외주개발 보안 등) 보안
. 위험에 대비한 사업연속성 계획과 사고·재해 시 대응 방안
. 임직원 정보보호 교육
. 전사적 위험관리 방법 및 계획 수립
. 정보보호 인증 취득 및 유지 관리 등

- 관련 법규, 내규 등을 조직과 관계 기관에 적용하고 정보보호 대응 전략 수립

- 정보보호위원회 활동에 대한 지원

- 보안 기술, 보안 제품 및 신기술 트렌드 등을 파악하여 CISO 등에 보고

2) 감사부서에서 진행하는 정보보호 감사에 대한 지원

- 감사를 위해 사용하는 정보보호 점검항목 도출 협조 또는 실질적인 점검 지원

[참고]

정보보호(보안)부서 업무 조사

❒ **미국, 업무혁신보안위원회(SBIC, Security for Business Innovation Council)**

❍ RSA를 필두로 하여 100개 이상의 글로벌 기업의 보안 전문가들이 포함되어 있는 전문가 그룹으로서 정보보호 거버넌스에 관련한 보고서를 개발함

❍ “Designing a State-of-the-Art Extended Team”은 2014년 5월에 SBIC에서 발간한 연구 보고서로 정보보호(보안)부서의 미래상과 앞으로의 과제 및 기회, 또한 현재 정보보호조직이 취해야할 권고사항을 제시함

(1) 정보보호(보안)부서 핵심역량의 재정의 : 정보보호 업무를 네 가지 주요 분야인 사이버위험 인텔리전스 및 보안 데이터 분석, 보안 데이터 관리, 위험 컨설팅, 통제 설계 및 보증으로 나누어서 재정의하고, 강화되어야할 정보보호 조직의 핵심역량 제시

① 사이버위험 인텔리전스 및 보안 데이터 분석
- 증가하는 위험을 감안하여, 위험 탐지 개선
- 특히, 인텔리전스 중심의 접근방법의 개발이 중요
- 그러기 위해서는 내외부 자원으로 부터 사이버 인텔리전스 데이터를 수집 및 취합하고, 공격 지표 또는 비정상적인 동작 패턴을 탐지하는 데이터 분석기술 필요

② 보안 데이터 관리
- 위험 탐지를 위한 데이터 분석 시, 조직은 무엇보다 보안 데이터 관리 전략 및 인프라에 대한 필요성 인식
- 이를 위해선 로그 기록, 전체 패킷 데이터 스트림 및 시스템 데이터베이스, 비즈니스 어플리케이션 같은 보안 데이터의 집계가 필요

③ 위험 컨설팅
- 향후 정보보호조직은 조직적 차원에서 정보보호, 개인정보보호 및 법적 문제, 컴플라이언스와 같은 문제에 대한 자문 역할 수행
- 정보보호조직은 조직의 정보보호뿐만 아니라 비즈니스 프로세스에 대한 명확한 인식이 필요

④ 통제 설계 및 보증
- 비즈니스 목적과 연계되는 혁신적인 통제항목을 개발
- 향후 정보보호조직의 핵심적인 역할

(2) 일상적인 운영업무의 위임 : 기존의 정보보호조직은 일상적이고 반복적인 업무만 수행하였지만 이러한 반복적인 업무는 외부 서비스 제공자나, 내부의 타부서에게 전가되어야 하고, 정보보호조직은 좀 더 능률적이고 전략적인 업무에 집중

(3) 외부 전문가 활용 : 전문가 부족은 현 정보보호조직이 풀어야할 과제 중 하나

(4) 현업부서 중심의 위험관리 : 향후 정보보호조직의 핵심 역할 중 하나는 정보 위험관리와 관련된 활동이 무엇이 있는 지 이끌어내고 해당 위험의 책임자는 누구인지 식별하고, 위험 책임자를 식별함으로써 명확한 책임과 책임추적성이 규명

(5) 프로세스 최적화 전문가의 고용 : 정보보호를 조직의 비즈니스 프로세스의 한 부분으로 강조하기 위해선 정보보호 조직 내에 프로세스 전문가를 고용하는 것이 필요

(6) 타부서와의 협업체계 구축 : 정보보호 책임 인력의 연계와 협동 환경의 조성을 위해 정보보호 조직은 조직 전반에 걸쳐 강력한 관계를 구축하는 것이 필요하다. 타부서와 협업을 구축할 때 가장 중요시 여겨야할 것 중 하나는 정보보호 조직에 있어 조직 내의 가장 중요한 부서(crown jewels)가 어디인지를 파악

(7) 전문가 육성 : 전문가 육성을 장기적인 관점에서 고려되어야 하며, 소프트웨어 개발, 데이터베이스 관리, 비즈니스 분석, 국방 기밀 보안, 법률 및 개인정보보호 등과 같은 분야의 전문가 육성 및 활용

❒ CIO의 역할 및 책임

1) 원활한 IT 활동을 위한 최고경영층과의 소통 강화

- 최고경영층에게 IT 서비스와 관련된 신기술 사업결정을 위한 타당성 검토 결과를 공유

- 성과관리체계를 수치화·가시화하여 IT 활동의 정당성 제공

2) 비즈니스를 고려한 현재와 미래의 IT 목표 제시

- IT 목표 달성을 위한 조직의 중장기 IT 정책에 대해 적정성을 평가하고 정보보호 관련 사항은 CISO와 협의

- ROI 등을 토대로 산출된 IT 인력 및 예산에 대한 적정성 평가

IT 정책

▶ IT 관련

- 물리적·환경적 접근, 내부사용자 및 이용자 비밀번호 관리, 서버 통제, 단말기·무선통신망·악성코드 통제, 전자금융거래 기록관리, 프로그램(S/W) 통제, 외주개발 통제, 업무연속성, 보안사고 대응, 정보보호 정책을 반영한 IT·정보보호시스템 운영 등

▶ 기타

- 위험의 식별 및 평가, 규제대응 등

3) 평가된 IT 정책 등을 IT(운영) 부서에 지시

- IT 목표와 목표 달성을 위해 구현될 필요성이 있는 전략을 IT(운영) 부서에 지시

4) IT 정책을 수행하는 IT(운영) 부서 관리 감독

- IT(운영) 부서의 IT 활동에 대해 주기적으로 관리 감독

5) CIO의 IT 활동 등 외부 전문가(조직)를 통해 주기적 평가

❐ CPO의 역할 및 책임

1) 원활한 개인정보보호 활동을 위한 최고경영층 간의 소통 강화

- 개인정보보호에 대한 법규 위반, 규제기관 대응, 사고 대응 방안 및 기술적 대응을 위해 CISO, CIO와 긴밀히 소통

- 이사회, 최고경영자 또는 책임을 가진 위원회에게 개인정보보호 현황을 정기적으로 보고

2) 비즈니스를 고려한 현재와 미래의 개인정보보호 목표 제시

- 마케팅, 제품개발 및 사업 전략 등 조직의 비즈니스를 고려하여 최고경영층에게 개인정보보호의 전략적인 정책 제시

- 관련 법규의 제·개정 사항 모니터링 및 개인정보보호 정책의 최신성 확보

- 개인정보보호 정책의 조직과 관계사 적용 관련 적정성 평가

- 개인정보 관련 규제 등이 비즈니스에 어떠한 영향을 미치는지 영향 평가를 수행하고 그 결과를 검토

- 정보보호 문화 조성의 일환으로 임직원을 대상으로 하는 개인정보 보호 교육을 수행하고 그 결과를 평가

3) 개인정보보호 정책 등을 개인정보 취급 부서에 지시

- 개인정보 취급 부서에게 개인정보보호 법률에서 정한 규정을 준수하도록 지시

4) 개인정보보호 정책을 수행하는 부서에 대한 관리 감독

- 개인정보 수행부서의 개인정보보호 활동에 대해 주기적으로 관리 감독

5) CPO의 개인정보보호 활동 등을 외부 전문가(조직)를 통해 주기적 평가

❒ 준법감시인의 역할 및 책임

1) 원활한 컴플라이언스 정책을 수행하기 위한 소통 강화

- 컴플라이언스 활동의 중요성을 소통을 통해 효율적이며 효과적으로 임직원에게 전파

- 정보보호 수행부서가 적절한 정보보호 정책 수립 및 운영을 할 수 있도록 컴플라이언스 측면에서 지원

2) 임직원들에게 조직의 컴플라이언스 목표 제시

- 관련 법규에 대한 제·개정 사항 모니터링 및 컴플라이언스의 최신성 확보

- 컴플라이언스의 조직과 관계사 적용에 대한 적정성 평가

- 정보보호에 대한 법규 위반, 규제기관 대응 및 사고발생시 CISO (정보보호(보안) 부서)와의 협력 방안에 대한 평가

- 정보보호 문화 조성을 위해 임직원을 대상으로 하는 정보보호 컴플라이언스 교육에 대한 평가

3) 컴플라이언스 준수를 관련 부서에 지시

- 컴플라이언스 준수할 수 있도록 관련 부서에 지시

4) 컴플라이언스를 수행부서에 대한 관리 감독

- 수행부서의 컴플라이언스 활동에 대해 주기적으로 관리 감독

5) 준법감시인의 컴플라이언스 활동 등을 외부 전문가(조직)를 통해 주기적 평가

❒ 감사인의 역할 및 책임

1) 원활한 감사 활동을 수행하기 위한 최고경영층과의 소통

- 정보보호 수행부서가 적절한 보안정책 수립 및 운영할 수 있도록 내부통제 및 위험 평가 측면에서 협력

- 감사 활동의 중요성을 소통을 통해 효율적이며 효과적으로 임직원에게 전파

2) 비즈니스를 고려한 현재와 미래의 감사 목표 제시

- CISO(정보보호(보안) 부서)와의 협의를 통해 정보보호 감사 항목 도출

- 비즈니스, 정보보호, IT 등 감사 정책에 대한 적정성 평가

3) 감사 정책을 수행부서에 지시

- IT부문에 대한 보안감사 수행 또는 보안감사를 수행하는 보안담당 부서 지원

4) 감사 활동을 수행하는 수행부서에 대한 관리 감독

- 수행부서의 감사 활동에 대해 주기적으로 관리 감독

5) 감사인의 감사 활동 등을 외부 전문가(조직)를 통해 주기적 평가

❒ 정보보호위원회의 역할 및 책임

1) 정보보호위원회의 장은 CISO가 맡으며 최고경영층이 참석하여 정보보호 활동에 대해 심의·의결

※ 정보보호 활동 의지 표명의 일환으로 최고경영자가 위원장을 맡는다면 CISO는 간사 역할 수행 가능

심의·의결

▶ 정보보호 활동에 대한 심의·의결

- 법률에 요구하는 심의·의결 사항 준수
- 수립된 정보보호 정책
  - 최종 책임에 대한 명확화
  - 정보보호 정책 및 지침의 제·개정에 관한 조직 적용
- 연간 정보보호 활동 계획 수립과 집행
- 정보보호 활동 우수자에 대한 포상

▶ 결과에 대한 심의·의결

- 위험평가 결과에 대한 검토와 필요시 개선 요청
- 내부 정보보호 감사 결과 및 사후 조치
- 정보보호 기술, 제품 등에 대한 자체 보안성 검토

2) 부서간 정보보호 협업 강화와 갈등에 대한 중재 및 조정 역할

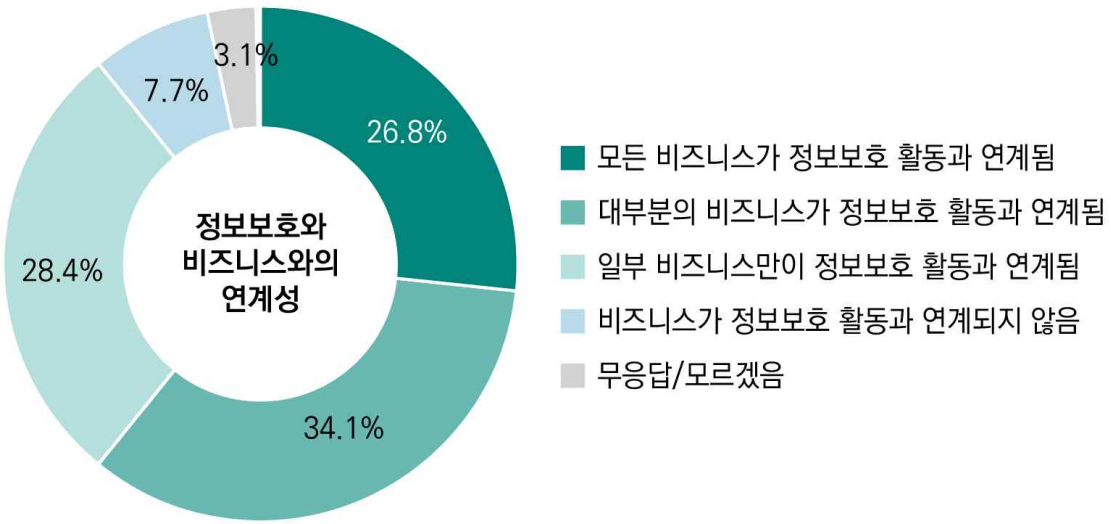
3) 기타 위원장 및 최고경영층이 필요하다고 인정하는 사항에 대한 논의

[참고] Deloitte, 정보보호와 비즈니스와의 연계성

❒ 정보보호와 비즈니스와의 연계성 조사

- 정보보호와 비즈니스와의 연계에 대한 설문조사를 살펴보면, 정보보호 활동에 대한 비즈니스의 참여 정도는 약 61%로 조사됨

〈 정보보호와 비즈니스와의 연계성 조사 〉



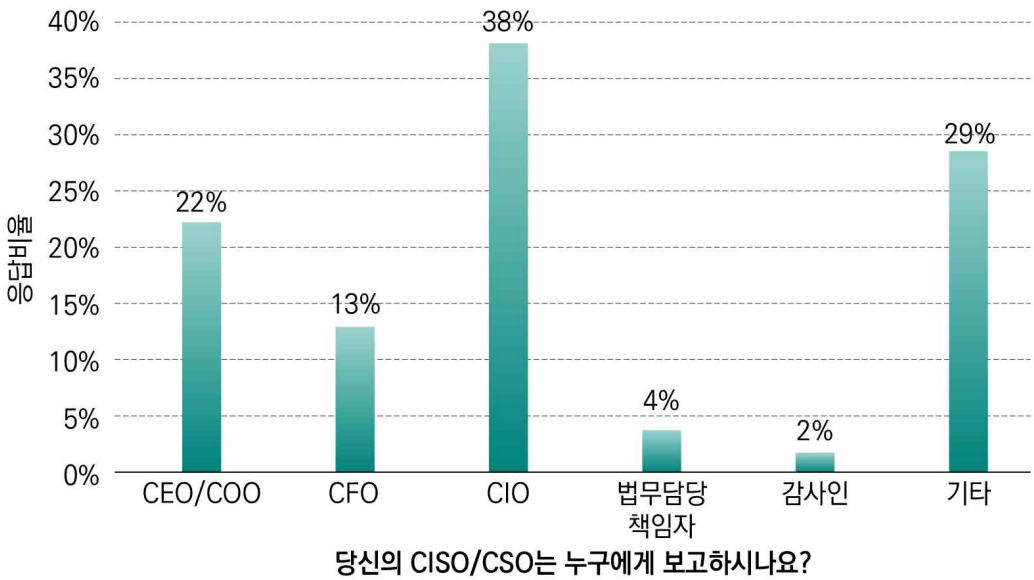
2 올바른 의사결정을 위한 보고체계 수립

❒ **최고경영자의 올바른 의사결정을 지원하기 위해 정보보호 활동 결과가 누락 없이 전달될 필요**

❒ **CISO가 최고경영자에게 직접 보고할 수 있는 보고체계 구성**

- 해외 조사에 따르면, CISO가 CEO/COO, CFO 등 Non-IT 부서장에게 보고하는 경우가 점차 늘고 있으며, 이는 CIO와 CISO의 분리가 필요함은 물론 정보보호가 비즈니스와도 연관성이 많다는 인식이 증가하고 있음을 의미

〈 전사적 보안 거버넌스 설문조사 보고서 〉



당신의 CISO/CSO는 누구에게 보고하시나요?

〈자료출처 : CMU, 2012〉

- 국내도 CISO의 독립성 강화를 위해 정보보호(보안)부서를 최고경영자 직속에 두는 것이 바람직한 것으로 인식

〈 CISO의 소속부서는 어디가 되어야 한다고 보시나요? 〉

최근 의무화 지정 논의 중인 CISO의 소속부서는 어디가 되어야 한다고 보시나요?		
구 분	비율(%)	응답자수(명)
CEO 직속의 별도 보안담당 부서	65.63	1,187
IT 및 전산부서	17.53	317
감사부서	8.42	152
경영지원부서	5.98	108
법무관련 부서	2.45	44
기타	0	0
※ 합계	100	1,809

〈자료출처 : 설문[1], 2014〉

3 위험 감소 및 완화를 위한 전사적인 위험관리 체계 확립

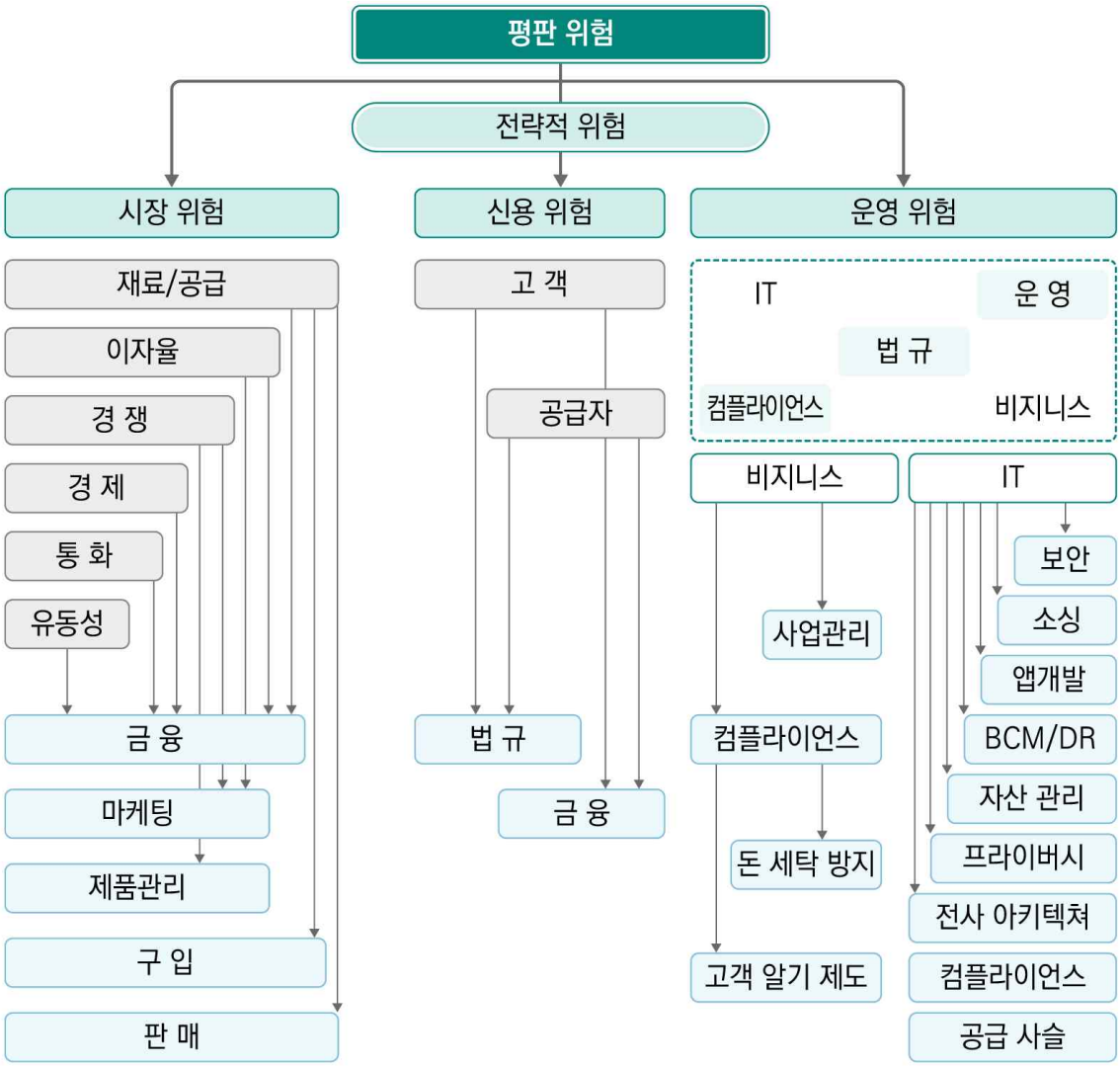
❒ **일반적으로 정보보호 위험관리가 전사적으로 이뤄지지 않고 IT중심으로 관리되고 있어 최고경영자가 정보보호 위험에 대한 잘못된 의사결정을 내릴 가능성이 존재**

❒ **조직의 목표 달성을 위해 전사적으로 정보보호 위험을 파악하고 관리할 필요**

- 해외 조사에 따르면, 정보보호 위험관리는 조직의 목표, 전략, 개발, 인적 자원의 관리 등을 기반으로 함
- 효과적인 정보보호 위험관리를 통해 위협으로 인한 각종 손실 등의 감소 및 완화 기대

1) IT 및 보안담당자 1,809명을 상대로 설문, http://www.boannews.com/media/view.asp?idx=43548

〈 전사적 위험관리 〉



〈자료출처 : Gartner, 2010〉

❒ **체계적인 정보보호 위험관리를 위해 가장 중요한 것은 위험요소에 대한 정보를 최고경영자에게 적시 보고하는 것임**

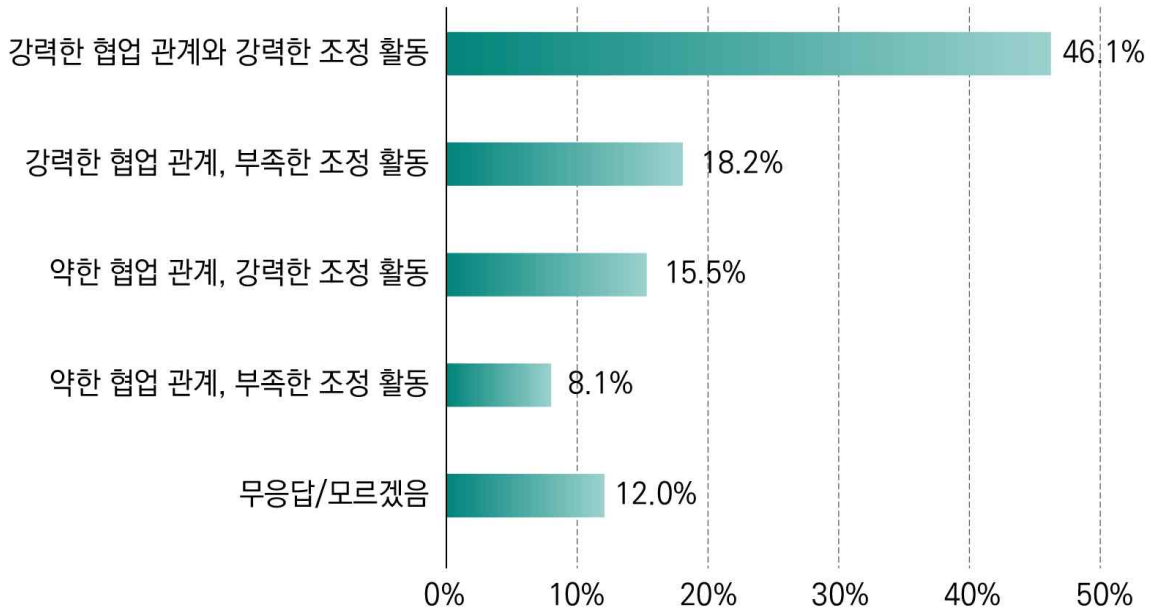
[참고] Deloitte, 협업 및 관계의 중요도

❒ **정보보호 부서와 위험관리 부서 간의 협업 및 관계**

- 응답자 중 과반수에 가까운 46%가 '강력한 협업 관계와 조정 활동이 수행되고 있다'라고 응답했으며 협업 관계나 조정 활동이 다소 미흡하다고 응답한 비율은 33%, '협업관계가 전혀 수행되지 않고 있다'가 8%임

- 이는, 점차 정보보호 위험을 전사적 위험의 일부로 보고 있는 현상임을 확인할 수 있음

〈 협업 및 관계의 중요도 〉



4 정보보호 활동의 현재와 미래에 대한 최고경영층의 이해를 돕기 위한 방법 제시

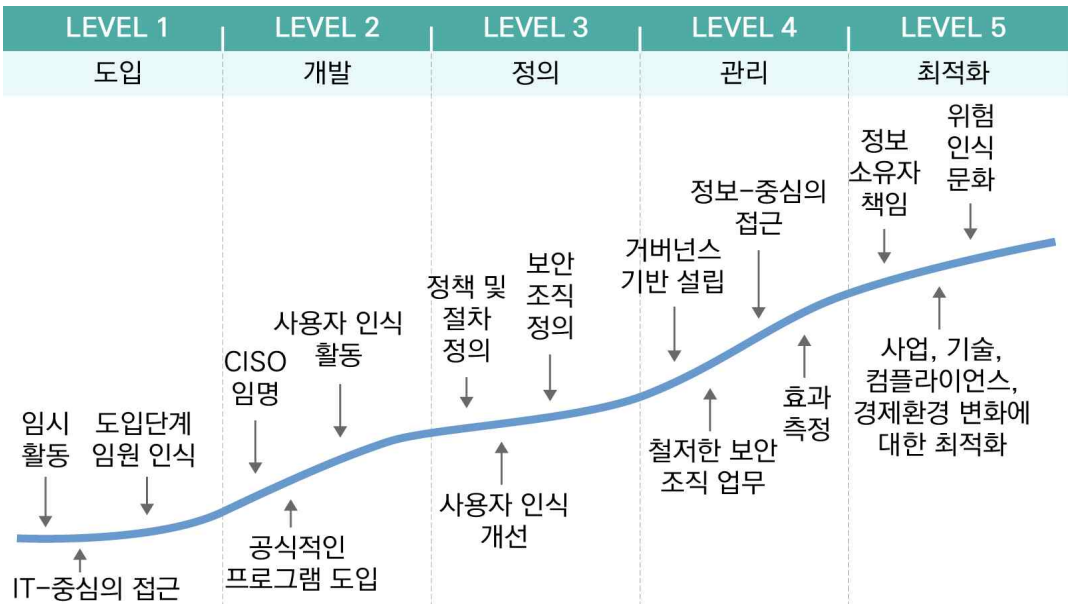
❒ **조직의 정보보호 활동 수준을 파악할 수 있는 방법 마련 필요**

❒ **IT에 대한 성과지표는 있으나 정보보호에 대한 성과지표의 마련은 아직 초기 단계**

❒ **정보보호 활동 자체를 정량적으로 측정하기는 어려운 면이 있으나 이를 지표화하는 노력은 필요**

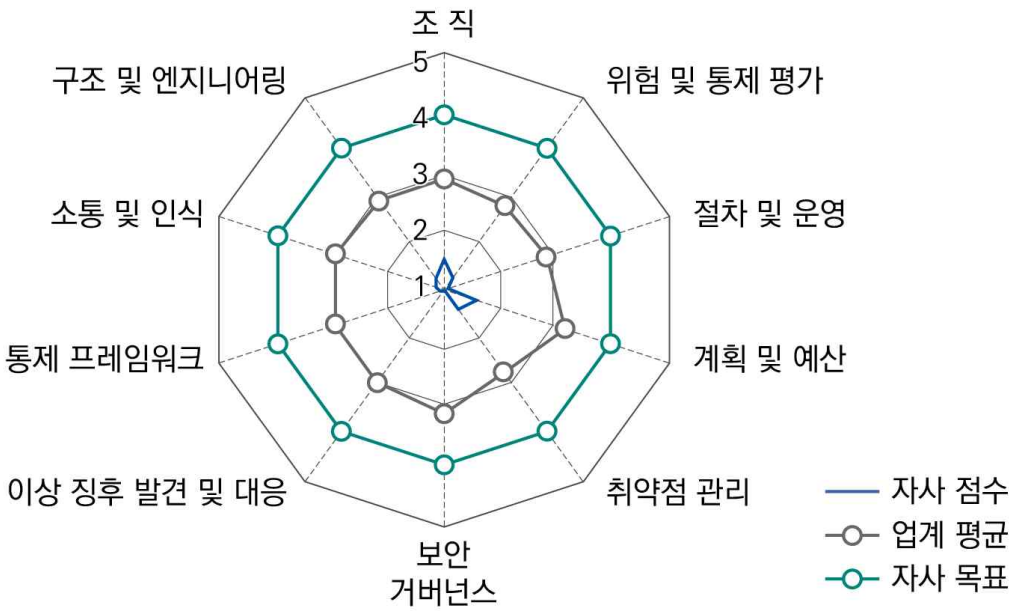
- 정보보호 성과지표로 규제(내규) 준수 여부, 정보보호 교육 이수율, 각종 인증 획득 등이 고려될 수 있음.
- 해외의 경우 정보보호 성과를 성숙도로 표시하여 조직의 현재 수준을 파악하는 방안도 제시되고 있는 상황

〈 정보보호 성숙도 지표 〉



〈자료출처 : Gartner, 2013〉

〈 정보보호 활동 스코어 〉



〈자료출처 : Gartner, 2013〉

❒ **성과지표는 사고시 조직의 정보보호 활동에 대한 증명 자료로서 사용 가능**

❒ **각각의 조직 문화에 맞는 성과지표를 수립하여 정보보호 활동의 원활한 투자를 유도할 필요**

❒ **이사회, 투자자, 금융당국 등 이해관계자에 정보보호 거버넌스 활동 및 주요 성과 등을 홍보할 수 있는 보고서*를 발간하는 방안도 고려 필요**

* 지속가능경영(Corporate Sustainability Management) 또는 사회책임경영 (Corporate Social Responsibility) 보고서

5 원활한 정보보호 활동을 위한 최고경영층 등의 소통 강화

❒ **정보보호 정책의 이행 및 사고예방과 신속한 대응을 위해 최고경영층 간, 실무조직 및 현업조직간 원활한 소통이 중요**

❒ **CISO가 가져야 할 주요 조건으로 IT·정보보호 지식, 금융업무 이해, 법률·규제의 이해 등은 물론 각 이해관계자간 소통 능력도 중요**

❒ **최고경영층은 정보보호와 관련하여 임직원들과 꾸준한 소통을 통해 시너지 창출할 필요**

- 최고경영층은 정보보호위원회 등을 통해 정보보호 관련 정보를 공유하며 중요사항을 심의·의결

❒ **조직의 정보보호 정책을 원활하게 수행하기 위한 체계화된 소통문화 마련 필요**

- IT 중심적인 논의보다는 비즈니스를 고려한 소통을 통해 정보보호에 대한 최고경영층의 이해도 제고

- 정보보호를 담당하는 실무조직과 현업조직과의 원활한 소통으로 조직의 정보보호 목표를 원활하게 달성

6 안정적인 정보보호 활동을 위한 정보보호 예산 수립, 집행 및 전담인력 배치

❒ **안정적인 정보보호 활동을 위해 적정한 정보보호 인력 및 예산을 확보할 필요**

❒ **대내·외 환경 및 금융회사의 위험분석 결과 등을 종합적으로 고려하여 적정한 정보보호 인력 및 예산 비율을 산정하고 이를 준수하여 수립·집행**

- 다만, 전자금융거래에 대한 최소한의 안전성 확보를 위해 일정 비율 이상*의 IT·정보보호 인력 및 예산 확보를 권고 (최소 기준)

  * IT인력 : 총 임직원의 5% 이상, 정보보호 인력 : IT인력의 5% 이상, 정보보호 예산 : 전체 IT예산의 7% 이상

※ **(국내)** 국내 금융권의 정보보호 예산은 IT 예산 대비 평균 10.6%, 정보보호 인력은 IT 인력 대비 평균 10.2%(금융감독원, `19.6월)
(해외) 해외 기업의 정보보호 예산은 IT 예산 대비 평균 7.6%(금융부문), 정보보호 인력은 IT 인력 대비 평균 5.6%(Gartner, `19.12월)

❒ **금융회사에서 정한 정보보호 인력 및 예산 비율이 최소한의 기준을 상회하며, 금융회사의 위험을 적절히 반영하였는지 주기적으로 검토**

[참고] 정보보호 인력 산정기준

1. 총 임직원 및 외주인력

(1) 총 임직원 수는 금융회사 등의 상시 종업원(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준)으로 하되, 1년 이상 장기휴직자와 외주(outsourcing)인력은 제외

(2) 외주인력이란 금융회사 등과의 외부주문 등에 따라 업무를 처리하는 업체에 소속된 자로서 다음 기준에 따라 산정
- 금융회사 등의 정보기술부문 업무 수행을 위한 정보화 기획, 전자금융기반시설 운영, 정보보안 등의 IT업무 종사자를 포함
- 전자금융기반시설의 하드웨어 또는 소프트웨어 등의 유지보수를 수행하기 위한 제조사의 상시 운영 기술인력 포함
- 정보시스템 개발 프로젝트를 수행하기 위하여 상주하는 외주업체의 IT업무 종사자는 제외
- 외주인력 중 월·주 단위 등 부정기적이거나 일시적인 인력은 제외

2. 정보보호 인력

(1) 금융회사의 총 임직원 중 내부 규정에 따라 정보보호 업무를 처리하는 사람

(2) 다음 기준에 따라 소속되어 정보보호 업무를 담당하는 상시 종업원 중 해당 금융회사의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으로서, 전자금융감독규정 제60조 제1항 제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람(이 경우, 해당 금융회사의 정보보호 인력 규모는 다음 각 호의 회사 또는 기관이 공동으로 위탁 받은 정보보호 업무에 대한 운영비용 분담비율에 따라 산정한다)
- 「금융지주회사법」 제2조제1항에 의한 자회사 또는 손자회사로써 금융업을 영위하는 회사에 대한 전산·정보처리 등의 용역을 제공하는 회사
- 금융회사 또는 전자금융업자가 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사 또는 전자금융업자에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사
- 「독점규제 및 공정거래에 관한 법률」 제2조제2호에 의한 기업집단에 속하는 금융회사들 또는 전자금융업자들이 합하여 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사들 또는 전자금융업자들에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사
- 회원사, 상호저축은행, 신용협동조합, 조합, 지역금고 등의 전자금융기반시설에 대한 운영을 공동 수탁하는 기관

(3) (2)번의 인력을 제외한 외주인력 중 해당 금융회사 또는 전자금융업자의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으로서, 전자금융감독규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람

7 선순환 구조를 위한 정보보호 문화 확립

❒ **많은 조직에서 기본적인 정보보호 법규 준수만을 고려하고 있는 상황**

❒ **조직 스스로가 정보보호 활동을 자발적이고 적극적으로 임해 선순환 구조를 이룰 필요성이 있으며, 이를 위해 최소한의 법규 준수뿐만 아니라 자율적인 정보보호 활동 수행이 필요**

- 금융회사가 보안위험에 적절히 대처할 수 있고 디지털 리스크를 감소시킬 수 있도록 적정한 예산을 설정하고 인력을 배치하는 노력 필요

❒ **정보보호 활동이 규제가 아닌 하나의 조직문화로 발전해야 금융보안 거버넌스가 보다 효율적이고 효과적**

- 정보보호 활동을 더 이상 기술적 · 정책적 관점에서만 바라보지 않으며, 임직원들이 자연스럽게 체득해야 할 문화로 인식

- 문화는 신념에 기초로 하기 때문에 자신이 처리하는 정보가 중요하고, 보호할 가치가 높다는 점을 스스로 인식

부록 | 정보보호 업무 및 CISO와의 관계[2)]

1 정보보호 업무에 대한 RACI 차트

❒ CEO, CISO, CIO 등의 정보보호 업무에 대한 역할 및 책임

업무영역	업무	CEO	CISO	CIO	준법, 감사	내부 관리*	현업
정보보호 조직 체계 구성	1. 정보보호 조직 및 인력구성	A	R	C		C	
	2. 정보보호 최고 책임자 지정	A	I	C		R	
정보보호 사업계획 평가 및 승인	1. 사업계획 평가 및 승인	A	C	C		R	C
	2. 정보보호 예산 확보	A	R			C	
	3. 성과 평가	A	C			R	
최고경영층 지원	1. C레벨 정보보호 아젠다 지원	I	A			C	
	2. 이사회 정보보호 아젠다 지원	I	A			C	
전사적 협업체계	1. 정보보호위원회 설치 · 운영	A	R			C	
	2. 정보보호실무위원회 설치 · 운영	I	A			C	
	3. 정보보호 태스크포스 구성	I	A	C		C	
	4. 관계 및 소통관리		A/R			C	
정보보호정책	1. 정보보호 정책의 수립, 운용	A	R		C	C	
	2. 정보보호 정책의 유지 관리		A		C		
인적보안	1. 정보보호 교육 및 훈련	I	A			C	
	2. 정보보호 역할 및 책임 정의		R	C		A	C
	3. 정보보호관련인사규정제정	A	C			R	
위험관리	1. 위험관리 방법 및 계획 수립	I	A	C			
	2. 위험(취약성)식별및평가		A	R	C	C	C
	3. 정보보호대책 수립 및 모니터링	I	A	C			
계획	1. 중장기 전략 수립	I	A				
	2. 단기 계획 수립		A				

* 경영지원, 경영기획, HR조직(CFO 등, 이 조직들의 담당 임원 포함)

2) 중앙대 김정덕 교수, CISOLab 강은성 대표의 "해외 정보보호 거버넌스 우수 구축 사례 조사" 내용의 일부를 부록으로 수록함

업무영역	업무	CEO	CISO	CIO	준법, 감사	내부 관리*	현업
규제대응	1. 규제기관 대응		A	C	I	C	
	2. 그룹사 가이드라인 대응	I	A	C			
보안감사	1. 보안감사 계획 수립	A	C	I	R	I	I
	2. 보안감사 시행		C		A/R		
	3. 감사결과 승인 및 후속조치		R		A/R		
정보보호 인증 취득 및 유지 · 관리	1. 정보보호 인증 획득	I	A	C	C	C	C
	2. 정보보호 인증 유지 · 관리	I	A	C		C	
물리적 · 환경적 보안	1. 전산실 보안		C	A		R	
	2. 사무실 보안		C	C		A/R	
접근통제	1. 계정 및 권한관리	I	A	C			
	2. 내부사용자 및 이용자 비밀번호 관리		C	A/R			
	3. 네트워크 접근통제	I	A	C			
	4. 서버 통제		C	A/R			
	5. 데이터베이스 통제		A	C			
운영보안	1. 영역별 보호대책 수립		A	C			
	2. 단말기 보호대책		C	A/R			
	3. 전산자료 보호대책		C	C		A/R	
	4. 정보보호시스템 설치 및 운영	I	A	C		C	
	5. 무선통신망 보호대책		C	A/R			
	6. 악성코드 감염 방지대책			A/R			
	7. 암호 프로그램 및 암호키 관리		A	C			
전자금융거래 보안	1. 전자금융거래시 정보보호 요구사항 반영 및 이행		A	C			C
	2. 전자금융거래 기록 · 보관			A/R			C
외부주문 보안	1. 외부주문 계약시 정보보호 요구사항 반영 및 이행		C	C			A/R
	2. 외부주문시 보호대책 수립 · 운용		A	C			C
IT도입 · 개발 · 유지보수 보안	1. 사업추진시보안성검토	I	A	C		C	
	2. 프로그램 통제		C	A/R			
	3. 보안성 심의		A	C			
	4. 외주개발 보안		C	A/R			
업무연속성 관리	1. 정보보호 리스크에 대비한 업무지속성 확보 방안 수립 · 시행	I	A	C		C	
보안사고 대응	1. 보안사고 대응체계수립		A	C		C	
	2. 보안사고 대응	I	A	C			
	3. 보안이슈 대응	I	A	C			

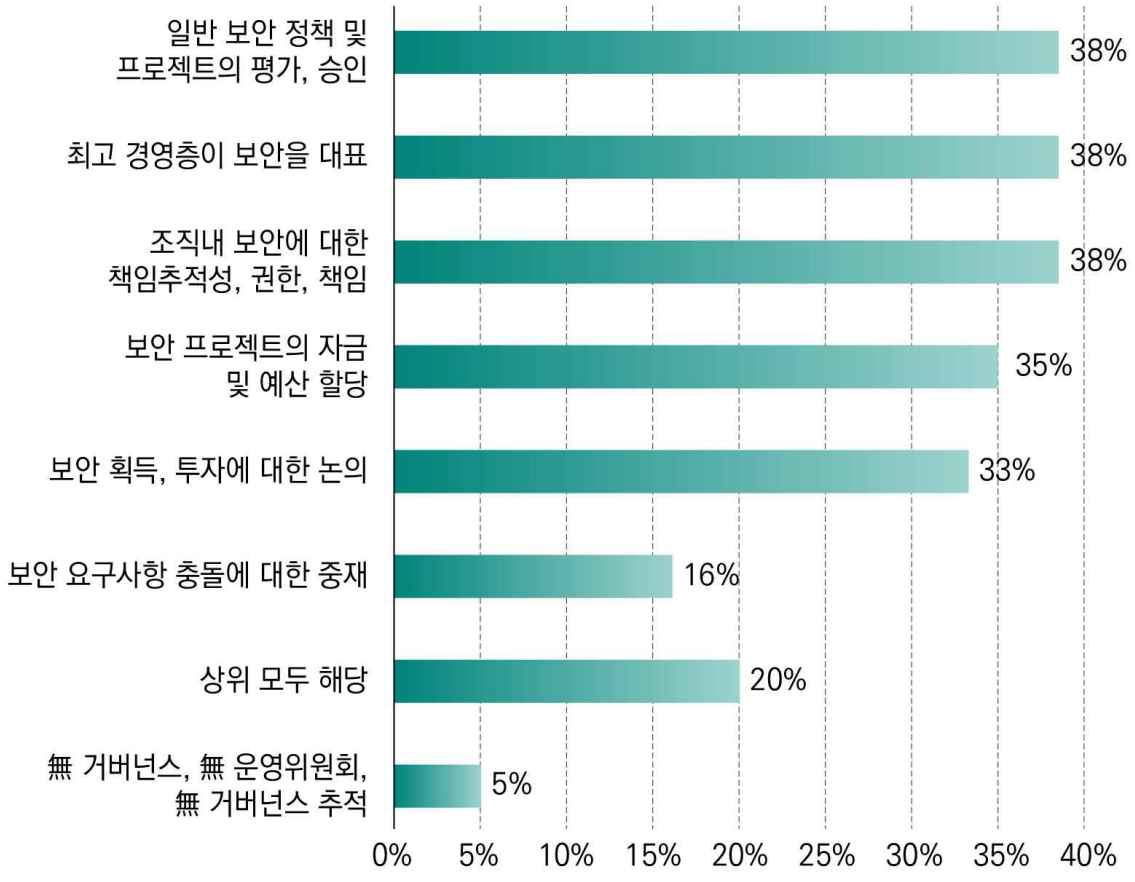
[참고] 해외 정보보호 기능, 업무 조사

□ Gartner, 정보보호 기능별 중요도 조사

○ 가장 중요하게 생각하는 정보보호 거버넌스의 기능은 정보보호 정책과 프로그램의 평가 및 승인, 정보보호 성과 보고, 정보보호 책임추적성과 권한의 정의 순으로 조사됨

○ 정보보호 관련 갈등 조정을 위한 중재와 관련된 기능에 대한 중요도가 16%로 낮게 나왔으나, IT 부서 및 현업 부서와의 갈등 조정이 점차 중요해짐에 따라 중요 거버넌스 기능으로 인식이 필요함

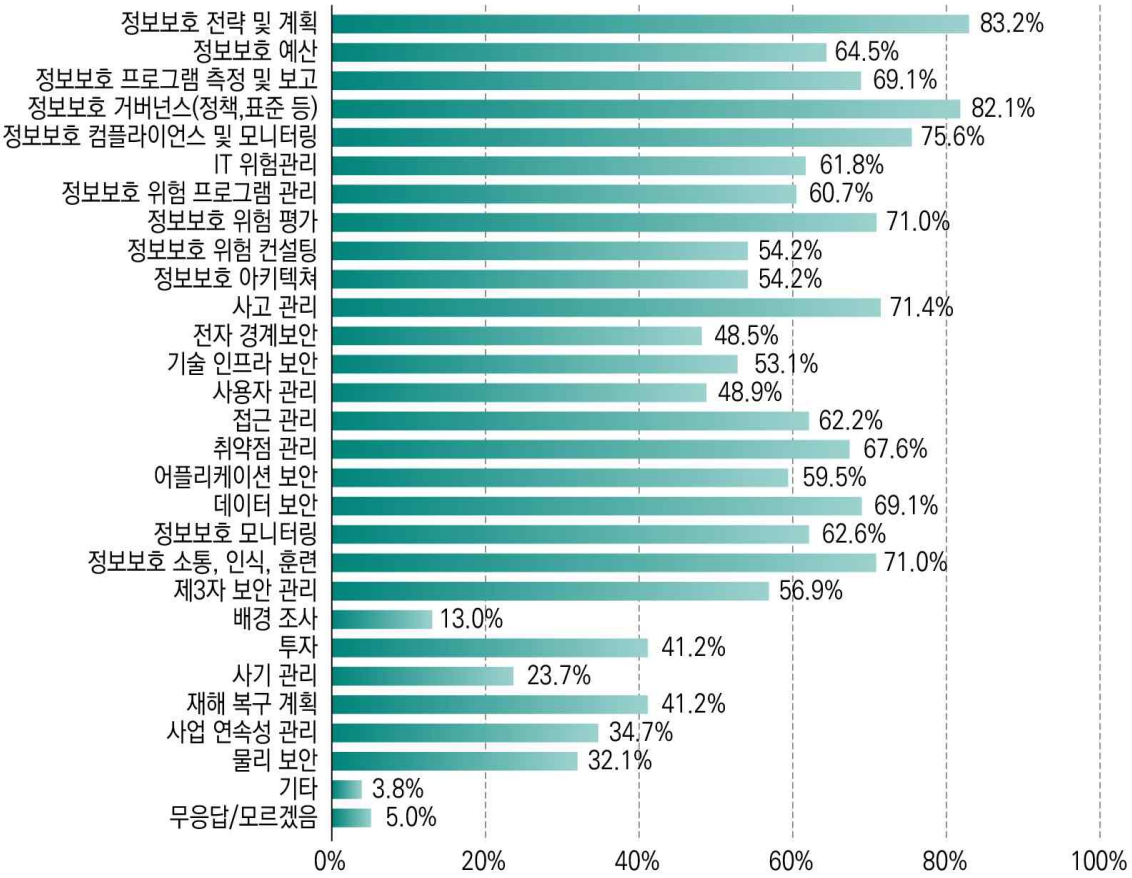
〈 Gartner에서의 정보보호 기능별 중요도 조사 〉



□ Deloitte, 정보보호 거버넌스 기능의 중요도 조사

○ 정보보호 전략 및 계획의 수립, 정보보호 거버넌스, 정보보호 컴플라이언스 및 모니터링, 정보보호 위험평가, 정보보호 교육 및 인식 프로그램, 데이터 보안 등의 순으로 조사됨

〈 정보보호 거버넌스 기능의 중요도 조사 〉



□ 독일, 도이치 방크(Deutsche Bank) 업무 정의

○ 도이치 방크의 “Information security policy” 보고서는 정보보호와 관련된 위험을 효율적으로 관리하고 내외부의 정보보호 관련 요구사항을 적정 수준으로 충족시키기 위해 정보보호 업무와 관련된 이해관계자들을 8개의 범주로 나누어 각각의 역할 및 책임을 정의함

(1) 최고경영층 : 최고경영층은 기업의 이익과 손실에 대한 궁극적인 책임을 지니고 있으며 정보 및 정보와 관련된 자산에 대한 최종 책임 할당과 위험 수용 수준을 결정하고, 정보보호 예산 및 자원에 대한 집행 및 할당, BISO(Business Information Security Officer)의 임명 및 비즈니스와 관련된 정보보호 위험에 대한 통제 등과 같은 업무를 수행

(2) IT 관리자 : IT관리자는 정보보호와 관련된 업무의 총괄책임 및 비즈니스 요구사항을 충족시킬 수 있는 적절한 수준의 보안 구현을 보장해야하고, TISO(Technology Information Security Officer)의 임명 및 정보 및 정보와 관련된 자산의 소유자의 식별 등과 같은 업무를 수행

(3) 정보 자산 소유자 : 실질적으로 정보 또는 정보와 관련된 자산을 소유한 현업부서로 해당 정보 자산에 대한 최종 책임 및 위험 수용에 대한 결정을 가지며, 정보보호 정책을 수립하는데 있어서 BISO를 지원하고 정보보호 운영의 총괄적인 관리 및 통제 등과 같은 업무를 수행

(4) 비즈니스 정보보호 책임자(BISO) : 비즈니스와 연계하여 정보보호와 최고경영층 및 정보 자산 소유자가 설정한 위험 수용 수준 내에서 적절히 위험을 통제하는 일차적 책임을 가지며, 최고경영층과 IT 관리자를 지원하고 정보보호 정책에 의해 위험 통제를 구현하는 등의 업무를 수행하고 CISO에게 보고

(5) 기술 정보보호 책임자(TISO) : 정보보호 영역의 지식뿐만 아니라, 보안 및 관리 문제에 대한 배경 및 지식이 요구되며, IT(전산 기반시설, Application 등) 관리 업무흐름에 있어서 정보보호 문제에 대한 관리 및 운영업무의 역할을 수행하고, 정보보호 정책, 표준 및 비즈니스 요구에 따른 서비스 지원 등의 업무를 수행하고 CISO에게 보고

(6) 정보보안 위험 그룹 : 정보보호 위험 그룹은 보안 전문가들로 구성되며 고객의 정보의 안전한 사용을 책임지고 조직의 정보자산 보호에 대한 적절한 수준을 보장

(7) 사용자 : 조직 내 정보자산의 접근 및 이용 권한이 부여된 내외부 사용자를 의미하며 사용자는 정보자산의 사용에 있어서 일련의 모든 행동에 대해 개별적으로 책임 부여

(8) 감사조직 : 조직의 정보보호 정책에 대한 준수 및 평가를 위해 정기적으로 독립적인 감사를 수행

□ 인도, 은행업권의 정보보호 업무 및 중요도

○ KPMG의 “State of data security and privacy in the India banking industry”는 DSCI(Data Security Council of India)와 함께 인도 은행업권 20개 은행을 대상으로 실시한 설문조사 보고서이며, 주목할 것은 은행업권에서 정보보호 업무를 식별하고 중요성을 분석한 점임

〈 정보보호 업무 및 중요도 〉

부문	최고 경영층	CCO	CISO	IT 보안	IT 인프라 부서	감사 부서	외부 컨설턴트	외부 서비스 제공자
정보보호 갭분석/기준평가	11%	0%	39%	56%	11%	39%	22%	11%
정보보호 전략 및 계획 수립	5%	0%	84%	37%	0%	5%	16%	0%
비즈니스 관련 정보보호 요구 사항 충족	22%	11%	78%	44%	0%	0%	6%	0%
정보보호 정책 및 절차 준비	5%	5%	84%	47%	0%	5%	16%	5%
정책 및 절차의 구현	22%	6%	61%	67%	33%	17%	6%	6%
보안 아키텍처 정의 및 관리	0%	0%	68%	63%	42%	5%	5%	5%
고객 규정 준수 보고	0%	0%	50%	0%	25%	25%	0%	0%

부문	최고 경영층	CCO	CISO	IT 보안	IT 인프라 부서	감사 부서	외부 컨설턴트	외부 서비스 제공자
개인정보보호 자문	0%	11%	74%	;37%	5%	5%	11%	0%
보안 솔루션의 평가 및 조달	0%	5%	68%	63%	32%	0%	5%	0%
보안 솔루션 설치	0%	6%	33%	61%	56%	0%	6%	11%
보안 솔루션 관리	0%	5%	25%	55%	55%	0%	0%	15%
보안 테스팅 (VA, PT)	0%	5%	30%	45%	10%	20%	15%	15%
어플리케이션 보안 테스트, 코드검토	0%	5%	26%	42%	16%	21%	11%	26%
내부감사, 평가 실시 및 관리	0%	0%	22%	33%	6%	83%	11%	6%
정보보호 모니터링	0%	0%	63%	63%	11%	5%	0%	16%
변경 요청의 보안 인증	11%	0%	56%	50%	17%	0%	0%	6%
보안사고 대응	6%	11%	67%	50%	11%	11%	0%	6%
위협/취약점 추적	6%	0%	89%	44%	11%	0%	0%	11%
위험 조치 전략	6%	0%	100%	39%	6%	0%	0%	6%
규제 요구사항 추적	6%	44%	78%	22%	6%	11%	0%	0%
클라이언트 미팅 참여	14%	0%	71%	57%	14%	7%	7%	0%
관리 및 테스트 (BCP/DRP)	50%	0%	60%	25%	50%	5%	0%	0%

2 CISO와 CIO, CPO 및 감사조직과의 관계

▶ 어떠한 역할이든 겸직을 하게 될 경우 확실한 역할 지원 및 보상이 반드시 고려

① CISO와 CIO와의 관계

❍ 2015년 4월에 시행되는 전자금융거래법 개정에 총자산, 종업원 수 등을 감안하여 CISO와 CIO 겸직을 금지함으로 인한 역할간의 충돌에 대한 고민

- IT 조직이 회사의 경영목표 달성을 위해 효율성과 효과성을 극대화하는 조직이라면, 정보보호 조직은 회사 목표 달성에 수반하는 보안위험을 최소화하기 위해 일을 하는 조직

- 두 조직 사이에는 목표 달성을 위해 건강한 갈등이 필연적으로 일어날 수밖에 없고, 아무런 갈등이 없다면 도리어 위험 신호로 간주

- 무엇보다도 IT보안을 위해 두 조직의 협업은 필수불가결하며, 이 협업이 잘 되지 않는다면 회사의 보안위험은 실제 사고로 이어질 가능성이 매우 높기 때문에 그 산하의 IT조직과 정보보호조직 역시 적극적인 협업이 반드시 필요

- 정보보호시스템은 IT조직이 운영하되, 내부통제용 정보보호시스템은 정보보호(보안)부서가 운영하는 것으로 규정

(첫째) 정보보호 내부통제의 대상이 되는 IT운영자가 그 내부통제용 시스템을 운영하는 것은 보안상 문제

(둘째) 현 IT조직의 경험과 역량을 이용하는 것이 IT시스템의 일종인 정보보호시스템을 운영하는 것이 효율적임

(셋째) 정보보호조직의 규모가 크지 않은 상황에서 일반 정보보호시스템을 정보보호조직이 운용한다면 정보보호 인력이 크게 증가

② CISO와 CPO와의 관계

❍ 개인정보보호법에서 CPO 역할을 규정하고 있지만 대부분 겸직을 하고 있기 때문에 어떤 직책을 맡은 사람이 CPO를 겸직하는 것이 가장 효과적인지가 고민

- 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축, 개인정보 보호 교육 계획의 수립 및 시행 및 '개인정보의 안전성 확보조치 기준' 고시에 나타난 업무는 일반적으로 CISO가 수행하는 업무이지만, 개인정보보호법에는 CPO의 업무

- 따라서, 개인정보가 실질적으로 보호되기 위해서는 CPO가 정보보호 솔루션이나 IT보안정책을 관장하는 CISO와 협업하는 것이 필수적임

- CISO와 CPO가 협업을 잘하기 위해서는 두 조직이 정기적인 협의를 통해 현안을 파악하는 일부터 시작

- CISO가 CPO를 맡는다면, CISO는 개인정보 관련법까지 자신의 영역을 확대해야 하며, 개인정보보호 정책을 관장하는 부서로서 개인정보 이용부서와도 활발하게 협의

- 기존 정보보호조직에 관리적 보안업무를 담당하는 인력이 있다면 정보보호 정책업무와 개인정보보호 정책업무는 상당 부분 유사하기 때문에 시너지 발생

③ CISO와 감사조직과의 관계

❍ 정보보호조직의 위상 강화로 인한 감사조직과의 업무 마찰에 대한 고민

- 감사조직과 보안조직의 임무가 다르거나 업무 성격이 상충하는 것은 아니나, 정보보호 강화로 인한 정보보호조직의 보안감사 기능이 필요하다는 의견도 있어서 추후 갈등 요소로 나타날 가능성 존재

- 두 조직 모두 통제조직으로서 성격이 비슷하므로 협업하는 것이 그리 어렵지 않을 것이며, 감사조직의 권위와 정보보호조직의 전문성 결합을 통해 시너지 발생

금융보안 거버넌스 가이드

2019년 12월 인쇄

2019년 12월 발행

발행인 : 김 영 기

발행처 : 금융보안원

경기도 용인시 수지구 대지로 132

전 화 : (02) 3495-9000

〈비 매 품〉

금융보안 거버넌스 가이드

금융보안원
FINANCIAL SECURITY INSTITUTE

(본원) 경기도 용인시 수지구 대지로 132 금융보안원
(교육센터) 서울특별시 영등포구 의사당대로 143 금투센터 8층
TEL 02-3495-9000 FAX 02-3495-9799