방송통신정책연구

10-진흥-라-6

국제표준 사이버보안지수 개발 및 방법론 연구

(A Study on Development and Methodology of Globally Standardized Cybersecurity Index)

2010. 11. 30

연 구 기 관 : 순천향대학교 산학협력단

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

10 I 진흥 I 라 I 6

국제표준 사이버보안지수 개발 및 방법론 연구

2010. 11. 30

순천향대학교 산학협력단

방송통신정책연구
10-진흥-라-6

국제표준 사이버보안지수 개발 및 방법론 연구

(A Study on Development and Methodology of Globally Standardized Cybersecurity Index)

2010. 11. 30

연 구 기 관 : 순천향대학교 산학협력단
총괄책임자 : 염 흥 열 (순천향대학교)

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 **『 국제표준 사이버보안지수 개발 및 방법론 연구 』**의 연구결과보고서로 제출합니다.

2010. 11. 30.

연 구 기 관 : 순천향대학교 산학협력단

총괄책임자 : 염 흥 열 (순천향대학교)

참여연구원 : 여 돈 구 (순천향대학교)

이 동 희 (순천향대학교)

이 상 래 (순천향대학교)

장 기 헌 (순천향대학교)

장 재 훈 (순천향대학교)

정 영 곤 (순천향대학교)

최 현 우 (순천향대학교)

요 약 문

1. 제목

○ 국제표준 사이버 보안지수 개발 및 방법론 연구

2. 연구의 목적 및 중요성

○ 연구목표 : 글로벌한 사이버 보안 지수 개발 및 국제 표준화 추진

○ 정보통신분야에는 국제전기통신연합(ITU, International Telecommunication Union)의 DI(Development Index)와 세계경제포럼(WEF, The World Economics Forum)의 NRI(Network Readiness Index), 세계경제협력기구(OECD, Organisation for Economic Cooperation and Development)의 CO(Communication Outlook) 등의 국제적인 평가 기준이 개발되어 있지만, 정보보호분야의 국제적인 사이버 보안 지수는 개발되지 않은 상태임

○ 현재 세계경제포럼과 세계경제협력기구에서 시행하고 있는 보안 평가 지표는 보안 서버의 개수만을 이용하므로, 변화하는 정보보안 서비스와 각국의 정보보호 수준을 평가할 수 있는 지표로는 턱없이 부족한 실정임. 따라서 정보보호 지수의 평가를 위해 사이버 보안 지수는 원시 데이터의 신뢰성을 확보할 수 있는 적절한 대표적인 지표가 선정되어야 하며, 정보보호 정책의 집행 효과를 측정하기 위한 글로벌 차원의 사이버 보안 지수 또는 정보보호 지수의 개발이 시급히 요구됨

○ 본 연구는 국내·외 정보보호수준 평가 연구에서 벗어나 국제 정보보호분야의 표준화 전문가들의 합의 하에 글로벌한 정보보호수준 평가 지표 개발이 시작된다는 점에서 기존의 연구와 차별화됨.

3. 연구의 구성 및 범위

○ 국내외 정보보호 평가 지표 현황 분석
○ 정보보호 서비스 및 관련 기술의 변화를 반영할 수 있는 지표 개발
○ 다양한 지표들을 지수화하기 위한 효과적인 방법론 개발
○ 국제 표준화를 위한 권고초안 작성

4. 연구내용 및 결과

○ 국제표준 사이버보안지수 지표 개발 관련 학술논문 1편
○ 국가정보보호지수 개선 연구 관련 학술논문 1편
○ 국내·외 정보보호 수준 평가 체계 및 지표 동향 관련 학회지 1편
○ 사이버보안지수(X.csi)의 가이드라인을 위한 신규 워크아이템 선정(ITU-T SG17, 2010.4)
○ X.csi의 1차 권고 초안 제출(Tokyo Q.4 인트림 회의, 2010.10)
○ X.csi의 2차 권고 초안 제출(ITU-T SG17, 2010.12)

5. 정책적 활용내용

○ 국가정보보호지수의 국제 표준화 추진을 위한 기반 마련
○ 국가 단위뿐만 아니라 조직 단위의 정보보호 수준을 평가하는 데 활용
○ 개발된 지수를 통해 국가별 집중 투자가 필요한 분야를 식별 가능
○ 국가차원의 정보보호 관련 예산의 확보와 중장기적인 정보보호 정책 수립에 활용

6. 기대효과

○ 장기적으로 개발될 지수를 활용해 국제전기통신연합(ITU-T)으로 하여금 향후에 국가별 정보보호 수준 현황을 파악하고, 이를 등급화 하는데 활용 가능함

○ 국내 실정을 반영할 수 있는 사이버보안 지수의 국제 표준화 추진

○ 추후 국제 표준으로 승인될 경우 한국의 정보보호 수준 향상에 도움이 될 것으로 판단

○ 빠르게 변화하는 정보보호 이슈 및 개발도상국의 상황을 고려할 수 있는 신뢰성 있는 합의된 사이버 보안 지수를 개발할 수 있을 것으로 기대됨

○ 지수의 평가를 통해 정보보호 인식제고를 위한 교육 및 홍보에 이용될 것으로 기대됨

○ 정보보호 전반에 대한 정량적 집계가 가능하므로 국가의 정보보호 수준을 객관적이고 지속적으로 평가할 수 있음

SUMMARY

1. Title

A Study on Development and Methodology of Globally standardized Cybersecurity Index.

2. Objective and Importance of Research

○ Objective of the research: The development of a global standardized cybersecurity index and performance of international cybersecurity index in global standard body, ITU-T

○ The Development Index, the Networks Readiness Index and the Communication Outlook have been developed in an information communication area by the International Telecommunication Union, the world Economics Forum, the Organization of Economic Cooperation and Development, respectively. Note, however, that there is no international agreed-upon cybersecurityi index in an information security area.

○ The security indicator of the WEF and the OECD consider only the number of specific vendor's SSL(Secure Socket Layer) certificates to measure the level of the information security. It is also not enough for measuring the current level of the fastest growing information security services and a country's information security. For measuring of the level of information security, therefore, global agreed-upon cybersecurity indicators needs to be developed for ensuring accuracy, reliability and integrity of raw data. The development of Cybersecurity Index or Information Security Index for measuring the effectiveness of the enforcement of information security

policies is urgently required.

○ The difference of this research lie in that it not only researches on information security index taking into those of domestic and foreign countries, but also focus on standardiing this cybersecurity index by global Standardization Experts in ITU-T.

3. Contents and Scope of the Research

○ Analysis of indicators for existing domestic and international information security index

○ Development of information security indicators, which can reflect rapid changes of fastest growing information services and related technologies.

○ Development of an efficient methodology for cybersecurity index consisting of the various indicators

○ Completing a draft Recommendation ITU-T X.csi for the cybersecurity index for the international standardization.

4. Research Results

○ A papers on the development of international standards related to cybersecurity.

○ A paper on the improvement of national information security index .

○ A paper on the trends of measuring system and indicators of domestic and international information systems and indicators.

○ A proposal for establishing a new work item on guidelines for Cybersecurity Index(CSI)

○ The initial text on ITU-T X.csi : Guidelines for cybersecurity index(ITU-T SG17, 2010.4)

○ Proposal for a revised initial text on ITU-T draft Recommendation X.csi Guidelines for cybersecurity index.(Tokyo ITU-T SG17 Q.4 interim meeting, 2010.10)

○ The 1st draft text on Recommendation ITU-T X.csi: Guidelines for cybersecurity index.(ITU-T SG17, 2010.12)

5. Policy Suggestions for Practical Use

○ Establish a foundation for international standardization for National Information Security Index.

○ Used for measuring the level of information security in national level or organizational level.

○ Used to identify a specific area that needs to be invested by government of organization.

○ Used to identify area that needs budget investment or policy making related to information security in national level.

6. Expectations

○ The cybersecurity index developed by the International Telecommunication Union (ITU-T) can be used to measure the level of current information security in the country level or organizational level.

○ Performing standardization activity for the cybersecurity index for reflecting domestic circumstances.

○ The cybersecurity index can be used to improve the level of information security in Korea, if approved as an international standard.

○ The Cybersecurity index considering rapidly-changing information security issues and situation expects to be used by developing countries.

○ The Cybersecurity index can be used to improve the public awareness through indicator evaluation.

○ The Cybersecurity index can evaluate the level of information security in the national level by using the figure evaluated quantitatively

목 차

Contents

표 목 차

그 림 목 차

제 1 장 개 요

지난 2009년 국제전기통신연합(ITU), 세계경제포럼(WEF), 세계경제협력기구(OECD) 등의 정보통신관련 지수 결과는 정보통신 한국의 정보화능력이 세계적인 수준임을 보여주었다. 급속한 정보화 사회의 발전은 다른 산업의 성장의 원동력이 되었으며, 10대~30대 국민의 99%가 인터넷을 이용하는 현실은 이미 인터넷은 우리 생활의 일부가 되었음을 보여주고. 하지만, 급속한 정보화 과정에서 2005년 리니지2-인정보유출사고, 2008년 옥션-중국발 해킹사고, 2008년 LGT/GS칼텍스-개인정보유출사고, 2009년 7·7 DDoS 공격 등 정보화 악영향으로 인한 사회적 불안감은 커져만 가고 있다.

이와 같은 보안 사고들이 증가하면서 기업 및 국가의 정보보호에 대한 관심과 투자가 증가하고 있다. 기업의 경우, 기업정보 및 고객정보에 대한 관리 수준을 인정받기 위해 ISO 27001, K-ISMS(KISA-Information Security Management Systems), PIMS 등 다양한 정보보호평가 체계를 이용하고 있으며 국가의 경우, 안전한 정보통신 프레임워크를 제공하기 위하여 국가 차원의 정보보호대책을 수립하고 주요정보통신시설 및 공공기관의 안전성 확보를 위하여 주기적인 점검활동을 수행 중에 있다.

또한, 표준화 기구인 국제전기통신연합(ITU), 세계경제포럼(WEF), 세계경제협력기구(OECD 등은 국가차원의 정보화 발전 추세 및 정보보호수준 등을 평가하기 위한 지표를 공개하고, 각국에서 수집된 데이터를 바탕으로 매년 각국의 평가지수를 공개하고 있으며, 이 결과는 국가의 정보화 정책을 수립하는데 중요한 요소로 작용하고 있다. 하지만, 국가의 정보보호 수준측정을 위해 사용하는 지표는 '인구 수당 인터넷 보안서버의 수'만을 이용하고 있기 때문에 국가의 전반적인 정보보호 수준을 반영하지 못하는 문제점이 있다.

정보보호 수준을 평가하는 지표가 국제 표준화기구에만 있는 것은 아니다. 비록 표준화되어 사용되고 있지는 않지만 미국의 NIST, 한국의 KISA, 영국의 BERR 등의 국가별 기구에서 자체적으로 개발되어 사용되고 있는 정보보호 수준측정 지표들이 있다. 하지만 '국가별 지표의 다양성', '평가영역의 한계성' 및 '참여국의 제한' 등의 문제로 인해 국제적 지표로

이용하기에는 어려움이 있다. 이는 글로벌한 정보보호 평가지수 개발을 위해서 반드시 국제적인 표준화기구의 역할의 조율이 필요함을 의미한다.

2010년 (ITU-T, International Telecommunications Union - Telecommunication Standardization Sector) SG17(Study Group 17) 스위스 제네바 회의에서 국가차원의 정보보호수준 평가지표의 개발의 필요성을 담은 기고서를 제안(순천향대학교 염흥열 교수와 한국인터넷진흥원 송혜인 연구원)하였고, 신규 표준화 워크아이템으로 채택되었다. 이에 X.csi의 메인 에디터로 선정된 순천향대 염흥열 교수가 본 과제의 연구책임을 맡게 되었다. 본 과제에서는 조직 및 국가의 정보보호 수준을 평가할 수 있는 지수 개발하는데 있어 국내 정보보호 평가체계의 평가지표를 반영하여 앞으로 X.csi가 국제표준으로 승인될 경우, 한국의 정보보호 평가수행을 수월하게하고 우수한 국내 정보보호 수준을 국제적으로 인정받을 수 있게 하는데 목적이 있다.

제 1 절 연구의 필요성

정보통신분야의 국제 표준화 기구인 국제전기통신연합(ITU)의 개발지수(Development Index), 세계경제포럼(WEF)의 네트워크 준비지수(Network Readiness Index), 세계경제협력기구(OECD)의 통신전망(Communication Outlook)등 평가 기준이 제정되어 있지만, 국가 차원의 정보보호분야의 전반을 측정할 수 있는 표준화된 지표는 개발되지 않은 상태이다. 현재 세계경제포럼과 세계경제협력기구에서 시행하고 있는 정보보호 평가지표는 보안 서버의 개수만을 이용하므로, 변화하는 정보보안 서비스 및 관련 기술의 변화를 측정할 수 있는 지표로는 턱없이 부족한 실정이다.

국가별로 개발된 보안 지표들은 각 국가의 정보통신 서비스 및 관련 기술의 변화에 맞게 개발되었기 때문에 이를 국제적으로 이용하는데 있어 일관성 및 신뢰성을 보장할 수 없다. 반면, NIST(National Institute of Standards and Technology)나 KISA(Korea Internet & Security Agency)의 경우, 국가의 정보보호 현황을 체계적으로 분석할 수 있지만 국제적으로 합의에 도달하지 못했기 때문에 국제적으로 널리 이용되지 못하는 실정이다. 따라서 정보보호 지수의 평가를 위한 원시 데이터의 신뢰성을 확보하면서 정보보호 수준을 측정할 수 있는 가장 적절한 대표적인 지표가 선정되어야 하며, 정보보호 정책의 집행 효과를 측정하기 위한 글로벌 차원의 사이버 보안 지수 또는 정보보호 지수의 개발이 시급히 요구된다.

본 과제는 지표 개발은 물론, 개발된 지표를 국제 정보보호분야의 표준화 전문가들의 합의 하에 글로벌한 정보보호수준 평가 지표 개발이 시작된다는 점에서 기존의 연구와 차별화된 독창성을 보인다.

제 2 절 연구개발의 목적 및 범위

1. 연구 개발의 목적

○ 연구목표 : 글로벌한 사이버 보안 지수 개발 및 국제 표준화 추진

정보보호 지수의 평가를 위한 원시 데이터의 신뢰성을 확보하면서 사이버 보안 지수를 가장 적절한 대표적인 지표가 선정되어야 하며, 정보보호 정책의 집행 효과를 측정하기 위한 글로벌 차원의 사이버 보안 지수 또는 정보보호 지수의 개발이 시급히 요구된다.

국내·외 정보보호 인증체계 및 관련 정보보호 지표를 분석하여 객관적인 데이터를 수집할 수 있는 지표를 성정 및 개발하고 그 결과를 표준화에 반영한다. 또한, 국가정보보호지수 및 국내의 우수 지표들을 최대한 반영하여 국내 정보보호 지표의 국제 표준화를 추진한다.

2. 내용 및 범위

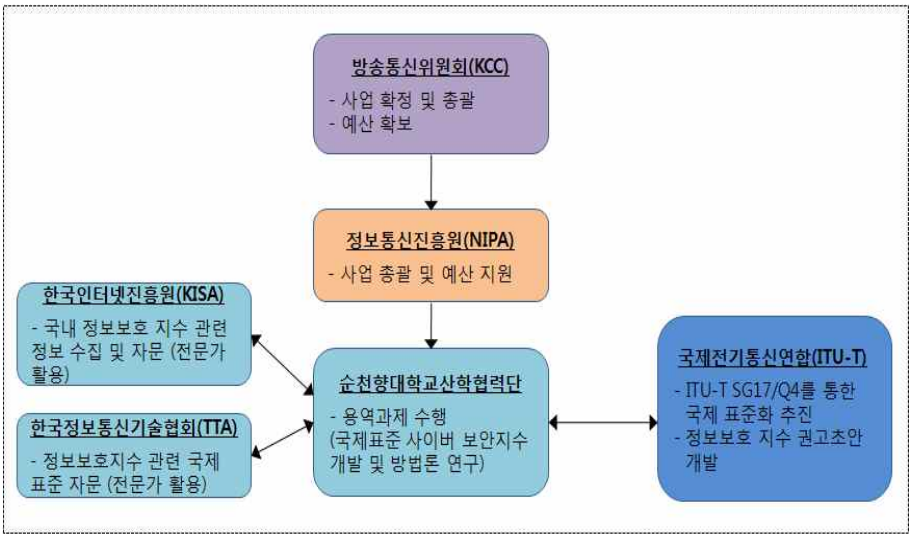
본 과제의 연구 내용 및 연구 범위는 다음과 같으며, 크게 사이버 보안지수 지표 개발 부문과 사이버 보안 지수의 표준화 추진 부문으로 나눌 수 있다.

○ 사이버 보안지수의 지표 개발 및 방법론 연구 부문
- 국내외 정보보호 평가 지표 현황 분석
- 정보보호 서비스 및 관련 기술의 변화를 반영할 수 있는 지표 개발
- 다양한 지표들을 지수화하기 위한 효과적인 방법론 개발

○ 사이버 보안지수의 국제 표준화 추진 부문
- 정보보호 지표 관련 국제 표준화 추진을 위한 신규 아이템 채택 추진
- 사이버 보안지수(X.csi) 권고안에 개발된 지표 반영
- 사이버 보안지수(X.csi) 권고안에 정보보호지수의 평가지표를 Annex로 반영

제 3 절 연구의 추진방법

1. 사업 수행체계



[그림 1] 사업 수행체계

2. 사업 수행방법

○ ITU-T 국제 표준화 회의를 통해 국제적으로 국가 및 조직에 대한 정보보호 수준 평가를 위한 글로벌한 공통 기준 개발의 필요성을 제안하여 국제 표준화 기구를 통한 사이버 보안 지수의 개발의 기반을 마련

- ITU-T SG17 내에 사이버 보안지수 개발을 위한 워킹그룹 신설로 국가적 차원의 정보보호 평가지수를 개발하기 위한 환경 조성

○ ITU-T 국제 표준화 회의에 참여하여 회원국에서 제안하는 관련 지표 수집 및 분석

- 국외 : 미국, 영국, 대만 등
- 국내 : K-ISMS, G-ISMS, 국가정보보호지수 등 다수

○ 정보보호 서비스 및 기술의 급격한 변화를 반영할 수 있는 지표 및 방법론 개발

- 수집 및 분석된 내용을 바탕으로 사이버 보안지수 지표 초안 도출
- 관련 분야 전문가 풀을 이용하여 개발된 지표의 개선 사항 도출(설문조사 실시)
- 관련 평가 지표들에서 사용 중인 방법론을 분석하고, 그 결과를 바탕으로 개발된 지표의 지수화를 위한 방법론 조사

○ 방송통신위원회, 한국인터넷진흥원, 한국정보통신기술협회의 전문가들로 구성된 운영위원회의를 주기적으로 개최하여 과제 진행사항을 확인

○ 사이버 보안지수의 국제 표준화 추진

- 방송통신위원회, 한국인터넷진흥원, 한국정보통신기술협회의 전문가들과 협조하여 국제 표준화를 위한 권고초안 개발
- 국가정보보호지수의 평가 지표를 Annex로 추가
- 장기적으로 3년간 사이버 보안지수의 표준화 추진
- 2010년 1차적으로 조직 단위의 표준화 추진 이후, 국가 단위의 표준화 추진 예정

제 1 장 정보보호 수준평가 관련 연구

제 1 절 국내 정보보호 수준평가 체계 및 지표

2008년 2월 정부조직개편에 따라 정보보호업무가 방송통신위원회, 지식경제부, 행정안전부로 이관되었으며, 정보통신기반시설 총괄은 행정안전부가, 정보보호컨설팅 전문업체 지정은 지식경제부가, 민간분야의 정보통신기반시설 총괄은 방송통신위원회가 담당하게 되었다. 현재 국내에서 시행 중인 정보보호 관련 체계 및 평가 지표는 시행 주체를 기준으로 크게 정부와 민간으로 나누어 볼 수 있다.

평가 대상을 기준으로 살펴보면 공공·행정기관을 대상으로 하는 체계 및 평가 지표로 정보보안 관리수준 평가, G-ISMS(Government-Information Security Management Systems), 공공기관 개인정보보호수준 진단, PIA(Privacy Impact Assessment)-공공/기업 등이 해당된다. 다음으로 기업을 대상으로 하는 체계 및 평가 체계 및 지표로 K-ISMS, PIMS(Personal Information Management System), 정보보호 안전진단, PIA-기업, eTrust가 있다. 국가정보보호지수의 경우 평가 대상으로 정부, 기업, 개인 부문을 모두 포함하고 있어 국가 전반의 정보보호수준을 평가할 수 있다.

정부의 경우, 민간보다 체계화된 정보보호 평가정책을 운영하는 것을 살펴볼 수 있으며, 일부를 제외하고 시행 법률에 기반을 두고 있어 정부나 기업의 관심 및 참여를 높이는 결과를 가져왔다.

민간의 경우, 정부 주체의 정보보호 관련 체계 및 평가 지표와 비교해볼 때 평가영역이 다소 제한적이며, 법률적 근거를 두지 않고 있는 경우가 많아 평가 대상의 자율적 참여로 이루어지고 있다. 주로 평가대상은 전자상거래와 관련된 업종 군으로 웹 사이트를 활용하는 조직이 수집·취급·관리하고 있는 개인정보보호 및 전자상거래 구매 과정에 대한 안전성 여부를 평가하고 있다.

1. K-ISMS

가. 의의

K-ISMS는 2002년 ISO/IEC 27001을 기반으로 국내 실정에 맞도록 개발된 정보보호 관리체계 인증제도(Information Security Management Systems)이다. 정보보호 관리체계 인증제도란 정보통신서비스제공자가 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 수립·운영하고 있는 기술적·물리적 보호조치를 포함한 종합적 관리체계를 말한다.

나. 목적

본 제도는 “정보통신망이용촉진및정보보호등에관한법률” 제47조, “정보통신망이용촉진및정보보호등에관한법률시행령” 제50조, 정보보호관리체계인증 등에 관한 고시(제2008-11호)에 근거하여 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화 하고 지속적으로 관리·운영하는 시스템을 운영하는 조직에 대해 안전성을 보장하는 인증서를 발급하고 있다.

(1) 데이터의 기밀성(Confidentiality) : 정보가 특정 권한을 부여받은 인가된 사용자에만 접근 및 공개됨을 보장해야 한다.
(2) 데이터의 무결성(Integrity) : 정보가 부적절한 방법에 의해 데이터가 변경되지 않았음을 보장한다.
(3) 데이터의 가용성(Availability) : 정보가 적절한 방법을 통해 특정 권한을 부여받은 인가된 사용자에게만 제공됨을 보장해야 한다.

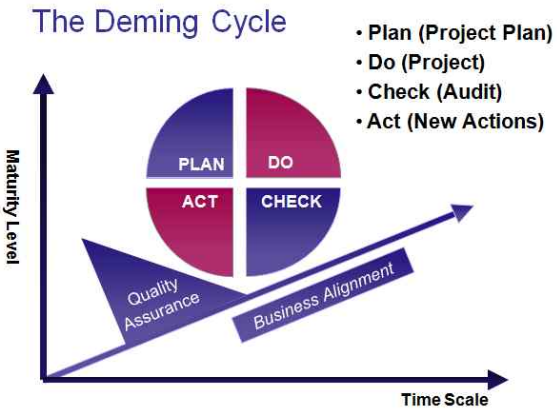
정보보호 관리체계 인증제도는 한국인터넷진흥원이 제3자의 객관적이고 독립적인 입장에서 평가 대상 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 통해 정보보호대책들이 적절성에 대해 평가하고, 정보보호 관리체계 인증제도기준에 대한 적합성 여부를 보증함으로써 조직의 정보자산의 신뢰성 향상 및 정

보보호관리에 대한 인식 제고와 더불어 국제적 신뢰도 향상시킨다. 나아가 본 제도의 활성화를 통하여 정보보호서비스 산업의 활성화를 도모함을 목적으로 한다.

다. 관리체계의 개념

정보보호 관리체계 인증제도는 ISO 9000의 품질경영에서 다루는 PDCA(Plan, Do, Check, Act) 사이클에 따라 조직 내부의 정보보호 관리체계가 문서화되고 이에 따라 적절하게 관리되고 있는지 여부를 확인하게 된다. 즉, 정보보호 정책을 수립(Plan)하고 수립된 정책을 이행(Do)를 거쳐, 정책이 올바로 수행되었는지 검토(Check)하는 과정을 거친다. 마지막으로 반영(Act) 단계에서는 검토 결과에 대한 보완 계획을 차후 수립 단계에 반영하게 된다. 이렇게 조직은 PDCA 사이클을 반복함으로써 조직의 정보보호 목표를 점층적으로 향상시키는 결과를 가져오게 된다.

정보보호 측면에서 PDCA 사이클은 (1) 조직의 정보자산을 보호하기 위한 목표와 전략 수립 및 전담 조직을 구성하는 정보보호 정책 수립(Plan)단계, (2) 정보보호 목표 및 전략에 따른 구현 및 운영과 정책 이행에 따른 모니터링 과정을 포함하는 정책이 이행(Do)하는 단계, (3) 정보보호 정책 대비 수행 여부를 점검하고 시정조치 계획을 수립하는 검토(Check)단계, (4) 시정조치 계획을 다음 사이클의 정보보호 정책에 반영하는 단계로 적용될 수 있다.



[그림 2] PDCA Cycle

라. 대상 및 범위

정보보호 관리체계 인증제도는 개인정보를 취급하고 있는 모든 민간기업을 대상으로 하고 있다. 예를 들면 공공기관의 입찰에 참여하는 기업·금융·교육·의료기관·통신업체 등 주요 자산을 취급하는 기업, 또는 이들 기업의 정보를 위탁·관리·가공·이용하는 아웃소싱업체들 또한 그 대상이 될 수 있다.

인증 범위는 전체 조직을 대상으로 하는 정보보호 관리체계 인증을 권고하지만, 조직의 상황에 따라 그 범위를 조직의 일부로 제한할 수 있다. 단, 한 조직이 조직의 일부를 추가로 인증 받는다고 해서 인증서의 개수가 증가되는 것은 아니며 기존 인증서의 인증 범위가 확대되게 된다.

마. 심사과정

본 인증을 유지하기 위한 심사과정은 4단계로 구분될 수 있다. 정보보호관리체계 인증 취득을 위한 최초심사, 정보보호관리체계 내의 심각한 변경이 발생한 경우 이루어지는 재심사, 정보보호관리체계를 지속적으로 유지하기 위해 주기적으로 이루어지는 사후관리심사 마지막으로 유효기간 만료 이후 정보보호관리체계의 인증을 유지하기 위한 갱신심사로 구분된다. 이 같은 심사과정은 ISO/IEC 27001을 모델로 정보보호관리체계에 동일하게 적용되는 부분이라고 할 수 있다.

바. 특징

K-ISMS는 15개 영역 120개의 통제항목과 396개의 세부통제항목으로 구성되어 있고, 기존 ISO/IEC 27001과의 비교해볼 때, 국내 실정을 반영하기 위하여서 정보보호 교육 및 훈련, 암호통제, 전자거래보안 영역 등이 추가되었다. 인증 제도의 활성화를 위해 인증서를 획득한 기업들에게는 정보보호 관련 보험 가입 시 요금 할인, 가산점 부여, 정보보호 안전진

단 면제 등의 혜택이 주어지고 있으며, 2010년부터는 매출액 50억 미만이나 종업원 수 50명 미만인 업체가 ISMS를 취득할 경우 최대 50%의 인증수수료를 인하하여 비용적 측면에서 부담이 되는 소규모 사업자의 참여를 지원하고 있다.

사. 지표구성

통제분야	통제내용	통제사항 수	세부통제사항 수
정보보호대책	1. 정보보호정책	5	10
	2. 정보보호조직	4	11
	3. 외부자 보안	4	8
	4. 정보자산 분류	4	7
	5. 정보보호 교육 및 훈련	4	14
	6. 인적 보안	5	18
	7. 물리적 보안	12	36
	8. 시스템개발 보안	13	53
	9. 암호 통제	3	6
	10. 접근 통제	14	38
	11. 운영관리	22	99
	12. 전자거래 보안	5	21
	13. 보안사고 관리	7	20
	14. 검토, 모니터링 및 감사	11	37
	15. 업무 연속성 관리	7	18
소계		**120**	**396**

[그림 3] K-ISMS 평가 지표

2. G-ISMS

가. 의의

G-ISMS 인증제도는 2009년 12월 행정안전부의 '전자정부 정보보호관리체계 인증업무 지침'에 따라 지자체에 대해 정보보호 관리과정, 문서화, 정보보호 대책 등 정보보호체계가 적절하게 수립·관리되고 있는지를 평가해 인증하는 제도다.

나. 목적

행정기관의 정보보호관리 수준을 보다 객관적이고 체계적으로 점검·관리하기 위해 행정안전부와 한국인터넷진흥원(KISA)이 주관해 인증심사 및 인증서를 발급하고 있다.

다. 대상 및 범위

행정안전부 훈령 제164호 인증심사기준에 의거하여 30개의 전자정부 대민서비스, 광역·기초자치단체의 대민서비스 및 대학·특수법인에서 제공하는 주요 서비스를 대상으로 하며, 2009년 12월 전자정부 정보관리체계 인증지침이 훈령으로 제정됨에 따라 전자정부 대민서비스를 제공하는 행정기관은 G-ISMS를 의무적으로 인증을 받아야 한다.

인증 범위는 전체 조직을 대상으로 하는 정보보호 관리체계 인증을 권고하지만, 조직의 상황에 따라 그 범위를 조직의 일부로 제한할 수 있다. 단, 한 조직이 조직의 일부를 추가로 인증 받는다고 해서 인증서의 개수가 증가되는 것은 아니며 기존 인증서의 인증 범위가 확대되게 된다.

라. 심사과정

인증기관이 G-ISMS의 인증기준으로 심사를 실시하게 되며, 서면 심사와 기술 심사를 진행하게 된다.

서면심사는 인증기관에서 신청기관이 제출한 신청서류를 확인하여 신청기관이 수립·운영하고 있는 G-ISMS가 인증심사기준에 적합한지에 대하여 심사하는 것이고, 기술심사는 인증기관에서 서면심사의 결과를 검증하기 위하여 신청기관이 인증을 신청한 G-ISMS가 운영 중인 현장을 방문하여 직접 해당 정보보호관리체계의 구축·운영 실태를 확인하는 것이다. 또한 인증기관은 기술 심사를 위하여 현장 방문시 신청기관의 요청이 있는 경우 인터넷 침해사고 등에 대한 안전성 검사를 위하여 해당 정보보호관리체계에 속한 정보시스템에 대한 모의진단을 실시할 수 있다.

본 인증을 유지하기 위한 심사과정은 4단계로 구분될 수 있다. 정보보호관리체계 인증 취득을 위한 최초심사, 정보보호관리체계 내의 심각한 변경이 발생한 경우 이루어지는 재심사, 정보보호관리체계를 지속적으로 유지하기 위해 주기적으로 이루어지는 사후관리심사 마지막으로 유효기간 만료 이후 정보보호관리체계의 인증을 유지하기 위한 갱신심사로 구분된다. 이 같은 심사과정은 ISO/IEC 27001을 모델로 정보보호관리체계에 동일하게 적용되는 부분이라고 할 수 있다.

마. 특징

G-ISMS는 ISO 27001의 11개 영역 126개 통제 항목을 기반으로 하되 공적기관의 암호화 알고리즘 업무 중복 및 개인정보보호관련 영역 분리로 2개의 세부항목(개인정보보호 및 암호화 관련 법규)이 제외되었다. 이후 시험인증 과정에서 암호화·개인정보보호·포렌식·취약점 관리 등에 대한 보안 점검 지침들이 아예 없거나 또는 구체적이지 못한 것으로 지적됨에 따라, 이러한 사항을 수정하고 2010년 6월에 총 12개 영역 44개 통제사항, 156개의 통제사항으로 개정되었다.

2010년 12월까지 정부통합전산센터, 광주정부통합전산센터, 서울시청, 관악구청 등이 G-ISMS 인증을 취득하였다.

바. 지표구성

통제분야	통제내용	통제사항 수	세부통제사항 수
정보보호대책	1. 정보보호정책	1	2
	2. 정보보호조직	1	8
	3. 자산관리	2	5
	4. 인적 보안	4	12
	5. 물리적 보안	2	13
	6. 통신 및 운영관리	10	32
	7. 접근통제	7	25
	8. 정보시스템 요구사항, 개발, 및 유지보수	6	16
	9. 보안사고관리	2	5
	10. 업무연속성관리	1	5
	11. 준거성	3	8
	12. 개인정보보호	5	25
소계		**44**	**156**

[그림 4] G-ISMS 평가 지표

3. 정보보안관리 수준평가

가. 의의

정보보호관리수준 평가는 국가사이버안전관리규정 제9조 제4항에 의거 사이버안전대책의 강구여부 등 정보통신망에 대한 안전성을 확인하기 위해 각급기관이 정보시스템의 중요도에 따라 소용되는 보안대책을 적절히 강구하고 있는지를 평가한다.

나. 목적

각급기관 스스로 정보보안수준을 진단할 수 있는 능력을 배양하고 보안대책이 미흡한 부분이나 정보보안 사각지대를 해소함으로써 국가 사이버안전을 확보하는데 목적이 있다.

다. 대상 및 범위

지방자치단체 및 공공기관의 정보통신망에 대하여 실시한다.

라. 심사과정

각급기관의 장은 국가사이버안전매뉴얼의 기관(정보통신망)분류 방법을 참고하여 '가'급, '나'급, '다'급으로 분류한 후, 각급기관의 장은 분류결과 및 근거를 국가정보원장에게 통보한다. 국가정보원장은 각급기관의 장이 통보해온 분류결과를 심의하고 그 결과를 각급기관의 장에게 통보한다.

각급기관의 장은 기관분류에 영향을 미치는 변경이 있을 시, 다시 기관분류를 수행하여 그 결과와 근거를 국가정보원장에게 통보한다.

마. 특징

중요도에 따라 보안대책의 강도를 달리하여 정보통신망을 보호하고 있으며, 이를 위해 각 기관별로 등급을 분류하고 차별화된 기준을 적용하도록 하고 있다.

기관분류의 기준은 수행업무의 중요도, 정보시스템 및 정보의 중요도 그리고 피해분석으로 구성되어 있으며, 각급기관의 정보통신망의 중요도는 해당 기관이 분류기준을 적용하여 자체 평가한 후, 중앙 행정기관이 검토하고 국가정보원에 통보하는 형식이다.

기관분류 기준	평가요소	평가점수			가중치	평가수준
수행업무의 중요도	수행업무의 국가사회적 중요도	VH	H	M	3	가급: 31~39 나급: 21~30 다급: 13~20
		3	2	1		
	인원 및 서버 규모	VH	H	M	1	
		3	2	1		
정보시스템 및 정보중요도	정보중요도	VH	H	M	3	
		3	2	1		
	정보시스템 의존도	VH	H	M	1	
		3	2	1		
	대외업무연계 정도	VH	H	M	1	
		3	2	1		
피해분석	위협발생 가능성	VH	H	M	2	
		3	2	1		
	피해영향 정도	VH	H	M	2	
		3	2	1		

[그림 5] 기관분류 기준

이 분류에 따라 점검 항목을 차등적으로 적용하기 위하여, 점검항목을 A, B, C 항목으로 분류하고 있다.

(1) A항목 : 모든 기관이 필수적으로 수행해야 할 항목

(2) B항목 : 중요 정보통신망을 운영하는 기관이 추가 수행해야 할 항목

(3) C항목 : 매우 중요한 정보통신망을 운영하는 기관이 추가 수행해야 할 항목

기관 분류 결과에 따라 다음과 같이 차별화된 점검항목을 적용한다.

(1) '가'급 기관 : A, B, C 항목을 모두 적용
(2) '나'급 기관 : A, B 항목을 모두 적용
(3) '다'급 기관 : A 항목을 모두 적용

바. 지표구성

대분류	중분류	소분류	A	B	C
1. 정보보안 관리체계	2	5	7	6	3
2. 정보보안계획 및 활동	4	8	14	9	1
3. 정보자산통제	3	7	14	2	4
4. 인적 보안	3	6	13	4	1
5. 물리적 보안	2	10	13	12	5
6. 접근 보안대책	5	17	18	25	13
7. 운영관리	7	12	28	13	3
8. 시스템 개발 및 유지보수	3	7	6	12	1
9. 보안시스템	4	9	26	0	0
소계	**66**	**160**	**139**	**83**	**31**

[그림 6] 정보보안관리 수준평가 평가 지표

4. 전자정부서비스 보안수준 실태조사

가. 의의

전자정부법 제39조 2항에 의거하여 전자정부서비스의 종합적인 보안대책 수립을 위해 전반적인 보안수준 실태조사의 필요선이 대두되었고, 전자정부서비스를 유형별로 분류하고 유형별로 보안대책을 수립하여 체계적인 보안관리 적용의 기준을 마련한다.

나. 목적

전자정부서비스 보안수준 실태조사는 다음과 같은 목적을 두고 있다.

(1) 전자정부 대민서비스 보안 수준측정 지표 개발 : 전자정부 대민서비스 보안관리 기준을 제공할 수 있는 보안수준 측정지표와 측정 프로세스를 개발하고 전자정부 보안 관련 법령/지침/기준 등을 반영하여 민원인 PC 구간, 전송 구간, 보안시스템 구간, Web/App 구간, DB 구간 지표 개발 방향을 수립한다.

(2) 전자정부 대민서비스 보안수준 측정 실시 : 전자정부 대민서비스에 대한 심층분석과 서류조사 및 인터뷰를 통해 보안수준을 측정한다.

(3) 전자정부 대민서비스 보안대책 수립 : 전자정부 대민서비스에 대한 종합보안대책 수립 및 관리적/제도적 측면의 전자정부 보안관리체계를 수립한다. 또한 대민서비스 보안관리 강화를 위한 법/제도 개선 방안 마련한다.

다. 대상 및 범위

대상은 정부 기관을 중앙행정 기관과 지방행정 기관으로 구분하고 중앙행정 기관에서는 주요 대민서비스를 제공하는 기관 중 대표적인 기관을 대상으로 하며, 지방행정 기관에서는 16개 시도/시군구 232개 시군구를 대상으로 한다.

조사 범위는 중앙행정 기관, 지방행정 기관의 전자정부 대민서비스 및 주요 행정정보 서비스, 홈페이지를 대상으로 한다.

라. 심사과정

조사대상 기관으로 선정된 기관을 대상으로 1차 서면조사를 실시한 후, 일부 기관 및 서비스를 선정하여 방문을 통한 심층조사를 실시한다. 그리고 서비스 정보 및 서비스 유형에 따른 요구되는 보안 기능별 연계 조사를 실시한다.

마. 특징

다양한 종류의 전자정부서비스에 대하여 등급을 분류하는 프레임워크가 존재하며, 보안등급에 따라 보안관리 기준을 적용한다.

등급별 서비스에 대해 적용시켜야 할 보안기술 적용 요소는 1등급으로부터 5등급까지 차례대로 필수기준, 권고기준, 선택기준 사항을 차별화 적용하여야 하며 온라인거래서비스와 증명서 열람/발급서비스 보안 기준은 해당 서비스 제공시 적용하여야 한다.

등급분류 기준	평가요소	배점	가중치	등급분류
서비스의 국가, 사회적 중요도	국가안보/국가단위 핵심행정/전 국민데이터 보유 업무	5	5	1등급: 50~60 2등급: 40~49 3등급 30~39 4등급: 20~29 5등급: 19미만
	국가경제/국가단위 행정/다수 국민데이터 보유 업무	4		
	국민행정/다수 국민데이터 보유 업무	3		
	광역자치규모행정/일부 국민 데이터보유 업무	2		
	기타 대 국민생활 관련	1		
서비스 사고 발생시 피해 영향도	전 국민 생활에 피해	5	5	
	대규모 지역주민 생활에 피해(특별시, 광역시 도 단위 또는 50만명 이상)	4		
	중규모 지역주민 생활에 피해(시 단위, 광역시 구 단위 지역 또는 인구수 20만명 이상 50만명 미만)	3		
	소규모 지역주민 생활에 피해(시군구 단위 지역 또는 10만명 이상 20만명 미만)	2		
	소규모 지역주민 생활에 피해(시군구 단위 지역 또는 10만명 미만)	1		
수행 서비스의 온라인 의존도	- 일일 평균 접속건수가 10,000건 이상인 서비스 - 금융거래 등 온라인 거래와 각종 증명서 열람 및 발급 기능을 제공하는 서비스	5	2	
	- 일일 평균 접속건수가 5,000건 ~ 9,999건 이하인 서비스 - 금융거래 등 온라인 거래 기능을 제공하는 서비스	4		
	- 일일 평균 접속건수가 2,000건 ~ 4,999건 이하인 서비스 - 각종 증명서의 열람 또는 발급 기능을 제공하는 서비스	3		
	- 일일 평균 접속건수가 1,000건 ~ 1,999건 이하인 서비스 - 온라인 거래, 각종 증명서 발급 기능은 없지만 타 시스템과 연동되는 서비스	2		
	- 일일 평균 접속건수가 1,000건 미만인 서비스 - 온라인 거래, 각종 증명서 발급 기능도 없으며, 단독 제공 형태의 단순 정보제공 서비스	1		

[그림 7] 기관 등급 분류 기준

바. 지표구성

통제분야	통제사항	필수	권고	선택
1. 관리적 보안	4	3	1	3
2. 제도적 보안	4	2	3	0
3. 인적 보안	4	2	1	2
4. 사용자PC 보안	2	5	2	1
5. 네트워크 보안	5	4	2	1
6. 서버 보안	2	2	2	0
7. DB 보안	1	1	1	0
8. 어플리케이션 보안	5	5	4	2
9. 가용성	1	2	2	0
10. 사후관리	2	1	2	1
11. 온라인거래서비스보안	6	8	2	0
12. 증명서서비스보안	6	8	2	0
소계	**42**	**43**	**24**	**10**

[그림 8] 전자정부서비스 보안수준 실태조사

5. 정보보호 안전진단

가. 의의

정보통신서비스 분야에 대한 정보보호조치를 강화할 필요성이 제기됨에 따라 인터넷을 기반으로 한 정보통신서비스의 정보보호 수준을 강화하여 안전한 이용 기반을 조성하고자 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'을 개정하고 정보통신망의 최소한의 안정 및 신뢰성을 보장하기 위하여 제시하는 보호기준을 의무적으로 준수하도록 도입하였다.

나. 목적

정보보호 안전진단 제도는 정보통신서비스제공자의 정보통신망에 대한 침해사고 예방과 정보보호조치에 대한 관리적/기술적/물리적 보호조치를 이행하고 수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정선 및 신뢰성을 확보하는데 목적이 있다.

다. 대상 및 범위

대상은 정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC) 및 쇼핑몰 등이 대상이며, 쇼핑몰 등의 다중서비스를 제공하는 안전진단대상사업자는 정보통신서비스 매출액이 100억원 이상이거나 전년도 말 기준 3개월간의 일일 평균이용자가 100만명 이상인 사업자를 대상으로 한다.

범위는 안전진단대상자가 조직내 소유/운영하고 있는 정보통신 및 시설 전체를 대상으로 '정보보호 안전진단 대상 정보통신설비 및 시설 선정 안내'을 참고하여 안전진단 이행 대상이 되는 정보통신설비와 시설을 선정하고 대상 목록으로 한다.

라. 심사과정

심사 절차는 안전진단대상자가 정보보호조치를 이행하고 안전진단 수검 후 안전진단결과 보고서 작성 및 확인증 교부까지의 절차를 의미한다.

[그림 9] 심사 절차

마. 특징

안전진단대상자는 의무적으로 준수해야 하며, 매년 이행여부를 안전진단수행기관으로부터 확인을 받아야 한다.

바. 지표구성

통제분야	통제내용	통제사항	세부 조치사항	주요 체크리스트
관리적 보호조치	1. 정보보호조직의 구성•운영	3	5	12
	2. 정보보호계획 등의 수립 및 관리	3	6	12
	3. 인적 보안	3	5	12
	4. 이용자 보호	1	1	4
	5. 침해사고 대응	1	1	4
	6. 정보보호 조치 점검	1	1	4
	7. 정보자산 관리	1	2	4
기술적 보호조치	8 네트워크 보안	3	3	10
	9. 정보통신설비 보안	12	21	43
물리적 보호조치	10. 출입 및 접근 보안	1	2	4
	11. 부대설비 및 시설 운영•관리	1	1	3
소계		**30**	**48**	**102**

[그림 10] 정보보호 안전진단 평가 지표

6. PIMS

가. 의의

PIMS는 방송통신위원회에서 민간 사업자를 대상으로 사업자가 개인정보를 안전하게 보호할 수 있는 환경조성하고 이를 검증받을 수 있는 인증 제도이다. 이 인증을 획득하는 기업은 개인정보 수집·이용·보유·제공·파기 등 전체 라이프사이클 전 과정에서 개인정보에 대한 안전성과 신뢰성 및 이용자 권리보호를 위한 전사적인 활동을 323개의 평가항목을 통해 공인 받게 된다.

나. 목적

개인정보 보호 활동을 체계적이고 지속적으로 수행하기 위한 개인정보보호 유관 법적 요구사항을 기반으로 전사적인 기술적·관리적 요구사항을 제시하고 한다.

다. 대상 및 범위

정보보호 관리체계 인증제도는 개인정보를 취급하고 있는 모든 민간기업을 대상으로 하고 있다.

인증범위는 조직에서 취급하는 개인정보 현황을 파악하여, 개인정보를 취급하는 모든 부서 및 시스템, 취급자를 포함한다. 전체 조직을 대상으로 하는 정보보호 관리체계 인증을 권고하지만, 조직의 상황에 따라 그 범위를 조직의 일부로 제한할 수 있다. 단, 한 조직이 조직의 일부를 추가로 인증 받는다고 해서 인증서의 개수가 증가되는 것은 아니며 기존 인증서의 인증 범위가 확대되게 된다.

라. 심사과정

본 인증을 유지하기 위한 심사과정은 4단계로 구분될 수 있다. 정보보호관리체계 인증 취득을 위한 최초심사, 정보보호관리체계 내의 심각한 변경이 발생한 경우 이루어지는 재심사, 정보보호관리체계를 지속적으로 유지하기 위해 주기적으로 이루어지는 사후관리심사 마지막으로 유효기간 만료 이후 정보보호관리체계의 인증을 유지하기 위한 갱신심사로 구분된다. 이 같은 심사과정은 ISO/IEC 27001을 모델로 정보보호관리체계에 동일하게 적용되는 부분이라고 할 수 있다.

마. 특징

PIMS는 생명주기 준거 요구사항 영역을 마련하여 개인정보의 수집부터 파기까지의 절차에 별도로 관리할 수 있도록 하고 있다. 이 영역은 ISO/IEC 27001과 K-ISMS에 존재하지 않는 영역이다. 방송통신위원회는 2010년 하반기부터 본 인증을 적용할 예정이다.

통제분야	통제내용	통제사항 수	점검항목 수
개인정보보호 대책요구사항	1. 개인정보수집에 따른 조치	7	17
	2. 개인정보 이용 및 제공에 따른 조치	16	49
	3. 개인정보 관리 및 파기에 따른 조치	5	12
	소계	**28**	**78**

[그림 11] 생명주기 준거 요구사항

바. 지표구성

통제분야	통제내용	통제사항 수	점검항목 수
개인정보보호 대책요구사항	1. 개인정보보호정책	6	11
	2. 개인정보보호조직	5	9
	3. 개인정보 분류	4	7
	4. 교육 및 훈련	4	7
	5. 인적보안	3	9
	6. 침해사고 처리 및 대응절차	7	20
	7. 기술적 보호조치	36	125
	8. 물리적 보호조치	5	12
	9. 내부검토 및 감사	9	24
	소계	**79**	**224**

[그림 12] PIMS 평가 지표

7. i-Safe, ePrivacy, eTRUST

가. 의의

한국정보통신산업협회에서는 e-BIZ 활성화를 막는 개인정보의 침해, 무단유출, 매매 등의 피해 사례가 증가함에 따라 민간차원의 자율규제(Self-Regulation) 활성화 및 개인정보 보호에 대한 마인드 확산, 그리고 개인(이용자) 및 사업자(공급자) 간의 신뢰기반을 조성을 위해 i-Safe 마크 제도와 ePrivacy 마크 제도를 운영하고 있다.

정보통신산업진흥원에서는 전자상거래에 대한 기업과 소비자의 신뢰를 향상시키고 건전한 시장 질서를 확립하기 위하여 전자거래기본법에 의하여 1999년부터 eTrust 인증 제도를 운영하고 있다.

나. 목적

i-Safe, ePrivacy, eTrust는 비슷하지만 각기 다른 목적을 가지고 있다.

(1) i-Safe : 안정된 네트워크 환경을 구축한 모범적인 인터넷 사이트 모델을 제시함으로써 국내 인터넷 사용 기반을 확대하고 관련산업 활성화로 국가 경쟁력 강화에 기틀을 마련

(2) ePrivacy : 인터넷 이용자의 개인정보를 효과적으로 보호하고, 안심하고 온라인 거래를 할 수 있는 신뢰기반 구축

(3) eTrust : 인터넷 거래에 대한 소비자의 신뢰성 확보 및 안전한 전자상거래 환경 구축

다. 대상 및 범위

i-Safe와 ePrivacy는 인터넷사이트를 통하여 개인정보를 수집, 취급, 관리하는 국내 사업자 및 일반인(단체)를 대상으로 하며, eTrust는 3개월 이상 영업한 우수 전자거래사업자

들을 대상으로 한다.

인증의 범위는 i-Safe와 ePrivacy는 운영 중인 사이트에 대하여 평가를 하고 있으며, eTrust는 전자상거래 관련된 구매 전 과정과 비즈니스 모델 적합성 등을 평가하고 있다.

라. 심사과정

i-Safe와 ePrivacy, eTrust의 심사 과정은 매우 유사하다. i-Safe와 ePrivacy는 먼저 신청업체, 기관의 현황을 필수 기준항목 준수 여부를 확인하여 적합, 부적합을 판정하고 적합은 계속 심사, 부적합은 재심 요구한다. 심사항목을 재그룹핑하여 적합 신청업체, 기관을 대상으로 적합도 평가하고, 적합, 부적합 판정을 내린다. 재심사는 신청업체, 기관이 부적합 부분을 개선한 후 신청할 수 있다. eTrust는 신규인증은 신청기관이 관련 자료를 제출하고 서류 및 사이트 심사 후 심사결과를 통보한다. 신청기관이 수정 및 보완을 하고 난 뒤에 재심사를 신청하면 Trust인증위원회 최종심의 및 의결 뒤 결정을 통보한다.

마. 특징

i-Safe는 금융, 의료 등 고도의 보안이 요구되는 인터넷사이트와 그 외 기타 인터넷사이트로 나누어 각기 다른 심사기준을 적용하고 있으며, ePrivacy는 2002년 2월에는 해외로의 인증 정책 활성화를 위하여 일본 경제산업성 산하 일본정보처리개발협회의 프라이버시마크와 국제 상호인정을 위한 MOU를 체결한바 있다. 또한 유일하게 민간에서 시행되고 있는 정보보호 평가 제도이다.

eTrust는 정부에서 주관하는 공신력이 있는 평가이며, 상품배달 및 교환·반품 등 웹 사이트 이용의 편리성 등을 평가하는 것이 특징적이다.

바. 지표구성

지표	심사 기준	관련 기준	지표 구성	
ePrivacy	개인정보보호	정보통신망법, 공공기관의 개인정보보호에 관한 법률, 개인정보보호 지침, i-Safe 심사기준	7개 분야 59개 항목 (필수 17개 항목)	
i-Safe	개인정보보호	정보통신망법, 개인정보보호지침, i-Safe 소비자 보호 부분	7개 분야 36개 항목 (필수 15개 항목)	
	시스템 보안	개인정보의 기술적•관리적 보호조치 기준, i-Safe 소비자 보호 부분	A그룹: 3개 분야 73개 항목 (필수 58개 항목)	
			B그룹: 3개 분야 66개 항목 (필수 39개 항목)	
	소비자보호	전자상거래 소비자보호 지침, i-Safe 소비자보호 부분	필수 6개 항목	A그룹: 115개 항목
				B그룹: 108개 항목

[그림 13] i-Safe, ePrivacy 평가 지표

심사영역	평가군	평가항목
공통 부문	5	19
쇼핑몰 부문	4	10
중개 부문	4	11
서비스 부문	3	8
금융 부문	4	9
무역 부문	5	13
B2B 부문	6	11
소계	**31**	**112**

[그림 14] eTrust 평가 지표

8. PIA(공공/기업)

가. 의의

개인정보영향평가(PIA:Privacy Impact Assessment)는 기존 사업 또는 신규 사업 추진 시 개인정보에 대한 침해 위험성을 사전에 평가하여 개인정보 침해 사고를 사전에 예방하기 위해 수립한 제도이다. 다량의 개인정보의 수집·활용하는 공공기관 및 기업은 신규 시스템 구축이나 기존 시스템에 중대한 변화가 조직이 소유한 개인정보에 미치는 영향을 사전에 조사·예측·평가함으로써 개인정보의 수집에서 파기까지의 전 과정에 발생할 수 있는 프라이버시 문제를 사전에 예방하기 위한 체계적인 절차를 말한다.

나. 목적

개인정보를 취급하는 사업자가 개인정보의 수집·저장·이용·제공·파기 등 개인정보 전반에 걸친 개인정보의 취급과 관련된 신규 사업 추진 및 기존사업 추진 시 스스로 고객의 개인정보의 유출 또는 오남용으로 인한 프라이버시 침해가 없는지를 조사·예측·검토하여 실제 정보시스템 구축 및 운영 시에 발생할 수 있는 개인정보 침해사고에 대한 침해요인을 사전에 제거·최소화하거나 효과적인 대응책을 수립하는 등 고객의 개인정보보호를 위한 개선절차를 마련하는데 그 목적이 있다.

공공기관 개인정보 영향평가는 공공기관의 개인정보보호에 관한 법률, 공공기관 개인정보보호 기본 지침, 공공기관 개인정보 관리 업무 매뉴얼, 공공기관 CCTV 관리 가이드라인, 공공기관 홈페이지 개인정보 노출방지 가이드라인, 공공기관 개인정보파일 관리 지침, 개인정보 처리단계별 기술적 보호조치가이드라인 등의 공공기관의 개인정보보호 관련 법규 준수 여부를 확인하는 과정을 거친다.

다. 필요성

조직의 개인정보의 범위가 확대되고 그 정보의 양이 증가함에 따라 개인정보유출 및 오남용으로 인한 프라이버시 침해사고가 점차 대형화되어 사회적 심각성이 증대되고 있다. 따라서 고객의 개인정보의 침해를 예방하고 개인정보의 개인정보가 침해되지 않도록 기업의 개인정보 상태를 수시로 점검할 수 있는 위험체계를 마련해야 한다.

라. 대상 및 범위

개인정보영향평가는 신규 및 기존 시스템을 변경하려는 조직의 주체적 결정에 따라 자율적으로 채택·시행된다. 또한 시행 주체는 기업 내의 개인정보보호 전담조직 또는 별도의 평가팀을 구성하여 수행한다. 단, 전담조직이 없는 경우 관련 사업관련 부서의 팀내 회의 및 외부 전문가로 구성될 수 있다. 수행 주체는 다음과 같은 지식의 보유해야 한다.(1) 개인정보보호 관련 법령 및 지침에 대한 기본적인 내용 이해 (2)시스템 개발 및 분석에 대한 전문지식 보유

마. 심사과정

개인정보영향평가는 아래와 같이 5단계로 이루어진다.

(1) 평가준비단계 : 조직에 위험관리가 필요한지 판단하고 위험관리가 필요한 경우 위험관리 수행을 위한 평가팀을 구성

(2) 평가계획 수립단계 : 평가 목적·사항·일정·활용방안을 구체화하여 평가계획을 수립 및 평가 계획서를 작성

(3) 평가시행단계 : 평가를 위한 평가관련 자료를 수집하고 평가사업의 주요 업무절차와 이에 따른 개인정보흐름을 분석하여 사업계획표 및 정보 흐름도 작성. (각 단계별 프라이버시 위험요소 및 개인정보 침해요인 분석 실시)

(4) 평가보고서 작성단계 : 개인정보 침해요인 분석을 통해 들어난 위험요소를 제거하거

이를 최소화할 수 있는 효과적인 대처 방안 마련

(5) 평가결과 활용 및 사후관리단계 : 위험요소에 대한 대처방안 수행을 위한 개선계획 수립

바. 기대효과

개인정보 침해사고 발생한 이후 침해사고 조치를 위해 외부조직의 개입이 일어나기 이전에 내부적으로 문제를 조사·처리하여 궁극적으로 사업자에 대한 고객의 신뢰를 향상시킬 수 있으며, 개인정보 침해사고 발생으로 일어날 수 있는 기업 이미지 손상 등 직·간접적인 경제적 손실을 방지할 수 있다.

사. 지표구성

평가영역	점검 항목 수	평가 항목 수
1. 사전 분석	3	15
2. 개인정보의 수집	1	10
3. 개인정보의 이용•제공•공유 등	1	9
4. 개인정보 처리의 위탁 등	1	12
5. 개인정보의 보유 및 파기	2	13
6. 정보주체의 권리보장을 위한 조치	1	7
7. 개인정보보호를 위한 인적•물리적 보안 조치	2	17
8. 개인정보 침해사고 발생 시 사후 구제체계	1	6
소계	**12**	**89**

[그림 15] 개인정보 영향평가 평가 지표 (기업)

평가영역	평가항목 수	주요 검토 내용 수
1. 개인정보보호 관리 체계	5	11
2. 개인정보 처리단계별 보호	6	33
3. 기술적 관리적 물리적 보호조치	4	73
4. 신규 IT 기술 활용 시 개인정보보호	4	82
소계	**19**	**199**

[그림 16] 개인정보 영향평가 평가 지표 (공공)

9. 공공기관 개인정보보호 수준진단 및 실태점검

가. 의의

각 기관의 개인정보 보호수준을 진단해, 각 기관의 개인정보관리 수준을 획기적으로 개선하여, 개인정보 관리 역량을 강화한다.

나. 목적

공공기관 개인정보보호 관리수준에 대한 객관적인 평가를 통해 위험을 미비점 보완 및 개언유도로 공공기관의 개인정보보호 수준을 향상시키는데 그 목적이 있다.

다. 대상 및 범위

2010년 기준으로 공공기관 개인정보보호수준 진단평가는 40개의 중앙부처, 246개의 지방자치단체, 417개의 공사 및 공단, 400개의 교육기관으로 총 1,103개의 기관을 대상으로 하며, 현장진단은 소관부처 및 기능을 고려하여 별도로 진행하게 된다.

개인정보보호수준 진단에서 언급하는 개인정보처리시스템은 업무단위의 개념으로 기관의 대표 홈페이지, 행정시스템, 전자민원 G4C등이 해당될 수 있다. 다시 말해, 서버단위나 내부 업무처리 시스템이 아닌 외부의 개인 및 조직의 개인정보를 수집·저장·이용·제공·파기하는 시스템을 의미한다.

라. 심사과정

공공기관 개인정보보호수준 진단은 온라인 시스템을 이용하는 자율진단과 현장 실사를 통해 증빙자료 확인 및 검증을 거치는 현장진단으로 나누어지며 총 5단계로 진행된다.

(1) 사전준비 : 행정안전부에서 실태점검 계획 수립

(2) 자율진단 : 각급기관에서 자율적으로 진단

(3) 취약점 분석·자체개선 : 각급기관에서 취약점을 분석하고 취약점을 자체적으로 개선

(4) 메타 진단 : 행정안전부가 별도로 구성한 진단전문위원회에서 각급기관의 진단결과를 검증

(5) 결과보고·발표 : 우수기관 및 미흡기관을 발표 및 문제점에 대한 제도·운영차원의 개선 과제를 발굴하여 다음해 개인정보보호대책 마련에 반영

마. 특징

자율진단의 경우 온라인 시스템을 활용하여 공공기관의 개인정보보호담당자가 직접 개인정보보호수준을 점검하도록 하고 있다. 현장진단은 전문가로 구성된 진단반이 직접 현장 실사를 통하여 제출한 증빙자료를 검토하여 추가 개선사항이 필요한 경우 컨설팅을 하는 것을 목적으로 수행된다.

공공기관 개인정보보호수준 진단은 질문에 대해 해당여부를 Yes/No로 표시하며 총 18개의 지표에 대한 결과와 진단 후 조치결과를 반영하여 계산된다. 18개의 지표 중 개인정보보호 예산은 배점 없이 현황지표로만 활용되며, 중앙부처의 경우 CCTV 항목은 배점이 없다. 즉, 해당 사항이 없는 항목은 기관의 평가에서 제외하고 (‘예’로 응답한 진단 항목별 비중의 합 * 항목별 배점)을 (해당되는 항목의 비중의 합)으로 나누게 된다.

바. 지표구성

구분	상위	진단지표 수	점검항목 수
개인정보보호기반	정책기반	4	13
	기술기반	3	14
처리단계별개인정보관리	수집 및 보유	4	16
	이용 및 제공	2	6
	파기	2	8
개인정보침해대응	개인정보침해 구제절차	1	6
	개인정보 유출 대응절차	1	4
	웹사이트 개인정보 노출대책	1	4
	소계	**18**	**75**

[그림 17] 공공기관 개인정보보호 수준진단 및 실태조사

10. 국가정보보호지수

가. 의의

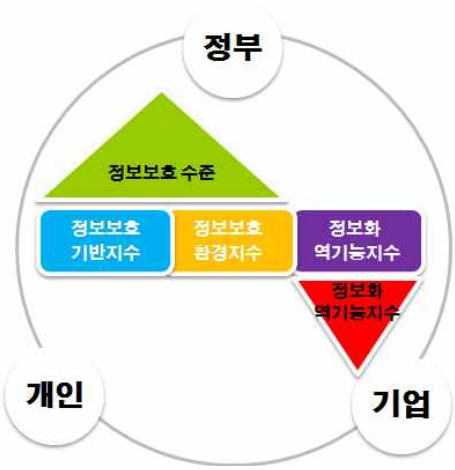
정보화는 20세기 후반의 사회·경제 활동 전반에 급속한 발전을 가져왔다. 또한 정보는 한 나라의 국익이나 경쟁력을 좌우하는 중요한 자산으로 인식되고 있다. 반면 정보화로 이난 정보의 유출·파괴·변조는 정보화 역기능으로 작용하여 국가적 현안이나 사회적 쟁점사항이 되고 있다. 그러므로 국가차원의 정보보호 정책을 효과적으로 수립할 수 있는 정보보호체계를 수립해야 한다. 국가정보보호지수는 한 나라의 정보보호 수준을 체계적· 객관적·정량적으로 분석함으로써 적절한 정보보호 정책의 수립과 효과적인 정책 추진 및 사후평가가 가능하다. 국가정보보호지수는 국제화지수를 목표로 개발되었다는 점에서 의의가 있다.

나. 목적

국가정보보호지수는 정보보호수준을 국가차원에서 객관적·효과적으로 분석하고, 그 나라의 다양한 정보보호 현상을 다양한 측면에서 체계적·객관적·정량·반복적으로 측정함으로써 국가 차원의 정보보호 정책에 효과적으로 반영할 수 있는 정보보호측정 기준을 수립하는 것이다. 또한 국가정보보호지수는 국가 간 정보보호수준도 비교할 수 있는 정보보호측정기준으로 개발되었다.

다. 대상 및 범위

국가정보보호지수의 프레임워크는 국가를 이루는 요소인 개인·정부·기업을 대상으로 정보보호 기반·환경지수 및 역기능지수를 평가한다. 국가정보보호지수는 개인 인터넷 이용자 정보보호 실태조사, 공인인증서 발급현황, 민간기업 정보보호 실태조사, WEF의 보안서버 수, 정보보호투자비율(재정경제부), 정보통신산업통계 및 정보보호산업통계를 바탕으로 세부평가지수를 산출하게 된다.



[그림 18] 국가정보보호지수 프레임워크

(1) 정보보호 기반지수 : 개인·민간의 정보보호에 대한 노력의 정도를 측정하는 지표로 백신 보급률, 패치 보급률, PKI 보급률을 이용해 평가한다. 기업의 경우 Firewall 보급률, IDS 보급률, 보안서버 보급률을 통해 평가

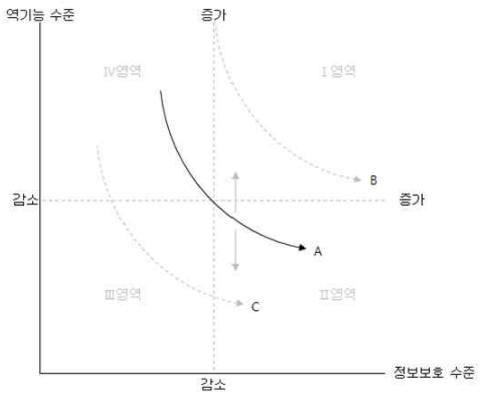
(2) 정보보호 환경지수 : 정보보호예산비율, 전문인력, 국민의 정보보호의식수준을 통해 평가

(3) 정보보호 역기능 수준 : 해킹·바이러스 신고비율, 개인정보 침해 신고비율, 스팸메일 수신비율 등을 바탕으로 평가

라. 특징

국가정보보호지수는 정보보호수준을 순기능과 역기능으로 나누어 측정하고, 두 지수의 움직임을 통해 정보보호 정책의 효율성을 효과적으로 분석한다. 매년 지수의 변화를 분석하여 정보보호 정책의 유효성을 판단할 수 있다. 그래프의 흐름이 Ⅳ영역에서 Ⅱ영역으로 이동해야 정책이 올바르게 적용되었다고 평가할 수 있다. 반면, Ⅰ영역으로 이동하는 경우는 역기능 수준이 증가하기 때문이고, Ⅲ영역으로 이동하는 경우는 정보보호 수준과 역기능 수준이 모두 감소한 것으로 평가할 수 있다. 또한 국가를 이루는 개인·정부·기업의 정보보호 수준을 평가함으로써 국가차원의 정보보호 정책 수립에 합리적인 의사결정 도구로 활용할 될

수 있다.



[그림 19] 국가정보보호지수 변화 그래프

국가정보보호지수는 단순합산방식에 의한 지수합산 방식을 이용한다. 이 방식은 WEF의 네트워크 준비지수 및 IMD(International Institute for Management Development)의 국가경쟁력지수의 지수화 방식과 동일한 방식이므로 다른 나라에서 국가정보보호지수를 보다 수월하게 도입할 수 있을 것이다.

마. 기대효과

국가정보보호수준 평가지수 개발을 통해 국가정보보호 정책 수립·추진에 있어 효과적인 성과분석이 가능하며, 우선순위에 따른 정책 추진이 가능하게 되어 효과적인 정보보호 예산 측정이 가능하다. 또한 사회전반의 정보보호 수준을 체계적으로 분석하여 개선이 필요한 영역을 찾아내고 이를 보완함으로써 국가차원의 정보보호수준을 향상시킬 것으로 기대된다. 향후 국가 간 정보보호 수준 비교를 위한 기준으로 활용될 수 있다. 실제로 방송통신위원회는 2009년 국가정보보호지수의 결과를 기반으로 국가 정보보호 관련 예산 확보와 정보보보 인식제고를 위한 교육 및 홍보 활동을 지속적으로 추진하는 한편, 인터넷 역기능을 예방하겠다는 계획을 발표했다.

바. 지표구성

구분	분류	지표
정보보호수준	정보보호기반	백신 보급률
		패치 보급률
		PKI 보급률
		Firewall 보급률
		IDS 보급률
		보안서버 보급률
	정보보호환경	정보보호 예산 비율
		정보보호 전문인력 비율
		국민 보안의식 수준 비율
정보화역기능수준	정보화 역기능	해킹 바이러스 신고 비율
		개인정보 침해 비율
		스팸 메일 수신 비율

[그림 20] 국가정보보호지수 평가 지표

[표 1] 국내 정보보호 관련 체계 및 평가 지표 현황

분류	기관	평가 지표 이름	지표 설명	
정부	국가정보원/방송통신위원회	국가정보보호지수	목적	정부와 기업, 개인 등 부문별 정보보호 수준을 종합적으로 측정하기 위하여 도입
			대상	정부, 기업, 개인
			법률	-
			지표	2개 부문, 3개 분야, 12개 지표
	국가정보원	정보보안 관리수준 평가	목적	주요 전산망에 대한 사이버안전 역량 제고 및 정보보안 관리수준 평가하기 위하여 도입
			대상	중앙행정부처, 광역자치단체, 주요 공공기관
			법률	국가사이버안전관리 규정
			지표	9개 분야, 246개 항목
	방송통신위원회	K-ISMS	목적	정보보호관리 절차와 과정을 체계적으로 수집하고 지속적으로 관리·운영하기 위하여 도입
			대상	기업

분류	기관	평가 지표 이름	지표 설명	
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 정보보호관리체계인증 등에 관한 고시
			지표	15개 분야, 120개 지표, 396개 항목
		정보보호 안전진단	목적	정보통신서비스제공자의 정보통신망의 안정성·신뢰성을 제고하기 위하여 도입
			대상	정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC) 및 쇼핑몰 등
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률
			지표	3개 분야, 11개 상위지표, 48개 지표, 102개 항목
		PIMS	목적	개인정보와 연관성 및 관리체계의 지속적 관리를 고려하여 도입
			대상	기업
			법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률
			지표	3개 분야, 119개 지표, 325개 항목
	행정안전부	전자정부서비스 보안수준 실태조사	목적	전자정부서비스를 제공하는 기관들의 보안수준 향상을 위하여 도입
			대상	중앙행정 및 지방해정 기관의 전자정부서비스 및 주요 행정정보 서비스

분류	기관	평가 지표 이름	지표 설명	
			법률	전자정부법
			지표	3개 분야, 12개 상위지표, 42개 지표, 77개 항목
		G-ISMS	목적 대상	행정기관의 정보보호 관리수준을 보다 객관적이고 체계적으로 점검·관리하기 위하여 도입
				전자정부서비스를 제공하는 행정기관
			법률	행정안전부 훈령 164호(전자정부법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법 시행령, 행정안전부와 그 소속기관 직제)
			지표	12개 분야, 44개 지표, 145개 항목
		공공기관 개인정보보호수준 진단	목적	공공기관의 개인정보관리 수준을 개선하기 위하여 도입
			대상	중앙행정기관, 지방자치단체
			법률	공공기관의 개인정보보호에 관한 법률, 시행령, 시행규칙
			지표	3개 분야, 8개 상위지표, 18개 지표, 75개 항목
		공공기관	목적	민감한 개인정보를 취급하는 공공기관의 개인정보 침해 위험성을 사전에 발견하여

분류	기관	평가 지표 이름	지표 설명	
		개인정보 영향평가		개인정보 침해발생을 사전에 예방
			대상	국가행정기관, 지방자치단체, 학교, 특수법인, 지방공사 등
			법률	-
			지표	4개 분야, 12개 상위지표, 32개 지표, 203개 항목
	정보통신산업진흥원	eTRUST	목적	인터넷 거래에 대한 소비자의 신뢰성 확보 및 안전한 전자상거래 환경 구축 도모
			대상	상업적 웹 사이트
			법률	전자거래기본법 제18조
			지표	7개 분야, 31개 지표, 112개 항목
민간	한국정보통신산업협회 (정보보호마크 위원회)	ePrivacy	목적	개인정보보호 정책 및 관리수준을 평가를 위하여 도입
			대상	인터넷사이트를 통하여 개인정보를 수집, 취급, 관리하는 국내 사업자 및 일반인(단체)
			법률	-
			지표	7개 분야, 59개 항목 (필수 17개 항목)

분류	기관	평가 지표 이름	지표 설명	
		i-Safe	목적	개인정보보호, 시스템 보안, 소비자 보호에 대한 평가를 위하여 도입
			대상	인터넷사이트를 통하여 개인정보를 수집, 취급, 관리하는 국내 사업자 및 일반인(단체)
			법률	-
			지표	3개 분야, 20개 지표, 224개 항목 (필수 79개 항목)

제 1 절 국외 정보보호 수준평가 체계 및 지표

1. ISO/IEC 27001

가. 의의

국제 표준화 기구 ISO/IEC JTC 1/SC27에서는 국제 사회에서 글로벌하게 사용될 수 있는 IT 보안 기술 분야의 다양한 표준을 제정하는 역할을 하고 있다. ISO/IEC 27001과 27001은 영국 BSI(British Standard Institute)에서 개발한 BS 7799의 Part 1과 Part 2를 표준화 한 것으로, 먼저 Part 2가 ISMS(Information Security Management Systems)의 요구사항에 대한 표준인 27001으로 표준이 되고, 이후에 Part 1이 실행 지침인 27002로 표준화되었다. 현재 정보보호분야의 공식적인 인증제도로 자리 잡은 ISO/IEC 27001은 ISMS에 대한 이해, 감시 및 검토, 유지, 개선 등에 대한 요구사항을 정의하며, 조직의 정보자산에 대한 보호 및 관리를 위해 ISMS를 수립·운영하기 위한 정형화된 프로세스인 PDCA, 절차, 정보보호 통제(27001) 등으로 구성된 정보보호 관리체계를 갖추었는지를 평가하고 인증하는 표준이다.

나. 목적

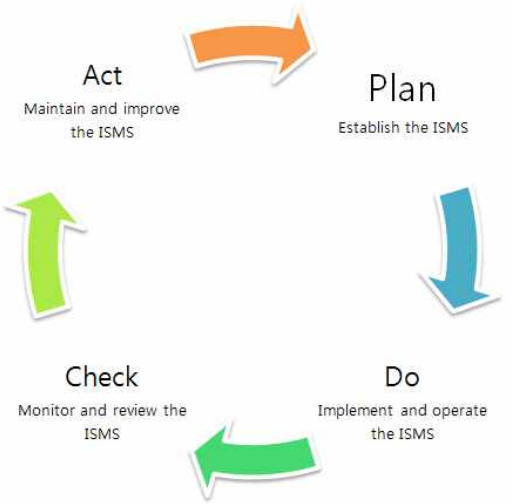
ISO/IEC 27001은 국제표준화기구(ISO)의 공동기술위원회 ISO/IEC JTC1와 정보기술 소위원회 SC27에서 공동으로 개발한 국제 정보보호관리체계의 표준규격으로 위험관리·보안정책·정보보호사고 대응 등 다양하고 엄격한 심사와 검증을 통해 조직의 위험관리 수준을 일정수준 이상으로 향상시킬 수 있다. 정보보호관리체계 인증을 통해 조직은 조직의 정보 자산을 균형 잡힌 보안통제를 통해 관리하고 있음을 공인받고 고객 신뢰도 향상 및 회사 안정성 제고를 달성할 수 있다.

조직의 서비스를 효과적으로 제공하기 위하여 조직 내의 다양한 활동을 파악하고 관리해야 한다. ISO/IEC 27001:2006 정보보호관리체계(ISMS:Information Security

Management System)은 정보보호관리의 전반적인 업무와 관련된 정보보호 요구사항 및 정책과 목표 수립의 필요성의 이해를 돕고, 조직의 전반적인 업무와 관련된 위험 관리를 위한 통제사항을 제시한다.

다. 대상, 범위 및 특징

정보보호 관리시스템은 모든 유형의 조직(예를 들면 상업적 기업, 정부, 비영리 조직 등)을 대상으로 조직의 전반적인 업무 활동 및 조직이 직면한 위험들과 관련하여 정보보호 관리시스템을 문서화하고, 정보보호 관리시스템의 수립·실행·운영·모니터링·검토·유지 및 개선하기 위해 프로세스 접근방식인 PDCA 모델을 기반으로 한다. PDCA 모델을 통해 조직은 정보보호와 관련된 전반적인 업무를 프로세스화하여 각 프로세스간의 상호작용을 통하여 조직의 정보보호관리체계에 대한 지속적인 위험관리 및 지속적 개선이 가능하도록 한다.



[그림 21] PDCA 모델

2005년 발표된 ISO/IEC 27000 시리즈는 27000:2009 ISMS에 대한 개요 및 용어 정리, 27001:2005 ISMS의 PDCA(Plan-Do-Check-Act) 프로세스에 기반한 정보보호 요구사항 정의, 27002:2005 ISMS의 정보보호 관리를 위한 실행지침서, 27003:2010 ISMS에 대한 구현 가이드라인, 27004:2009 정보보호관리에서의 정보보호 매트릭스와 측정에 관한 표준,

27005:2008 정보보호 위험관리에 대한 표준, 27006:2007 ISMS의 감사 및 증명 제공을 위한 인증기관에 대한 요구사항, 27011:2008 ISO/IEC 27001에 기반한 정보통신업체를 위한 정보보호관리 가이드라인 등이 국제 표준으로 제정된 상태이다.

라. 지표 구성

통제분야	통제항목	세부통제항목
1. 보안정책	1	2
2. 정보보안 조직	2	11
3. 자산 관리	2	5
4. 인원 보안	3	9
5. 물리적 환경적 보안	2	13
6. 통신 및 운영 관리	10	32
7. 접근 통제	7	25
8. 정보시스템 취득, 개발, 유지보수	6	16
9. 보안 사고 관리	2	5
10. 사업 연속성 관리	1	5
11. 준거성	3	10
소계	**39**	**133**

[그림 22] ISO 27001 평가 지표

2. PwC - ISBS

가. 의의

영국의 정보보안 시장의 가치는 865,000,000 파운드로 조사되었으며(DTI), 정보보안 시장의 가치는 지속적으로 증가하고 있다. 영국 산업은 매우 혁신적이라고 널리 알려져 있으며 BS 7799 등의 표준과 우수 관행의 개발 분야를 이끌어왔으며 2008년까지 BIS()와 BERR(Department for Business Enter)가 정보보호 위반조사를 수행해왔다. BERR은 그 조사 결과를 분석하여 중·소 기업측면에서 주의를 요하는 몇 가지 보안 이슈를 제시한다.

나. 목적

BERR(Department for Business Enterprise & Regulatory Reform)은 2007년 6월에 설립된 영국의 정부부처로 무역산업부(DTI)의 주요 업무를 수하던 기관이었다. 2010년 현재 BERR은 DIUS(Department for Innovation, Universities and Skills)와 합병되어 BIS(Deportment for Business, Innovation and Skills)로 새로이 출범하였다. 현재 BIS의 정보보호부서(Information Security)에서 기업조언(Business Advice)관련 업무를 수행 중에 있다. BIS는 영국 기업의 이 중 위험 관리(Risk Management) 업무에서 위험통계(Risk Statistics)를 위해 정보보호 위반조사(Information Security Breaches Survey)를 2년마다 실시하고 있으며, 조사 결과로 중·소 기업측면에서 주의를 요하는 몇 가지 보안 이슈를 제시하고 있다. 2010년부터는 PwC(PriceWaterhouseCoopers LLP)이 조사를 담당한다.

다. 대상 및 방법

설문조사는 산업 종사자를 대상으로 전화 설문조사와 정보보호 관련 포럼을 통한 설문조사 그리고 정보보호 담당자 인터뷰를 통하여 실시된다. 설문조사는 산업 종사자를 대상으로 전화 설문조사와 정보보호 관련 포럼을 통한 설문 조사 그리고 정보보호 담당자 인터뷰를 통하여 실시된다.

라. 특징

2008년 설문은 33개의 항목, 80개의 세부 항목으로 구성되었으며, 사용자 편의를 위해 15개의 공통 항목과 A그룹 9개, B 그룹 8개의 항목으로 나누어 설문을 실시하고 있다. 2010년 설문의 경우, 설문 항목 수를 줄이고 데이터 유출방지 및 소셜 네트워크, 가상화에 대한 설문을 추가하였다. 보안 위협, 주요 보안 위반, 보안정책, 소비자 정보보호 및 데이터 보호 법률 준수에 대한 기업의 인식도를 평가한다. 보고서의 구성은 전반적인 보안 트랜드를 제시하고, 각 설문 결과 도표를 설명과 함께 제시하고 있다. 설문 항목의 특성은 기술적 지표라기보다는 종사자들이 체감할 수 있는 후행적 지표의 특성을 지니고 있다.

2010년 ISBS는 539개의 기업을 대상으로 실시되었으며, 2008년의 질의항목에 데이터 손실 보호, 가상화, 소셜 네트워크 영역에 대한 설문이 추가되었다. 클라우드 컴퓨팅, 소셜 네트워크 및 가상화를 이용하는 기술이 지속적으로 개발되고 있다는 것을 보여주었다.

마. 지표 구성

분류	항목
1. 정보보호에 대한 태도	3
2. 변화하는 환경	3
3. 보안 문화	3
4. 보안에 대한 투자	3
5. 보증에 대한 수요	2
6. 데이터 유출 방지	2
7. 보안 위반의 발생률	3
8. 보안 사고의 유형	2
9. 바이러스와 악성 소프트웨어에 의한 감염	2
10. 시스템 오류 및 데이터 손상	1
11. 컴퓨터 절도 및 사기	2
12. 직원에 의한 다른 사고 야기	2
13. 외부인에 의한 비인가 접근	3
14. 위반의 영향	1
15. 사업 중단	2
16. 사고 대응 비용	1
17. 직접적인 재정 손실	1
18. 간접적인 재정 손실	1
19. 평판 피해	1
20. 사고의 총 비용	1
21. 긴급 사태 계획	1
소계	**40**

[그림 23] ISBS 평가 지표

3. NIST - SP 800 series(53A/55Rev1.)

가. 의의

NIST는 2008년 7월, 조직의 정보 시스템과 프로그램 수준의 보안수준 평가를 위한 지표 및 지표 방법론 제시를 위한 정보보호를 위한 성능 평가 가이드라인을 발표했다.

나. 목적

SP800-55 rev.1은 SP800-55(Security metrics Guide for Information Technology systems)와 SP800-80(Guide to Developing Performance Metrics for Information Security)을 통합하고 SP80-53(Recommended Security Controls for Federal Information Systems)에서 제시한 보안통제를 기초로 개정되었으며, 정보보호 프로그램 구현의 측정을 돕기 위해 기존의 SP800-55에서 소개했던 개념과 절차를 확장하였다.

기관은 SP-800 55 rev.1 가이드라인은 현재 기관이 수행하고 있는 보안제어, 정책, 절차의 수준 및 추가적인 보완이 필요한 정보보호분야를 판단하도록 도와준다. 또한 평가 개발 및 절차 구현 방법을 제공하고 지속적인 보안감사를 위한 보안통제 항목 선택과 우선순위 선정에 도움을 준다.

SP800-53A와의 차이점은 보안통제 구현 및 정보시스템 및 프로그램 수준의 효율성을 측정하고 분석할 수 있는 정량적인 접근 방법이라는 점이다. 또한 엔터프라이즈 수준에서의 정보보호 측정 및 분석하기 위한 다양한 정보 시스템으로부터의 정보를 통합하는 접근방식을 제공한다. SP800-53A는 평가를 위한 절차를 제공한다는 점에서 차이가 있다.

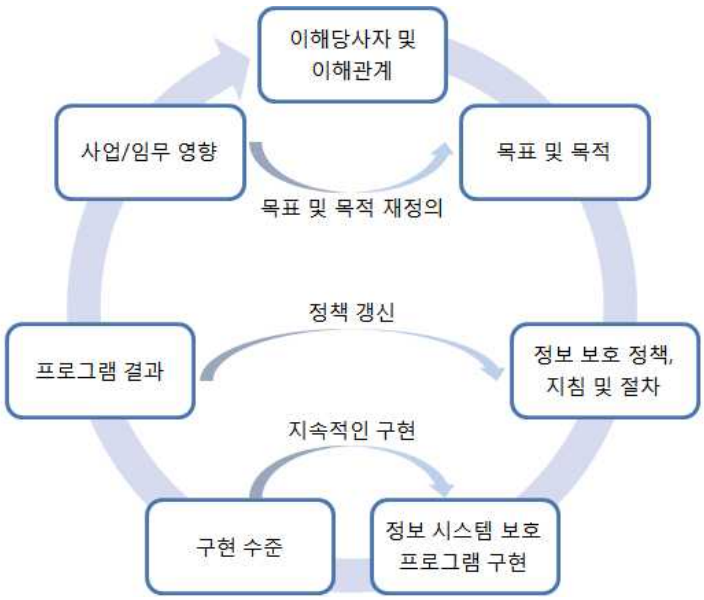
다. 대상 및 방법

SP800 시리즈는 기업·공공기관을 위해 체계적으로 구성된 정보보호 사이클을 구성한다.

[그림 24] FISMA 사이클

이와 같이 다양한 관련문서들 중에서 SP800-53A에서 보안통제를 위한 정보시스템 및 네트워크 부문의 유효성 평가를 위한 평가항목을 다루고 있으며, SP800-55 rev.1에서 정보보호 프로그램의 구현·측정을 위한 가이드를 제시하고 있다.

SP800-55 rev.1은 기업의 효율적 측정을 위해 7단계의 정보보호 성능측정 프로그램 개발 절차와 6단계의 정보보호 측정구현 절차를 제시하고 있으며 정보보호 측정 프로그램을 개발하는데 필요한 다양한 가이드를 제공한다.



[그림 25] 정보보호 성능측정 프로그램 개발 절차

(1) 주주들의 관심 식별: 주주들과 관련되고 주주들이 관심을 가지고 있는 정보보호 측정을 식별

(2) 목표와 목적 정의: 정보보호시스템 보호 성능 목표와 목적을 식별하고 문서화

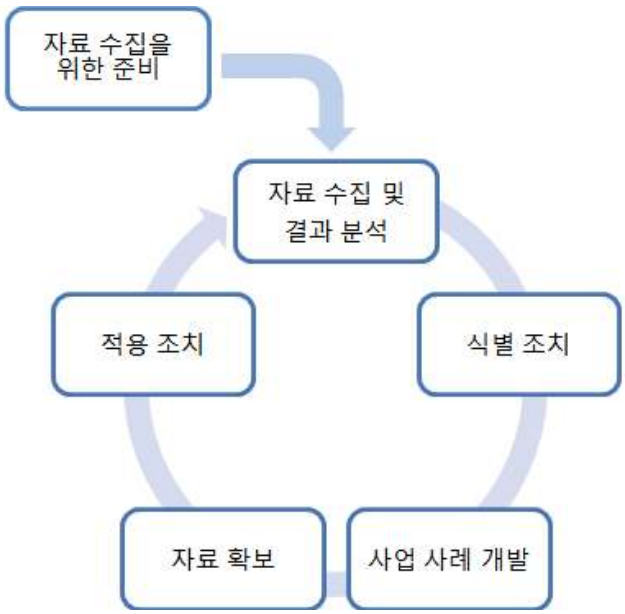
(3) 정보보호정책, 가이드라인 및 절차 검토: 조직의 특성에 맞는 정보보호 수행에 초점

(4) 정보보호프로그램 구현 검사: 점검되어야 할 측정 데이터를 도출하는데 사용될 수 있는 모든 측정데이터의 저장

(5) 측정 개발 및 분야: 추적 절차 구현, 효과/효율성, 업무영향 등을 포함

(6) 측정 개발 템플릿: 개발, 최적화, 수집, 보고 활동의 반복을 보장하기 위해 표준화된 형식으로 성능측정을 문서화

(7) 측정 개발 절차에서의 피드백: 지속적인 정책 구현, 정보보호정책 변경에 대한 노력, 목표 및 목적의 재정의, 지속적인 개발



[그림 26] 정보보호 측정 프로그램 개발

(1) 데이터의 수집 준비: 측정 프로그램 구현 계획에 대한 문서화

(2) 데이터 수집 및 결과 분석: 정보시스템보안을 이해하고 적절한 개선 절차를 식별

(3) 개선 조치 확인: 2단계에서 확인된 격차를 줄이는 로드맵으로 사용될 계획 개발

(4) 비즈니스 사례 개발 및 자원 획득: 3단계에서 식별된 완화 조치 구현에 필요한 자원을 위한 예산 사이클

(5) 개선 조치 적용: 보안프로그램에 대한 개선조치 사항의 구현 및 보안 통제

라. 지표 구성

통제항목	통제 수	항목 수	비고
1. 접근 통제	20	42	기술 통제
2. 인식 및 훈련	5	6	운영 통제
3. 감사 및 책임	11	25	기술 통제
4. 인증, 인가 및 보안 평가	7	11	관리 통제
5. 구성 관리	8	18	운영 통제
6. 비상 계획	10	39	운영 통제
7. 식별 및 인증	7	11	기술 통제
8. 사고 대응	7	15	운영 통제
9. 유지 보수	6	16	운영 통제
10. 미디어 보안	6	13	운영 통제
11. 물리적 환경적 보안	19	37	운영 통제
12. 계획	6	7	관리 통제
13. 인원 보안	8	9	운영 통제
14. 위험 평가	5	9	관리 통제
15. 시스템 및 서비스 인수	11	16	관리 통제
16. 시스템 및 통신 보안	23	42	기술 통제
17. 시스템 및 정보 무결성	12	30	운영 통제
소계	**171**	**346**	

[그림 27] NIST SP 800-53A 평가 지표

분류	지표	평가 타입	실행 증거
프로그램 수준	1. 보안 예산	영향성	2
	2. 취약성 관리	효율성	2
	3. 인식 및 훈련	이행	6
	4. 보증, 인가 및 보안 평가	유효성	5
	5. 구성 관리	이행	4
	6. 긴급 사태 계획	유효성	3
	7. 시스템 및 통신 보안	이행	3
시스템 수준	8. 접근 관리	유효성	6
	9. 감사 및 책임	효율성	3
	10. 식별 및 인증	유효성	2
	11. 유지 보수	효율성	3
	12. 위험 평가	효율성	5
프로그램/시스템 수준	13. 사고 대응	유효성	4
	14. 미디어 보안	유효성	4
	15. 물리적 환경	유효성	2
	16. 계획	이행	3
	17. 인적 보안	이행	2
	18. 시스템 및 서비스 인수	이행	2
	19. 시스템 및 정보 무결성	유효성	6

[그림 28] NIST 800-55 rev.1 평가 지표

4. III - Cyber Health Check

가. 의의

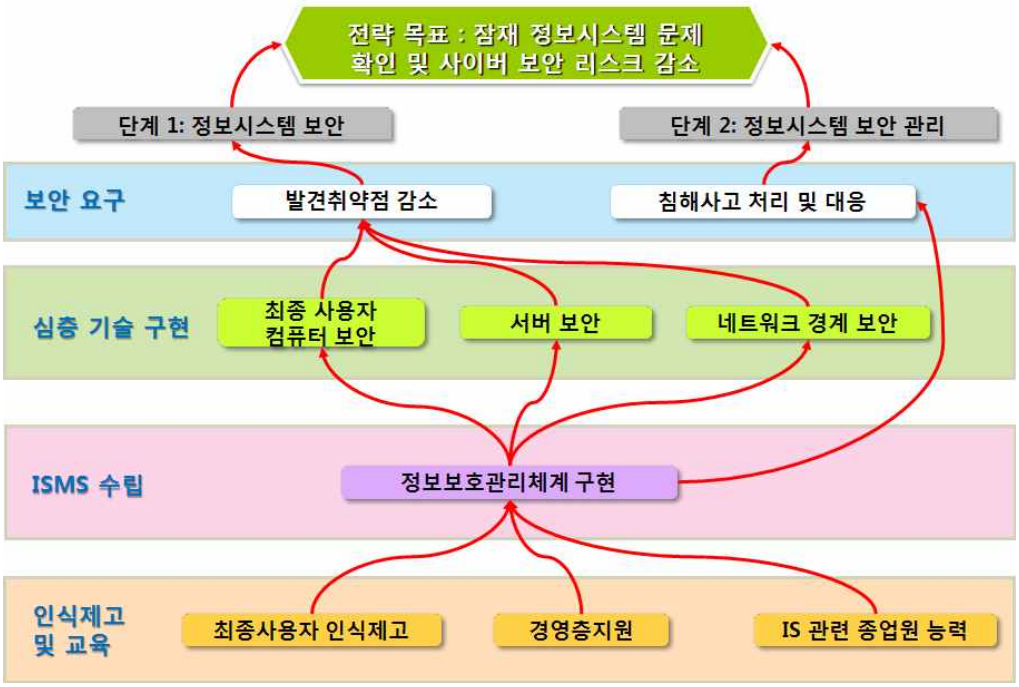
대만 정부기관인 정보산업연구소(III:Institute for Information Industry)에서 만든 Cyber Health Check는 국제 표준인 ISO/IEC 27001의 정보보호관리체계와 병행할 수 있는 상호보안적인 정보보호 평가체계를 마련하였다.

나. 목적

정보산업연구소는 기업의 정보보호 성능을 측정하기 위한 ISO/IEC 27001과 함께 병행할 수 있는 Cyber Health Check 시스템을 개발하였다. ISO/IEC 27001은 정성적 평가로 이루어지므로 정량적 평가를 통한 조직의 정보보호수준을 측정하는 것이 불가능하였다. 사이버 건강검진은 체계적인 정보보호수준 평가를 통해 정보보호 관리체계(ISMS)를 보완·개선하는데 활용할 수 있다.

다. 대상 및 방법

Cyber Health Check는 인식제고 및 교육, ISMS 수립, 심층 기술 구현, 보안 요구의 4단계를 거치는 정보시스템 보안과 정보시스템 보안 관리 전략 수립을 통해 잠재적인 정보시스템 문제 확인 및 사이버 보안 리스크를 감소시킨다.



[그림 29] Cyber Health Check 모델

(1) 인식제고 및 교육 평가는 최종 사용자의 인식제고, 경영층지원, 정보시스템 관련 직원의 능력 등을 측정한다.

(2) ISMS 수립은 정보보호 관리체계를 구현한다.

(3) 심층 기술 구현은 ISMS 수립 결과를 기반으로 최종 사용자의 컴퓨터 보안, 서버 보안, 네트워크 경계 보안 등을 구현한다.

(4) 보안 요구는 심층 방어 구현을 기반으로 노출된 취약점을 완화시키고, ISMS의 결과를 기반으로 침해사고를 처리하고 대응한다.

라. 특징

사이버 건강점검의 특징 중 하나는 실제 소셜 엔지니어링을 대상으로 실험 메일을 전송하고, 그 응답 비율을 측정한다는 것과 Likert scale을 이용하여 평가기준(metrics)와 지표의 순위를 매기고 10개의 등급으로 분류하여 각 Raw 데이터에 대한 등급을 정규화한 결과

를 다시 등급화하여 하는 리커트(Likert) 척도를 사용하여 등급을 매기고 있다.

지수화 방식은 (1) 관점별 핵심성과지표(KPI) 정의 (2) 후행지수(Lagging Indicator) 정의 (3) 선행지수(Leading Indicator)정의 (4) Raw 데이터 정의의 균형성과지표 설계 과정을 거쳐 총 46개의 후행지표로부터 25개의 핵심성과지표를 도출하고 이를 9개의 분야로 나누어 합산하여 각 관점별 지수를 구하게 된다.

마. 지표 구성

관점	주요 영역	핵심성과지표	후행지표
보호요구	노출 취약성 감소	3	4
	고급 침해사고 처리 대응	2	6
심층 기술 구현	최종 사용자 보안	5	6
	서버 보안	8	9
ISMS 수립	ISMS 구현	4	22
인식제고 및 교육	최종사용자 인식제고	1	1
	IS 관련 직원 능력	1	1
	경영층 지원	1	1
	소계	25	50

[그림 30] Cyber Health Check 평가 지표

[표 2] 국외 정보보호 관련 체계 및 평가 지표 현황

분류	기관	평가 지표 이름	지표 설명	
국제 표준	ISO/IEC	27001	목적	조직의 정보보호 관리체계에 대한 국제기준의 적합성 평가
			대상	기업
			법률	-
			지표	11개 분야, 39개 상위지표, 133개 지표, 330개 항목
	WEF	Network Readiness Index	목적	국가별 정보통신 인프라의 전반적인 보안 수준 평가
			대상	각 표준화 기구 회원국
	OECD	Communication outlook	법률	-
			지표	1개(인터넷 보안서버의 수)
미국	NIST	SP 800-53 A	목적	정보기술보안 기술 개선 및 연방 정보보안 관리법(FISMA)을 따르는 연방기관들을 돕기 위해 개발
			대상	연방기관 및 일반 조직
			법률	연방 정보보안 관리법(FISMA)
			지표	17개 분야, 163개 항목

분류	기관	평가 지표 이름	지표 설명	
		SP 800-55 rev.1	목적	조직의 정보 시스템과 프로그램 수준의 보안수준 평가를 위한 지표 방법론을 제시하고 정보보호의 평가를 위해 개발
			대상	일반 조직
			법률	-
			지표	3개 분야, 19개 항목
	DHS	CSSP(Primer Control Systems Cyber Security Framework and Technical Metrics)	목적	사이버 보안지수 프로그램 개발을 위한 가이드라인으로 측정 가능한 시스템 속성들을 제안
			대상	-
			법률	-
			지표	10개 항목
영국	PWC	ISBS	목적	영국 기업들이 직면하는 정보보호 위협에 대한 이해를 돕기 위해 실시
			대상	기업
			법률	-

분류	기관	평가 지표 이름	지표 설명	
			지표	33개 분야, 79개 항목
대만	III	Cyber Health Check	목적	정보보호 관리체계의 잠재적 문제 식별 및 사이버 보안 위험 감소
			대상	ISMS를 수립한 조직
			법률	-
			지표	5개 분야, 25개 지표, 51개 항목

제 2 절 국내 정보보호 수준평가 관련 연구

1. 기업의 정보보호수준 측정모델 개발에 관한 연구

이 연구는 이희명, 임종인(2008.10)이 정보보호활동 성과를 정량적으로 평가하여 각종 보안사고의 예방 및 대응방안 수립에 활용 가능하도록 BSC(Balanced Scorecard)를 적용하여 개발한 연구로 정보보호수준을 지속적으로 개선·평가·관리가 가능하도록 하는 새로운 모델 제시하고 있다.

이 연구에서는 ISO 27001 기반 정보보호 평가모델의 문제점을 지적하고 있다.

(1) 보안정책 및 제도 수립 여부 진단에 초점, 보안실천수준 진단기능이 약함
(2) 심사원 및 심사 환경에 따라 다른 결과가 나올 수 있음
(3) 서술적 심사 결과로 정보보호 전문지식이 없는 경영진에게 비효과적
(4) 단순한 평가결과(Yes, No, Partial, N/A)

구분	기존 모델(체크리스트)	신규 모델(PDCA)
평가기준	- 체크리스트 항목기준 - 예/아니오/부분적 기준 모호	- 현재 수행중인 정보보안 업무대상 - 실행형태에 따른 단계적 배점(5단계)
수준측정	- 현재 시점의 단순점수 파악 - 개선이 필요한 통제항목 도출	- PDCA 구현수준으로 현재수준 파악 - 개선이 필요한 실행업무 도출
평가근거	- 평가근거 기준이 모호하여, 평가자의 주관이 개입될 여지가 있음	- 각 단계별로 활동근거를 확인함(문서, 양식)

[그림 31] 모델 비교

개발 된 측정모델은 지표 Pool를 활용하여 다양한 정보보호 분야에 적용 확대 및 특정 영역에 집중된 지표 쏠림 현상 방지하고 있다. 또한 수준평가를 임의수행(10점)/계획(30점)/이행(50점)/평가(70점)/개선(90점) 5단계로 나누어 현재 기업의 정보보호 수준을 측정할 수 있다.

지표의 구성을 살펴보면 기반지표/이행지표/결과지표 3단계로 구성되어 있으며, 각 지표의 설명은 아래와 같다.

(1) 기반지표 : 기본적인 정보보호관리체계 측정을 위한 지표로 구성

(2) 이행지표 : 정보보호 수행 정도 측정을 위한 지표로 구성

(3) 결과지표 : 기반/이행지표 결과로 보안사고 예방을 진단하기 위한 지표로 구성

기반지표	이행지표	결과지표
- 보안조직구조 구성/절차 - 자산분류 절차 정의 - 보안교육 R&R - 정보백업 절차 정의 - 보안모니터링 성숙도 - 서버접근통제 성숙도 - 기술취약점관리 절차 - 보안사고관리 절차 - 시스템감사 절차 정의	- 보안정책 검토율 - 보안위원회 개최율 - 제3자 계약 보안성 검토율 - 외주파트너 PC 지급율 - 정보자산 갱신율 - 방화벽 로그 분석 실행율 - 시스템 위험 평가 실시율 - 로깅 설정 서버 비율 - 외부방문자 사무실출입율	- 악성코드 발생율 - 침해사고 발생 빈도 - 침해사고 조치 완료시간 - 모의해킹 취약점 발견율 - 출입증 분실 부서비율 - 보안징계발생 부서비율 - 보안교육 성취도 - 변경작업후 사고발생율 - 장애발생주기(MTBF)

[그림 32] 제안 모델 평가 지표

2. 전자정부 정보보호관리체계(G-ISMS) 적용 정책

이 연구는 한근희(2009.10)가 행정기관의 정보보호 현황 및 문제점 조사하고 개선안을 제시하고 있다.

이 연구에서 문제점을 기반 환경/정책 환경/서비스 환경에 따라 행정기관에 발생하고 있는 문제점을 지적하고 있다.

(1) 기반 환경 : 정보보호 전담조직 설치률, 전담 인력수, 정보보호 예산
(2) 정책 환경 : 순환근무 정책 및 전문인력 부족으로 인한 근무 기피 현상
(3) 서비스 환경 : 증가하는 웹 해킹 공격과 대응 가능한 전문 인력 부족

앞서 지적한 문제점을 개선하기 위하여 3가지의 개선안을 제시하고 있다.

(1) 행정기관의 정보보호 강화를 위한 인사제도 개선
(2) 전문인력 확충을 위한 교육 강화 및 가산점 부여
(3) ISO 27001을 개선한 표준화된 행정기관 정보보호관리체계 인증 제도 도입 제안

2009년 12월 11일에 제정된 G-ISMS로 시험인증을 한 결과 몇몇 문제점이 지적되었다. ISO 27001와 큰 차이가 없다는 것과 암호화/개인정보보호/포렌식/취약점 관리 분야의 점검 항목 개선 필요하다는 지적이었다. 개선된 지표는 이러한 지적을 수정하여 2010년 6월 7일 G-ISMS를 개정하여 배포하였으며, 지식정보보안컨설팅 전문업체를 대상으로 30개 공공기관의 정보보호관리체계 컨설팅 사업 착수 컨설팅 사업 착수(12억 규모)하였다.

5. 효율적인 개인정보관리체계(PIMS) 인증제도 도입방안 연구

이 연구는 심미나(2010.02)가 운영 보장하며, ISMS와의 중복성 해소하여 PIMS 도입을 위한 연구 수행하였다.

ISMS와 PIMS의 중복성 해소를 목적으로 수행되었다. PIMS는 기업이 수집, 저장, 보유, 이용, 제공, 및 파기하는 모든 개인정보보호에 대한 안전성과 신뢰성을 제공하고, 이용자 권리보호를 위한 전사적, 체계적, 지속적인 개인정보보호 시스템 의 운영을 보장하기 위해 개발된 인증제도이다.

ISMS와의 차이점 모색을 위하여 형식적 측면의 제도적 관점과 내용적 측면의 방법론적 관점으로 구분하여 중복요인을 밝히고, 중복요인을 기준으로 평가 항목을 분석하는 방법으로 연구를 실시하였다.

(1) 제도적 관점 : 근거 법령 및 목적, 행위주체간 효용성
(2) 방법론적 관점 : 심사절차, 심사 방법, 심사기준
(3) 평가항목 관점 : 통제분야, 목적

구분	완전중복	부분중복	비중복
관리통제	47개(54.7%)	30개(34.9%)	9개(10.4%)
생명주기준거	0개	8개(26.7%)	22개(73.3%)
전체	**47개(40.5%)**	**38개(32.8%)**	**31개(26.7%)**

[그림 33] ISMS와 PIMS의 중복 비교

제 3 절 국내외 정보보호 수준평가 지수화 방법론

1. 지수화 방법론 연구

지수란, 다양한 평가 지표를 종합하여 단일 값으로 나타낸 수치를 말한다. 지수는 종합적, 각 분야별, 시대별 정보보호 수준을 비교하여 장·단점을 파악할 수 있으므로 현실적 목표와 정책방향 결정에 기초자료로 활용될 수 있다. 반면, 지수는 지표에 해당하는 모든 정보를 수렴하여 하나의 값으로 표현하기 때문에 부정확한 데이터나 데이터 누락에 의하여 전체 지표를 왜곡시킬 가능성이 있다.

국가정보보호지수와 ITU의 IDI에서는 지수화를 위하여 산술평균의 개념에 의한 대표값 산출방식을 이용하고 있다. 이러한 방식은 평가영역별 지표에 동일한 가중치를 할당함으로서 세부 지표의 수가 많은 항목에 상대적으로 적은 가중치가 할당되게 되므로 각 영역별 지표수가 고르게 개발되어야 한다.

다른 방식으로 다수의 후보지표를 개발한 이후에 델파이 방법을 이용하여 전문가집단의 설문조사를 실시하고 주요 지표를 결정하는 방법을 이용할 수 있다.

또 다른 방법론으로 Cyber Health Check에서 이용하는 표준편차를 이용한 방법이 있다. 국가별로 수집된 평가지표별 Raw 데이터를 수집하여, 데이터 분포의 분산을 구하고, 표준편차를 기준으로 +/- 5개의 점수 대역을 구분한 후 이를 등급화 한다. 즉, 각 국에서 수집도니 데이터의 상대적 위치에 따라 점수가 결정되게 된다.

X.csi의 표준화를 담당하는 ITU-T SG17의 경우, 표준화 회의가 주기적으로 개최되고 각국의 정보보호 전문가들이 참석한다는 점에서 각국의 지역적, 경제적 특성을 고려할 수 있으며, 각국에서 제안하는 평가 지표들을 대상으로 지표 풀(Pool)을 구성하여 지수화를 위한 지표를 선정하는 방법이 적합할 것으로 판단된다.

2. ICT 개발지수(ITU)

ICT 개발지수는 ITU가 기존에 발표하던 디지털기회지수(DOI)와 ICT기회지수(ICT-OI)를 통합하여 2009년 3월 처음 발표한 지수로서 국가별 정보통신 발전수준과 정보격차를 측정하기 위해 개발되었다. 지표 구성은 ICT 접근 정도, ICT의 이용 정도, ICT 활용능력의 2개 부문에 총 11개 세부지표로 구성되어 있다.

ICT 활용능력을 대변할 수 있는 지표가 대부분의 개발도상국에서 수집되지 않아 문해율과 교육수준을 대체지표로 사용하고 있으며, 부문간 가중치를 접근성과 이용 부문에 각각 30%, 활용능력 부문은 대체지표를 감안하여 상대적으로 낮은 20% 가중치를 부여하고 있다.

ICT access	Ref. Value	(%)	
a 1. Fixed telephone lines per 100 inhabitants	60	20	40
b 2. Mobile cellular telephone subscriptions per 100 inhabitants	150	20	
c 3. International Internet bandwidth (bit/s) per Internet user	100,000	20	
d 4. Proportion of households with a computer	100	20	
e 5. Proportion of households with Internet access at home	100	20	
ICT use	**Ref. Value**	**(%)**	
f 6. Internet users per 100 inhabitants	100	33	40
g 7. Fixed broadband Internet subscribers per 100 inhabitants	60	33	
h 8. Mobile broadband subscribers per 100 inhabitants	100	33	
ICT skills	**Ref. Value**	**(%)**	
i 9. Adult literacy rate	100	33	20
j 10. Secondary gross enrolment ratio	100	33	
k 11. Tertiary gross enrolment ratio		33	

[그림 34] ICT 개발 지수 방법론

ICT 개발지수는 지수 산출방법은 각 하위범주 유형 중 최종 11개의 지표를 선택하고 주성분분석(PCA)으로 데이터의 근본적인 성격을 분석하고 지표들 간 연관관계를 설명하였다. 또한 각 세부지표를 표준화하여 범위를 1에서 10까지로 재조정하고, 개별 지표에 동일한 가중치를 적용하여 각 하위지수의 값을 계산하였다. 자세한 계산 방법은 다음과 같다.

$$\text{ICT access} = \frac{a}{60} \times 0.2 + \frac{b}{150} \times 0.2 + \frac{\log(c)}{5} \times 0.2 + \frac{d}{100} \times 0.2 + \frac{e}{100} \times 0.2$$

$$\text{ICT use} = \frac{f}{100} \times 0.33 + \frac{g}{60} \times 0.33 + \frac{h}{100} \times 0.33$$

$$\text{ICT skills} = \frac{i}{100} \times 0.33 + \frac{j}{100} \times 0.33 + \frac{k}{100} \times 0.33$$

$$\text{IDI} = (ICT\ access \times 0.4) + (ICT\ use \times 0.4) + (ICT\ skills \times 0.2)$$

[그림 35] ICT 개발 지수 계산 방법

(1) 개별 지표별 지수값 : {수집된 데이터 값/기준값} * 개별지수별 가중치

(2) 분야별 지수값 : {개별지수 값의 합산} * 분야별 가중치

(3) 종합 지수값 산출 : 분야별 지수값의 합산

3. 국가정보보호지수(KISA)

국가의 구성요소인 개인, 정보, 기업을 대상으로 정보보호 수준을 결정하며, 정보보호지수는 정보보호수준지수와 정보화역기능수준지수로 나누어 측정한다. 정보보호수준은 정보보호에 관한 순기능으로서 정보보호활동을 중심으로 구성하고, 정보화역기능수준은 정보보호의 수기능이 작동하지 않아 발생하는 부분과 순기능과 무관하게 정보화 과정에서 발생하는 정보화 피해 등을 포함하고 있다. 이 두 지수의 움직임을 통해 정보보호 정책 효과의 유효성을 평가하는 방식을 채택하고 있다.

종합지표	가중치	항목	가중치	조정 계수	항목
정보보호 수준 (H)	ω_{t1}	정보보호 기반지수 (T)	ω_{t11}	α_{11}	백신 보급률 t11
			ω_{t12}	α_{12}	패치 보급률 t12
			ω_{t13}	α_{13}	PKI 보급률 t13
			ω_{t14}	α_{14}	Firewall 보급률 t14
			ω_{t15}	α_{15}	IDS 보급률 t15
			ω_{t16}	α_{16}	보안서버 보급률 t16
	ω_{e1}	정보보호 환경지수 (E)	ω_{e11}	β_{11}	정보보호 관련 예산 비율 e11
			ω_{e12}	β_{12}	정보보호 전문인력 비율 e12
			ω_{e13}	β_{13}	국민의 보안의식 수준 비율 e13
정보화 역기능수준 (N)	ω_{n1}	정보화 역기능지수 (N)	ω_{n11}	δ_{11}	해킹·바이러스 신고비율 n11
			ω_{n12}	δ_{12}	개인정보 침해 신고비율 n12
			ω_{n13}	δ_{13}	스팸메일 수신비율 n13

[그림 36] 국가정보보호지수 지수화 모델

국가정보보호지수의 자세한 계산 방법은 다음과 같다.

$$\mathrm{H} = \omega_{t1}\mathrm{T} + \omega_{e1}\mathrm{E}$$
$$\textbf{s.t}\ \omega_{t1} + \omega_{e1} = 1$$

$$\mathrm{T} = \omega_{t11}\alpha_{11}t_{11} + \omega_{t12}\alpha_{12}t_{12} + \omega_{t13}\alpha_{13}t_{13} + \omega_{t14}\alpha_{14}t_{14} + \omega_{t15}\alpha_{15}t_{15} + \omega_{t16}\alpha_{16}t_{16}$$
$$\textbf{s.t}\ \omega_{t1} + \omega_{t12} + \omega_{t13} + \omega_{t14} + \omega_{t15} + \omega_{t16} = 1$$

$$\mathrm{E} = \omega_{e11}\beta_{11}e_{11} + \omega_{e12}\beta_{12}e_{12} + \omega_{e13}\beta_{13}e_{13}$$
$$\textbf{s.t}\ \omega_{e11} + \omega_{e12} + \omega_{e13} = 1$$

$$\mathrm{N} = \omega_{n11}\delta_{11}n_{11} + \omega_{n12}\delta_{12}n_{12} + \omega_{n13}\delta_{13}n_{13}$$
$$\textbf{s.t}\ \omega_{n11} + \omega_{n12} + \omega_{n13} = 1$$

[그림 37] 국가정보보호지수 계산 방법

(1) 지표별 지수값 산출 : { 지수별 가중치*조정계수*개별지수값 }

(2) 조정계수 : 금액/지수/대수의 기준을 조정하기 위한 값

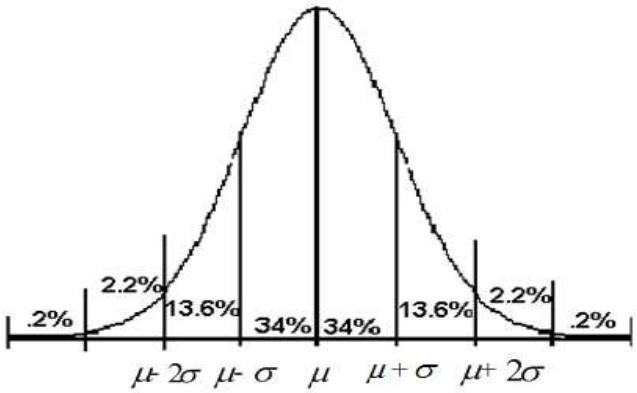
(3) 분야별 지수값 산출(T/E/N) : { 분야별 가중치*분야별 지수의 합 }

(4) 종합 지수값 산출(H/N) : { 분야별 지수값의 합산 }

4. Cyber Health Check(III)

Cyber Health Check는 다른 지표와는 다르게 어떠한 행위에 대한 결과를 측정하는 방식을 취하고 있다. 그리고 수집된 자료를 리커트(Likert) 척도를 사용하여 등급을 매기고 있다.

이메일 지표와 같은 경우는 오픈 비율과 클릭 비율의 두 개가 하나의 지표로 사용된다. 두 개의 비율을 정규분포를 사용하여 등급을 매기고 등급에 따라 랭크를 곱하여 하나의 랭크를 만들어내는 방식을 사용하고 있다.



[그림 38] 정규 분포 모델

Rank	Calculation
10	less than $\mu_{indicator} - 3\sigma_{indicator}$
9	$\mu_{indicator} - 3\sigma_{indicator} \sim \mu_{indicator} - 2\sigma_{indicator}$
8	$\mu_{indicator} - 2\sigma_{indicator} \sim \mu_{indicator} - 1.5\sigma_{indicator}$
7	$\mu_{indicator} - 1.5\sigma_{indicator} \sim \mu_{indicator} - \sigma_{indicator}$
6	$\mu_{indicator} - \sigma_{indicator} \sim \mu_{indicator}$
5	$\mu_{indicator} \sim \mu_{indicator} + \sigma_{indicator}$
4	$\mu_{indicator} + \sigma_{indicator} \sim \mu_{indicator} + 1.5\sigma_{indicator}$
3	$\mu_{indicator} + 1.5\sigma_{indicator} \sim \mu_{indicator} + 2\sigma_{indicator}$
2	$\mu_{indicator} + 2\sigma_{indicator} \sim \mu_{indicator} + 3\sigma_{indicator}$
1	more than $\mu_{indicator} + 3\sigma_{indicator}$

[그림 39] 계산된 점수에 따른 랭크

Rank	Range
10	82~100
9	65~81
8	50~64
7	37~49
6	26~36
5	17~25
4	10~16
3	5~9
2	2~4
1	1

[그림 40] 두 랭크의 곱에 따른 랭크

제 3 장 국내외 정보보호 수준평가 체계 및 지표 비교 분석

본 연구는 국제적으로 합의된 정보보호지수를 개발하는데 있어, 국내 정보보호평가 지표를 최대한 반영할 수 있도록 지표를 개발하는 것을 목적으로 하고 있다. 이는 추후 X.csi가 국제 표준으로 승인될 경우 국내에서 기존에 이용하고 있는 데이터를 기반으로 손쉽게 데이터를 확보할 수 있기 때문이다. 그러므로 본 연구에서는 1장에서 소개된 지표들을 대상으로 평가항목의 분석을 통해 공통된 평가 영역 및 지표를 산출하는 과정을 수행하였다. 먼저 모든 평가체계 및 평가지표의 항목을 전수적으로 비교하기에는 무리가 있다고 판단하여 다음과 같이 분야를 나누어 비교하였다.

(1) 체계부문 : ISO/IEC 27001, K-ISMS, G-ISMS(2009.10)

(2) 국내지표부문 : 정보보안관리수준평가, 전자정부서비스 보안수준 실태조사, 정보보호 안전진단

(3) 개인정보보호부문 : PIMS, i-Safe, ePRIVACY, PIA(공공/기업), 공공기관 개인정보보호 수준진단, G-ISMS(2009.10)[1)]

앞서 언급한 정보보호 체계 및 지표 중 일부를 선택하여 다음과 같이 공통지표를 파악하였다. 그 이유는 본 연구의 최종 목표가 국제적인 정보보호평가지수 표준화가 가능한 지표개발이기 때문에 국내에서 공통적으로 사용되는 평가지표가 일반화된 평가기준이 될 것이라는 판단에서 공통지표 분석을 실시하게 되었다.

---

1) 위 분류에서 G-ISMS가 체계부문과 개인정보보호부문에 모두 들어간 것은 2009년 10월 당시에는 개인정보보호항목이 별도로 존재하지 않았기 때문이다. 2010년에는 발표된 항목에는 개인정보보호부문이 따로 분리되어 있지만 본 연구를 진행하면서 최근에 공개된 지표의 세부항목 리스트를 구하지 못하여 2009년의 지표에서 개인정보보호 관련 지문을 별도로 분류하여 개인정보보호문의 다른 지표와 비교하였다. 좀 더 자세히 살펴보면, K-ISMS는 국내 상황에 맞게 침해사고 예방, 암호화, 전자거래 항목 등을 추가하였고, G-ISMS는 암호화와 개인정보보호 항목을 추가하여 기존의 통제사항과 세부통제 항목보다 그 수가 증가하게 되었다.

체계 부분과 국내지표부문, 개인정보보호의 지표 분류를 통하여 각각의 지표가 공통적인 분류에 포함되는 지표의 개수를 확인하였다. 이 분류 작업을 통하여 대략적으로 공통 지표의 개수를 파악할 수 있었으며, 공통 지표의 확인 작업을 간편하게 해주었다.

우선 지표별 설명에서 언급한 지표수와 아래 [표 3]에서의 지표수가 다른 것은 자세한 분석을 위해 세부점검항목을 고려하였기 때문이다. 비교 결과를 살펴보면 체계부문의 경우 중복항목이 많고 국내지표 및 개인정보보호 부문에서는 중복항목 수가 적게 나온 것을 볼 수 있는데, 이는 세부점검항목이 공개되지 않은 경우 평가지표만을 비교하였기 때문이다. 즉, 다른 지표에서 중복된 세부점검항목들이 세부점검항목이 공개되지 않은 평가지표로 흡수되었기 때문에 다수의 세부점검항목들이 있더라도 1개로 표시되게 되었다. 또한, 체계 부분의 지표는 ISO 27001을 기준으로 하여 개발하여 공통 분류나 지표나 많이 나온 반면에 국내 지표 부분이나 개인정보보호 지표를 특정 체계나 지표를 기준으로 하여 개발을 하지 않았기 때문에 공통 분류나 지표가 체계 부분에 비하여 많이 산출되지 않았다. 이와 같은 비교 분석 결과 150여개 공통 지표를 산출할 수 있었다.

[표 3] 분야별 평가지표 비교 분석

<table>
<tr><td></td><td colspan="3">지표수 비교</td><td colspan="6">공통지표</td></tr>
<tr><td rowspan="2">체계부문</td><td>ISO 27001</td><td>K-ISMS</td><td>G-ISMS</td><td>7개중복</td><td>6개중복</td><td>5개중복</td><td>4개중복</td><td>3개중복</td><td>2개중복</td></tr>
<tr><td>330</td><td>396</td><td>221</td><td>-</td><td>-</td><td>-</td><td>-</td><td>103</td><td>93</td></tr>
<tr><td rowspan="2">국내지표부문</td><td>정보보호관리
수준평가</td><td>전자정부서비스
보안수준실태조사</td><td>정보보호
안전진단</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">-</td><td rowspan="2">10</td><td rowspan="2">10</td></tr>
<tr><td>252</td><td>77</td><td>181</td></tr>
<tr><td rowspan="7">개인정보보호
부문</td><td>PIMS</td><td>i-Safe</td><td>ePRIVACY</td><td rowspan="7">1</td><td rowspan="7">1</td><td rowspan="7">4</td><td rowspan="7">7</td><td rowspan="7">4</td><td rowspan="7">3</td></tr>
<tr><td>323</td><td>224</td><td>112</td></tr>
<tr><td>PIA(공공)</td><td>PIA(기업)</td><td>공공기관개인정보보호
수준진단</td></tr>
<tr><td>203</td><td>85</td><td>76</td></tr>
<tr><td>G-ISMS
(개인정보보호)</td><td></td><td></td></tr>
<tr><td>91</td><td></td><td></td></tr>
</table>

[표 4] 체계 부분 비교

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
정보보호정책	정보보호 정책 승인 및 공표	2	5	10
	기타	3	5	3
정보보호조직	정보호호 조직의 구성	3	5	10
	정보보호 공조 활동	3	3	4
	정보호호 역할 및 책임	1	3	12
	정보시스템 도입	2		1
	비밀유지 서약	2	3	2
	정보보호에 대한 독립적 검토	4		4
	제3자 및 고객과 계약시 보안 요구사항	6	5	
자산분류 및 통제	자산 목록	2	2	3
	자산별 책임할당	2	2	4
	정보자산의 분류	1	1	3
	보안등급 라벨링	2	2	1
	기타	1		

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
인적보호	직무 역할 및 책임	3	2	3
	고용전(적격심사)	3	2	2
	인사규정(고용계약서)	2	8	1
	징계규정	2	1	1
	고용후(퇴직/자산반납/권한제거)	4	1	4
	정보보호 교육 및 훈련	3	14	8
	외부자와 관련되 위험파악			10
	기타		2	2
	관리자책임			
물리적/환경적보호	물리적 보호구역	3	4	4
	물리적 접근 통제	5	2	3
	사무실 및 설비 공간보호	1		3
	출입통제구역	1	6	1
	외부 및 환경 위협에 대한 보호	2	6	1
	운송 및 하역구역	2		1

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	기기의 위치 및 보호	2	3	1
	케이블 보호	2	1	1
	장비의 반입 및 반출	1		4
	시설 유지 및 장비 유지보수	3	2	2
	장비의 안전한 폐기 및 사용	1	6	1
	기타	7	6	
통신 및 운영관리	운영절차의 문서화	2	3	1
	변경관리	2	4	1
	직부분리	3	2	1
	개발과 운영 환경의 분리	2	3	1
	위탁 서비스 관리	4	1	5
	시스템도입	2	2	1
	시스템 인수		2	2
	성능관리		4	
	용량관리	3	4	

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	백업 및 복구 관리	2	8	3
	보안시스템운영		4	
	악성소프트웨어 통제	3	10	4
	이동코드 통제	1		1
	네트워크 통제	3	19	5
	정보 교환의 통제	2	1	3
	정보 교환 계약	2		2
	운송중인 매체의 보호	1		2
	전자적 교환 보안	2	3	1
	시스템 접속 통제	2		1
	전자상거래	2	8	10
	공개서버의 보안 관리	4	7	
	휴대용 저장매체의 관리	2	11	6
	매체 폐기	2	5	3
	정보 취급 절차	2		6

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	시스템 문서의 보안	2	2	1
	원격지 접속	4	6	2
	이용자 공지 사항		2	
접근통제	접근통제 정책	2	10	2
	사용자 등록	3	4	1
	특수권한 관리	2	3	2
	사용자 패스워드 관리	1	3	1
	사용자의 접근권한 검토	2	5	2
	패스워드 사용	2	2	1
	이석시의 장비 보안	1		5
	책상 정리 및 화면보호	3		1
	네트워크 서비스의 사용에 대한 정책	4	3	3
	네트워크 상에서의 장비 식별	1		2
	원격진단포트 및 시스템 설정 포트의 보호	2		3
	네트워크 분리	2	1	1

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	네트워크 연결 통제	2		3
	네트워크 경로제어	3		2
	안전한 로그온 절차	5	2	1
	패스워드 관리 시스템	4		2
	시스템 유틸리티의 사용	2		1
	세션 시간 종료	2	1	1
	연결시간의 제한	2		1
	정보에 대한 접근제한	3	2	5
	민감한 시스템 분리	3	2	
	데이터베이스 접근		2	
	사용자 식별 및 인증			2
	이동 컴퓨팅 및 통신			2
시스템 도입/개발 및 유지보수	보안 요구사항 분석과 설계	3	3	1
	입력 데이터의 검증	6	4	2
	프로세스의 통제			1

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	내부 처리 통제	4	5	
	출력 데이터의 검증	2	2	1
	메시지 무결성	2	1	1
	암호화 통제	9	10	9
	운영소프트웨어 통제	4	3	1
	시스템 테스트 테이터의 보호	3	4	1
	프로그램 소스코드에 대한 접근통제	4	5	1
	변경 통제 절차	5	8	4
	운영체제 변경시의 검토	4	4	
	소프트웨어 패키지 변경	3	4	
	외주 소프트웨어 개발	3		2
	응용소프트웨어 구현 및 시험		3	
보안사고 관리	보안사고 보고	4	6	2
	보안 취약점의 보고	3	1	1
	대응 및 복구	2	3	5
	보안사고 사후관리	3	10	5

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	증거수집	4		
업무연속성 관리	사업 연속성 관리 프로세스	9	7	1
	업무연속성 및 위험평가	4	2	3
	업무 연속성 계획의 작성 및 실행	6	4	
	업무연속성 계획의 시험, 유지 및 재평가	4	5	2
부합성	관련법규 규명	3	2	2
	지적재산권	5	2	1
	기관의 기록 보호	5	2	1
	정보보호 및 개인정보보호 대책	5	2	24
	정책의 준수	6	5	2
	정보처리시설의 오남용 방지	3		1
	기술적 점검	4	4	1
모니터링	로그관리	2	3	1
	관리자 및 운영자 로그	2	2	1
	시스템 사용 모니터링	2	3	1

평가 분야	세부 평가 항목	ISO 27001	K-ISMS	G-ISMS
	장애관리	1	4	2
	감사도구의 보호	3	1	1
	보안감사 계획 및 이행	3	9	1
	로그 정보의 보호	1	6	7
	시간 동기화	1	1	3
	정보 유출 방지	3		1
	기술적 취약성 통제	4		1
합계		330	396	310

[표 5] 국내지표 부문 비교

		정보보호관리 수준평가	전자정부서비스 보안수준실태조사	정보보호안전진단
정보보안정책	정보보안지침	5	1	15
	검토 및 평가	1	1	3
정보보안조직	정보보안조직	4		3
	정보보안협력	3		
	정보보안인력	3		15
정보보안계획 및 활동	정보보안계획	5		
	개인정보보안활동	5		
	정보보안사고 예방 및 대응	14	5	20
정보자산통제	정보취급절차	9		7
	정보자산 도입 및 폐기	8	2	
	매체 관리	6		
인적보안	인원보안	8	1	4

		정보보호관리 수준평가	전자정부서비스 보안수준실태조사	정보보호안전진단
	정보보안 교육 및 훈련	4	2	7
	정보보안의식 및 환경 조성	3		
	외주관리		1	8
물리적 보안	시설보안	20	1	12
	재난복구대책	10	1	
접근 보안대책	접근보안지침	4		
	네트워크 보안	21	7	10
	정보시스템 보안	10		
	사용자 인증 및 계정관리	19		5
	응용프로그램 접근통제	2	7	
운영관리	운영상의 변경통제	9		4
	정보보호시스템 보안	7		14
	악성코드 관리	4	5	
	PC보안 관리	6	5	

		정보보호관리 수준평가	전자정부서비스 보안수준실태조사	정보보호안전진단
	로그 및 모니터링	13	5	6
	백업	4	1	12
시스템 개발 및 유지보수	시스템 개발 및 정보보안 요구사항	11		
	운영소프트웨어 보안	5		
	외부 관리	3	1	
보안시스템	암호사용	9		
	암호장비	7		
	암호자재	7		
	암호논리	3		
이용자보호	정보보호 정보제공			7
정보통신설비보안	서버보안		4	14
	DB서버보안		2	7
	라우터/스위치보안			6

		정보보호관리 수준평가	전자정부서비스 보안수준실태조사	정보보호안전진단
	가용성		5	2
온라인거래 및 증명서 서비스 보안			20	
합계		252	77	181

[표 6] 개인정보보호 부문 비교

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
개인정보보호 관리과정	현황분석	5				8	3
	개인정보보호 대책마련	5					
	구현	2					
	사후관리	11					
개인정보보호 규정	정책 구비	3	1	3	2		5
	정책 승인 및 공표	4		1			
	정책 체계	2					
	정책 유지관리	2		1		7	1
개인정보보호 조직	개인정보보호 조직 구성 및 관리 책임자 지정	4			4		5

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
	책임 및 보고체계	5					
교육 • 훈련	교육 및 훈련 프로그램 수립	4		2	2		4
	시행 및 평가	3					
침해사고처리 • 대응절차	대응계획 및 체계	6			2		4
	대응 및 복구	10			1		4
	사후관리	4				6	
내부검토/이행 점검	법적요구사항 준수 검토	2					
	개인정보보호 정책 및 대책 준수검토	5		1			
	모니터링	9		2		3	
	이행점검에 대한 점검	8					
개인정보 수집에 따른 조치	최소한의 정보수집	6	10	8	1	4	

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
	개인정보 수집 시 고지 및 동의 획득	7	4	4	1	5	1
	개인정보취급 방침마련•게시	3	1	2	6	1	7
개인정보 이용에 따른 조치	동의 범위 내 개인정보 사용	2	4		14		
	개인정보취급자 관리	6		1	4		
	개인정보보호 서약	3		2			
	이용자 권리 보호	15		16	5		
	출력•복사시 보호조치	8				3	
	처리정보 이용 및 제공				9	3	

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
개인 정보 제공(위탁) 공유에 따른 조치	외부 위탁 시 개인정보보호	12		4	9	12	
	제3자 제공 시 개인정보보호	11					
	양도, 양수, 합병 등 개인정보 이전 시 개인정보보호	5		1			
	해외 이전 시 개인정보보호	4					
개인 정보 파기에 따른 조치	파기 규정	1			5	6	6
	파기 시점	3		1		2	2
	파기 방법	3		1		1	
	목적 달성 후 보유	4		1		4	

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
물리적 보안	물리적 보호구역, 물리적 접근통제, 환경 통제	6	12		73		
	개인정보 시스템 보호, 케이블 보호, 장비의 보수, 장비의 안전한 폐기 및 재사용	3					
	사무실 보호	3					
기술적 보안	분석 및 설계 보안, 구현 및 이행 보안, 변경관리	27	15				
	암호 정책, 암호 사용, 키관리	7				3	7

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
	접근통제 정책, 사용자 접근 관리, 접근통제영역	23					4
	운영절차와 책임, 네트워크 운영, 매체 및 문서관리, 악성 소프트웨어 통제, 원격 컴퓨터 및 원격작업	58		1		6	5
	공개서버의 보안관리, 이용자 공지사항	9					
기타	이메일발송 규정						

		PIMS	i-Safe	e-Privacy	PIA(공공)	PIA(기업)	공공기관 개인정보보호 수준진단
	만14세미만 아동 및 법정대리인 관련 규정		8	7			
	I-PIN 도입 여부				1		1
	기타(보험, 대리점 등)		3				
	소비자보호 분야		5				
	기타 홈페이지 관리 등						5
	CCTV				27		5
	RFID				16		
	바이오정보				24		
	위치정보				15		
합계		323	163	59	203	85	75

제 4 장 사이버보안지수 모델 및 방법론 제안

제 1 절 사이버보안지수 초안 지표 제안

앞서 언급한 정보보호 체계 및 지표 중 일부를 선택하여 다음과 같이 공통지표를 파악하였다. 그 이유는 본 연구의 최종 목표가 국제적인 정보보호평가지수 표준화가 가능한 지표개발이기 때문에 국내에서 공통적으로 사용되는 평가지표가 일반화된 평가기준이 될 것이라는 판단에서 공통지표 분석을 실시하게 되었다. 비교 분석 결과 150여개 공통 지표를 산출할 수 있었다. 하지만 대부분의 지표가 정량적 지표이어서 그대로 사용할 수 없는 문제점이 발생하였다. 이 지표들을 바탕으로 변경한 정량적 지표를 제시한다.

공통 지표 중에서 정량적으로 변경이 어려운 지표들은 필요하더라도 대부분이 제외되었다. 정량적으로 평가를 할 수 없다면 이 연구에서는 지표로 활용을 할 수 없기 때문에 평가에 필요하더라도 제외를 할 수 밖에 없었다. 그리고 공통 지표에 없는 지표나 필요하다고 판단되는 부분은 지표를 개발하여 조직 60개, 국가 21개의 사이버보안지수 지표 초안을 개발하였다.

제안하는 국가 및 조직 차원의 정보보호평가지수 모델은 설문지 [별첨X]를 통해 배포되었으며, 설문 결과 분석을 통해 초기 정보보호평가지수 모델을 개선하였다. 설문조사의 신뢰성 평가 및 분석 결과는 3장에서 언급하도록 한다.

제 2 절 사이버보안지수 지수화 방법론 제안

1. 지수화 방법

사이버보안지수의 지수화 방법론은 기존에 개발되어 있는 방법을 사용한다. 앞서 방법론 연구에서 언급했던 ITU의 ICT 개발지수와 III의 Cyber Health Check에서 사용하는 방법론을 이용하여 지수화 한다. 사이버보안지수의 지수화 방법은 지표 간 지수화와 지표 내 지수화를 나누어 사용한다.

지표 간 지수화와 지표 내 지수화를 살펴보면, 간단히 설명하면 지표간의 지수화는 서로 다른 지표들 간에 가중치와 점수를 계산하는 것이고, 지표 내 지수화는 해당 지표를 통해 얻어진 데이터에 대한 점수를 계산하는 것이다.

사이버보안지수에서 지표 간 지수화는 ITU의 ICT 개발지수의 방법론을 사용한다. 이 방법은 우리나라의 국가정보보호지수에서도 사용하는 방법으로, 같이 분야 안에서는 100을 지표의 수로 나누어 각각의 지표에 동일 가중치를 부여한다. 그리고 분야 간에 가중치는 전문가들의 의견을 통하여 가중치를 부여하는 방식을 사용한다.

그리고 지표 내 지수화는 III의 Cyber Health Check에서 사용하고 있는 정규 분포를 이용한 등급을 나누고 점수를 부여하는 방식을 이용한다. 이 방법을 통해 수집된 데이터에 대한 분포를 확인할 수 있고, 수집된 데이터가 분포하는 위치에 따라 10단계의 리커트(Likert) 척도를 사용하여 점수를 부여한다.

지표 내 지수화에서 수집된 데이터의 각각에 점수를 부여하여 지표 간 지수화 방법에서 수집된 데이터를 통한 점수화를 쉽게 할 수 있도록 하였으며, 분야 간의 가중치를 전문가의 의견을 통하여 부여함으로 중요한 분야와 중요도가 떨어지는 분야의 점수를 차별화하여 측정 시 조직이나 국가의 수준이 명확히 나타날 수 있도록 하였다.

2. 대체 평가 방법

대체 평가 방법이란, 국가 내에 정보보호를 수준을 평가·관리·감독을 담당하는 컨트롤타워가 설치되지 않은 경우 데이터 누락이 발생하는 것을 막기 위하여 해당 지표가 반영된 평가 인증체계로부터 인증 받은 인증서로 각 평가 지표를 대신하는 방안을 말한다.

예를 들면, 관리적 측면의 평가지표의 경우 전반적인 정보보호 분야의 관리 프로세스를 평가하는 ISO/IEC 27001의 평가 항목과 동일한 부분이 있다. 3.3절에서 지수화를 위해 선택된 지표들 중에서 어느 지표가 어느 인증기준에 부합되는지에 대한 결정은 각국이 지표와 함께 지표가 포함된 평가인증체계를 함께 제시하여 델파이 조사 과정 내에서 결정하는 방법이 있다.

또한, 국가정보보지수의 정보보호역기능 지표의 경우에도 컨트롤타워가 없는 국가의 경우, 기존 평가지표에 해당하는 데이터를 수집하지 못하여 데이터 누락이 발생할 수가 있다. 이렇게 데이터 누락이 발생하는 것을 피하기 위하여 피싱, 봇넷, 분산서비스 거부공격 지표의 값 산출에 APWG(Anti-Phishing Working Group), Shadowserver 조직의 통계, 조직의 정보보호 담당자 수준을 파악하는데 CISA, CISSP 자격증 취득자의 통계 등의 사용을 고려할 수 있다.

제 3 절 설문조사를 통한 신뢰성 평가 분석

지표의 신뢰성 및 지표 선정을 위하여 설문조사를 실시하였다. 설문 조사 대상은 설문의 신뢰성을 높이기 위하여 정보보호 및 정보통신 분야의 석사 학위 이상 또는 정보보호 및 정보통신 분야의 학사 학위 및 1년 이상의 실무 경력을 가진 대상으로 조사를 실시하였으며, 이러한 조건에 충족하는 대상에게 1차, 2차에 나누어 설문지를 배포하였다.

1차 설문지 배포는 정보보호 관련 종사자 및 KISA에서 추천한 전문가 등 총 37인에게 배포 되었으며, 2차 설문지 배포는 설문 응답자 중에서 설문 조사 대상을 추천이 온 14인에게 배포를 하였다.

1차, 2차에 걸쳐 총 51부의 설문지를 배포하여 최종적으로 32부를 돌려받았으며, 이 중에서 결측치가 많은 2부를 제외한 30부로 지표에 대한 설문을 분석하였다.

설문 분석에는 Cronbach 알파 측정과 수집가능성, 대표성, 적절성의 각각 값들의 평균을 이용하여 순위를 정하여 추출한 지표와 제거할 지표로 분류하였으며, 수집가능성, 대표성, 적절성의 각각의 평균으로 추출한 지표에서 수정이 필요한 지표를 다시 선정하였다.

1. 설문조사 분석 결과

본 연구에서는 여러 항목의 합산점수와 개별 항목의 점수 간 상관관계를 통해 신뢰성을 검증하는 내적일관성 신뢰도를 이용하여 신뢰성 분석을 실시하였다. 신뢰성 분석은 동일한 개념에 대해 지속적으로 반복 측정했을 때 동일한 값을 얻을 가능성을 말한다. 즉, 측정변수들이 같은 방향으로 움직이는지를 체크하는 것이 신뢰성분석의 목적이다. SPSS의 신뢰성분석을 통해 측정항목 간 내적일관성 정보를 Cronbach 알파 값으로 판단하게 되는데 학계에서는 일반적으로 0.8~0.9 이상, 마케팅 조사 실무에서는 0.6~0.7 이상이면 양호한 것으로 해석한다.

설문지의 평가 항목 수는 조직분야 58개(다수 누락이 있는 2개 항목 제외), 국가 분야 21개로 각 평가분야의 정보보호 수준을 측정하는 평가지표의 신뢰성 분석을 위해서 동일한 평가분야에 속하는 평가지표들의 1번~3번항목(수집가능성, 대표성, 적절성)의 값에 평균값을 이용하여 신뢰성 테스트를 진행하였다.

최종 30부의 최종 설문을 바탕으로 SPSS를 이용하여 일부 결측치를 제거한 후 Cronbach 알파를 이용하여 신뢰성을 테스트하였고, 각 평가 지표에 대한 신뢰성의 척도로 **데이터 수집가능성, 대표성, 지수화의 적절성(9점 척도)** 및 **중요도(3점 척도)**를 평가하였다.

(1) 데이터의 수집 가능성: 조직이나 각 국가에서 본 지표의 구현을 위해 원시 데이터 수집이 가능한 지표라고 생각하십니까?

(2) 평가 지표의 대표성: 본 지표가 통제 영역을 대표할 수 있는 지표라고 생각하십니까?

(3) 지수화의 적절성: 본 지표를 평가하기 위한 지수화 방법이 적절하다고 생각하십니까?

(4) 평가 지표의 중요도 측정: 평가에 있어 본 지표를 “필수/권고/선택/필요없음”으로 구분한다면 어떻게 선택하시겠습니까?

30부의 설문지를 받아 분석한 결과를 살펴보면 수집 용이성, 지표 대표성 지수화 적절성

에 대한 Cronbach 알파의 평균이 0.7 이상으로 지표에 문제가 없다고 판단 할 수 있다. 그리고 각 지표가 제외 되었을 경우(제외 CA)의 값이 크게 차이를 보이고 있지 않기 때문에, 각각의 지표 또한 적절히 개발되었다고 판단 할 수 있다.

수집 용이성, 지표 대표성, 지수화 적절성의 점수를 평균으로 하여 각 지표의 순위를 나누고, 지표의 중요도 점수와 함께 지표의 추출 기준으로 하였다. 이렇게 추출한 지표는 다시 전문가 의견을 통하여 지표를 수정하여 지표의 완성도를 높일 수 있도록 하였다.

아래 [표 8]과 [표 9]는 설문 결과를 토대로 신뢰성 분석을 실시한 결과이다. 설문 결과 Cronbach 알파 값이 9점 척도에 5.64~7.86의 값을 보였으며, 중요도의 경우 3점 척도에 1.65~2.76의 값을 보였다. 연구팀은 조직 및 국가 분야의 지표 선별을 위한 기준을 중요도 2.0 이상, 신뢰도 평균 6.5 이상, 신뢰도 순위의 경우 조직은 30위 이상, 국가는 10위 이하로 정하였다. 이 기준에 의해 2가지 이상의 기준을 만족할 경우 표준화를 위한 후보 지표로 선정하였다. 일부 지표의 경우 2가지 이상의 기준을 만족하지 않지만 국가정보보호지수를 개선하여 조직분야의 부호 지표로 개발한 경우가 있으며, 2가지 이상으로 기준을 만족하는 경우라도 표준화 지표로 선정함에 있어 기준을 제시할 수 없거나, 수집된 정보가 해커에 의해 악의적으로 이용될 수 있는 지표의 경우 후보 지표에서 제외하였다.

조직 추출 기준 : 중요도(2.0 이상) / 신뢰도 평균(6.5 이상) / 신뢰도 순위(30 이하)
국가 추출 기준 : 중요도(2.0 이상) / 신뢰도 평균(6.5 이상) / 신뢰도 순위(10 이하)

[표 7] 설문 결과 기호 설명

기호설명	
O	ITU-T SG17 제네바 회의(2010.12)에서 제안된 후보 지표 (국가분야의 경우, 조직분야의 표준화 이후 추진 예정)
△	후보 지표로 개발되었지만 2010.12 ITU-T SG17 제네바 회의에서 제안되지 않은 후보 지표(추후 지표 고도화 연구를 통하여 제안할 수 있음)
N	국가정보보호지수 혹은 국가정보보호지수를 보완한 지표로 추후 X.csi에서 국가 부분 지표를 표준화하는 경우에 사용될 수 있는 후보지표

[표 8] 설문결과 (조직)

설문 결과(조직분야)										
평가 지표	수집 용이성	제외 CA	지표 대표성	제외 CA	지수화 적절성	제외 CA	중요도	신뢰도 평균	신뢰도 순위	지표 개발 완료
1	6.24	0.79	5.93	0.72	5.62	0.79	2.345	5.93	55	O
2	7.03	0.81	5.93	0.74	5.61	0.81	2.357	6.19	40	O
3	6.70	0.79	6.27	0.73	5.97	0.79	2.200	6.31	34	
4	6.34	0.81	6.31	0.73	5.59	0.81	2.276	6.08	49	
5	6.33	0.82	5.71	0.74	5.29	0.82	2.080	5.78	57	O
6	6.93	0.80	5.93	0.73	5.93	0.80	2.077	6.26	36	O
7	7.00	0.78	6.66	0.74	6.21	0.78	2.448	6.62	24	△
8	7.03	0.79	6.67	0.74	6.57	0.79	2.133	6.76	12	△
9	6.60	0.80	5.83	0.75	5.33	0.80	1.786	5.92	56	
10	7.80	0.79	7.00	0.73	6.72	0.79	2.533	7.17	5	O
11	6.97	0.81	6.17	0.74	6.14	0.81	2.167	6.42	29	O
12	6.63	0.81	6.43	0.73	6.34	0.81	2.100	6.47	27	△
13	6.72	0.82	5.25	0.75	4.72	0.82	2.231	5.56	58	O
AVE CA		0.82		0.75		0.82				7개
14	7.23	0.92	6.43	0.86	6.37	0.90	2.429	6.68	21	O
15	7.13	0.91	6.14	0.87	6.29	0.90	1.964	6.52	25	△
16	7.33	0.92	6.21	0.87	5.61	0.90	2.345	6.38	30	O
17	7.60	0.92	6.87	0.86	6.40	0.90	2.333	6.96	10	O
18	6.79	0.92	6.18	0.87	5.46	0.91	2.172	6.15	45	O
19	6.67	0.92	5.87	0.87	5.47	0.91	1.966	6.00	53	
20	6.79	0.92	5.90	0.87	5.32	0.90	1.963	6.00	51	
21	7.52	0.92	6.30	0.86	6.21	0.90	2.000	6.67	23	O
22	7.20	0.92	6.28	0.87	5.96	0.90	2.250	6.48	26	O
23	6.67	0.92	5.80	0.87	5.97	0.90	1.767	6.14	46	
24	6.83	0.92	6.03	0.87	5.93	0.90	1.833	6.27	35	
25	6.81	0.92	6.00	0.87	5.74	0.90	1.867	6.19	43	
26	6.57	0.92	6.10	0.87	5.90	0.90	1.897	6.19	41	
27	7.38	0.92	7.00	0.87	6.73	0.90	2.467	7.04	8	O
28	7.21	0.92	7.00	0.87	6.79	0.90	2.448	7.00	9	O

설문 결과(조직분야)										
평가 지표	수집 용이성	제외 CA	지표 대표성	제외 CA	지수화 적절성	제외 CA	중요도	신뢰도 평균	신뢰도 순위	지표 개발 완료
29	6.86	0.92	6.17	0.87	5.66	0.90	2.233	6.23	38	
30	7.63	0.92	7.40	0.87	7.70	0.91	2.767	7.58	3	O
31	7.47	0.92	6.57	0.87	6.10	0.90	2.276	6.71	18	O
32	7.63	0.92	7.23	0.87	6.60	0.90	2.667	7.16	7	△
33	7.57	0.92	6.43	0.87	6.13	0.90	2.200	6.71	15	O
34	7.43	0.92	6.57	0.87	6.13	0.90	2.552	6.71	17	△
35	7.31	0.92	6.55	0.87	6.18	0.91	2.241	6.68	20	△
36	7.13	0.92	6.13	0.87	5.83	0.90	2.100	6.37	31	O
37	6.66	0.92	6.31	0.88	6.00	0.91	2.000	6.32	32	
38	6.97	0.92	5.83	0.87	5.52	0.90	2.153	6.11	48	
39	6.77	0.92	6.20	0.87	5.59	0.90	2.179	6.18	44	
40	6.22	0.92	6.28	0.87	5.90	0.90	2.037	6.13	47	
41	7.00	0.92	6.30	0.87	6.03	0.90	1.900	6.44	28	
42	7.17	0.92	7.07	0.88	6.10	0.90	2.400	6.78	11	△
43	6.73	0.92	6.53	0.88	5.50	0.90	2.267	6.26	37	
AVE CA		0.92		0.87		0.91				12개
44	6.17	0.83	6.20	0.80	5.64	0.73	2.034	6.00	52	
45	6.80	0.82	5.97	0.82	5.79	0.72	1.655	6.19	42	
46	8.10	0.83	7.73	0.81	7.73	0.74	2.767	7.86	1	O
47	7.25	0.84	6.37	0.81	6.43	0.74	1.833	6.68	19	O
48	6.90	0.82	6.07	0.83	5.00	0.77	2.207	5.99	54	
49	6.79	0.81	6.31	0.82	5.50	0.76	2.200	6.20	39	O
50	7.67	0.83	7.27	0.81	6.57	0.72	2.600	7.17	6	O
51	6.53	0.82	6.10	0.81	6.30	0.73	1.862	6.31	33	
52	6.14	0.81	6.07	0.80	6.00	0.71	1.814	6.07	50	
53	6.67	0.83	6.73	0.82	6.73	0.75	2.000	6.71	15	O
54	6.90	0.83	6.73	0.83	6.57	0.75	2.100	6.73	14	O
55	7.83	0.82	7.40	0.81	7.17	0.75	2.533	7.47	4	O
56	7.50	0.82	6.37	0.82	6.34	0.75	1.767	6.74	13	△
57	7.97	0.83	7.90	0.81	7.67	0.75	2.633	7.84	2	O

설문 결과(조직분야)										
평가 지표	수집 용이성	제외 CA	지표 대표성	제외 CA	지수화 적절성	제외 CA	중요도	신뢰도 평균	신뢰도 순위	지표 개발 완료
58	7.17	0.82	6.60	0.81	6.27	0.73	1.931	6.68	21	△
AVE CA		0.83		0.82		0.75				8개

[표 9] 설문 결과 (국가)

설문 결과(국가분야)										
평가 지표	수집 용이성	제외 CA	지표 대표성	제외 CA	지수화 적절성	제외 CA	중요도	신뢰도 평균	신뢰도 순위	지표 개발 완료
1	7.00	0.21	7.10	0.35	7.17	0.48	2.600	7.09	1	△
2	6.83	0.21	6.11	0.08	5.64	0.06	1.767	6.19	15	
3	6.38	0.53	6.14	(0.08)	5.59	0.47	2.036	6.04	16	N
AVE CA		0.43		0.19		0.44				
4	6.34	0.80	6.00	0.77	5.19	0.73	2.179	5.85	18	
5	6.25	0.79	5.86	0.74	4.81	0.71	2.172	5.64	21	O/N
6	6.83	0.80	6.57	0.79	6.43	0.77	2.167	6.61	6	△
7	6.66	0.82	5.45	0.76	5.12	0.73	1.929	5.74	20	O
8	7.04	0.83	5.78	0.75	5.28	0.73	1.889	6.03	17	O
9	6.53	0.80	6.86	0.79	6.56	0.76	2.379	6.65	5	O/N
10	7.17	0.81	6.86	0.77	6.43	0.75	2.069	6.82	4	N
11	6.72	0.85	6.28	0.81	6.17	0.75	1.897	6.39	9	
12	7.33	0.83	6.70	0.75	6.50	0.76	1.967	6.84	3	
AVE CA		0.83		0.79		0.77				
13	7.07	0.78	6.63	0.72	5.83	0.76	2.333	6.51	8	N
14	5.75	0.83	6.03	0.77	5.61	0.83	1.867	5.80	19	N
15	6.40	0.76	6.30	0.75	5.90	0.76	1.967	6.20	14	N
16	6.40	0.76	6.30	0.73	5.93	0.76	1.967	6.21	12	N
17	6.62	0.79	6.47	0.75	5.96	0.78	2.000	6.35	10	N

설문 결과(국가분야)										
평가 지표	수집 용이성	제외 CA	지표 대표성	제외 CA	지수화 적절성	제외 CA	중요도	신뢰도 평균	신뢰도 순위	지표 개발 완료
18	6.53	0.81	6.63	0.77	6.45	0.82	2.067	6.54	7	△
19	7.07	0.79	6.30	0.78	5.25	0.84	2.000	6.21	13	O
20	7.07	0.83	6.10	0.78	5.57	0.81	1.897	6.25	11	O/N
21	7.53	0.82	7.20	0.76	6.30	0.84	2.600	7.01	2	N
AVE CA		0.82		0.78		0.82				

2. 개선사항 분석 및 반영

앞서 분석한 설문지 점수와 전문가들의 의견을 토대로 지표를 제거 또는 수정하였다. 아래 표는 제거 또는 수정된 지표가 전문가들에게 받은 의견을 정리해두었다. 수정된 지표는 표준화로 추진하기 위한 기본 지표로 활용하였다. 그러므로 실제 기고서에 제안된 지표와는 차이가 있을 수 있다.

[그림 41] 사이버보안지수 모델

추출된 지표는 그림과 같이 정보보호 구현, 정보보호 기반, 정보보호 환경으로 다시 분류하였다. 정보보호 구현 5개 지표에는 위험제거 4개(취약점 조치비율, 취약점 권고비율, 사고, 최신패치 설치비율), 침해사고 대응 1개(보안사고 대응비율)이 포함되었고, 정보보호 기반 14개 지표에는 보안관리 11개(백신프로그램 설치비율, 긴급복구계획 테스트비용, 보안평가

승인비율, 보안서약비율, 원격접근 통제비율, 보호된 무선 AP비율, 네트워크 이중화 비율, 인사 보안 심사 비율, 개인식별 정보보호 비율, 백업정보의 무결성 점검비율, 출입통제시스템 도입비율), 정보보호 시스템 도입 3개(정보보호관리시스템의 범위 비율, 보안서버 비율, 정보보호 관리시스템 인증비율)가 포함되었다. 그리고 정보보호 환경 20개에는 정보보호 수준 13개(이용자의 스팸메일 인식 비율, 보안교육 및 훈련 비율, 정보보호 인력 비율, 전자서명 이용 비율, 정보보호 교육기관 설립 비율, 백신 보급률, 패치 보급률, PKI 보급률, Firewall 보급률, IDS 보급률, 보안서버 보급률, 정보보호 관련 예산 비율, 국민의 보안의식 수준 비율), 정보화 역기능 수준 7개가(악성소프트웨어 감염 비율, 개인정보 노출 비율, DDoS 측정, 봇넷 감염 비율, 해킹 및 바이러스 신고비율, 개인정보 침해 신고비율, 스팸메일 수신비율) 포함되었다.

지표의 분포를 보면 정보보호 구현에서 조직 대 국가 비율이 80 대 20의 비율이고, 정보보호 기반은 79대 21의 비율, 정보보호 환경은 65 대 35의 비율로 조직의 지표와 국가의 지표의 비율이 비슷해 보이나, 지표의 개수를 보면 정보보호 환경에 국가의 지표가 많이 있는 것을 알 수 있다. 이것은 국가 수준에서 측정할 수 있는 지표는 구현이나 기반을 측정하는 것이 환경적 측면에 대한 부분을 측정하는 것보다는 어려움이 많이 따르기 때문이다.

[표 10] 조직분야의 후보 지표

후보 지표(조직분야)				
지표 1				
수정전	평가분야	정보보호 구현	평가목적	정보보호 위험 제거
	평가지표	취약점 관리	지표성격	선행지표
	통제목적	조직은 조직 내의 취약점을 식별하고, 식별된 취약점에 대한 적적한 조치를 해야 한다.		
	지수화 방법론	$(\frac{\text{조치된 취약점의 개수}}{\text{식별된 취약점의 개수}}) \times 100$		

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">* 식별된 취약점의 개수를 기반으로 지수화 하는 것이 맞으나, 식별되지 않는 잠재적인 취약점에 대한 식별도 고려되어야 할 것 같습니다.
* 해당 조직마다 내부 환경과 여건이 서로 다르고, 취약점에 대한 데이터 수집 및 공개는 매우 민감한 사항이라 평가 행위가 불가능할 것이라 판단됨. 또한, 지수화 방법론에서 "식별된 취약점"에 대한 객관적인 수치나 기준이 있는지 궁금함.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 구현(S)</td><td>평가목적</td><td>위험 제거</td></tr>
<tr><td>평가지표</td><td>취약점 조치비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 취약점을 식별하고, 식별된 취약점에 대한 적정한 조치를 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{조치된 } CVE\text{의 개수}}{\text{연간 조치가 필요한 } CVE\text{의 개수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 2</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>감사 및 책임</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 부적절한 활동을 모니터링, 분석, 조사를 위해 정보 시스템 감사기록을 생성, 보호, 보관해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{중앙에서 감사로깅이 가능한 전체 } PC\text{개수}}{\text{전체 } PC\text{개수}}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 현실적으로 평가는 가능한 벡터라고 생각되지만, 중앙에서 감사로깅 가능한 PC가 많다고 안전성이 높다고는 판단되지 않음. 물론, 적다고 해서 불안전한다고 판단 암됨.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 구현(S)</td><td>평가목적</td><td>위험 제거</td></tr>
<tr><td>평가지표</td><td>감사로깅 비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 부적절한 활동을 모니터링, 분석, 조사를 위해 정보 시스템 감사기록을 생성, 보호, 보관해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{감사로깅이 가능한 } PC\text{대수}}{\text{전체 } PC\text{대수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 3</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>감사 및 책임</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 부적절한 활동을 모니터링, 분석, 조사를 위해 정보 시스템 감사기록을 생성, 보호, 보관해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{부적절한 활동이 탐지된 } PC\text{개수}}{\text{전체 } PC\text{개수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 부적절한 활동에 대한 명확한 정의가 필요할 것으로 보임. 개인정보에 대한 수집에 대한 법적인 대응력이 전제되어야 함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 조직의 피해기준을 정의하기 어려우며, 피해를 주는 부적절한 활동에 대한 기준 제시가 어려움</td></tr>
<tr><td colspan="5">지표 4</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>위협 평가</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{업무연속성 계획에 반영된 위협의 개수}}{\text{위험분석을 통해 식별된 위협의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 주기적인 수행여부를 수치화 할 수 있는 기준이 필요하며, 기준에 따라 주기적인 수행여부를 판단하여 이를 반영해야 함
* (기간 별 위험분석 실시 수) / (기간별 위험분석 실시 계획 횟수) x 100 이 먼저 이뤄져야 할 것입니다. 위협은 환경에 따라 달라질 수 있기 때문에 위협의 개수와 업무연속성계획에 반영했다는 것으로 판단하기 어려울 것 같습니다.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 조직의 위험분석 실시 기준에 대한 명확한 기준 제시가 어려움</td></tr>
<tr><td colspan="5">지표 5</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>위협 평가</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직원에게 메일링 서비스에 대한 안전한 교육을 실시하고, 스팸 메일의 대응 능력을 평가한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{스팸메일을오픈한수}+\text{첨부파일을클릭한수}}{\text{전체조직원의수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 이메일을 통한 악성코드 유포되고 있으므로 좋은 데이터가 될 것으로 판담됨.
* 인식 제고(교육/캠페인) 또는 스팸방지솔루션 등을 이용하여 보완 가능.
* 스팸 메일의 대응 능력을 평가한다는 면에서 스팸 메일 오픈한 수나 첨부파일을 클릭한 수를 확인한다는 취지는 좋지만 개인별로 스팸 메일이나 첨부파일에 대한 읽기, 삭제 등을 통제하고 확인한다는 것이 어려울 것 같습니다. 전체 조직원 대비 교육 수강 비율이나 설문조사가 실제적으로 적용가능 할 것입니다.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>모의훈련을 통한 스팸메일 대응비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 모의훈련을 통하여 조직원에게 메일링 서비스에 대한 안전한 교육을 실시하고, 스팸 메일의 대응 능력을 평가한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{스팸메일을오픈한 or 첨부파일을실행한인원수}}{\text{전체조직원의수}})]\times 100$</td></tr>
<tr><td colspan="5">지표 6</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>위협 평가</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{스팸메일신고건수}}{\text{전체스팸메일발송건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 스팸메일이 위협평가의 일부가 될 순 있다고 생각. 전체 스팸메일 발송과 메인신고와는 조직의 보안의식 수준과 관련되어 있을 것으로 생각됨</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>모의훈련을 통한 스팸메일 신고비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직원이 스팸메일의 위험성에 대한 경각심을 갖도록 교육을 실시하고, 모의훈련을 통하여 신고건수를 평가한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{스팸메일신고건수}}{\text{전제조직원의수}})\times 100$</td></tr>
<tr><td colspan="5">지표 7</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>위협 평가</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{업무연속성계획에따라조치된취약점의개수}}{\text{취약점스캔을통해식별된취약점의개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 업무연속성 계획에 반영된 위협의 개수도 중요하지만, 즉시 조치되거나 단기 및 중장기 계획으로 반영되는 사항도 고려해야 함. 조직마다 점검도구가 상이할 수 있으므로 타 조직과의 비교지표로 활용 시, 정확한 비교가 어려울 수 있음.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 1번 항목과 동일</td></tr>
<tr><td colspan="5">지표 8</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>유지관리</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보 시스템에 대해 주기적이고 시기적절한 유지관리 수행 및 효율적 통제를 제공해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{공식적인유지관리스케쥴에따라관리되는시스템의개수}}{\text{전체시스템의개수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">* 효율적인 통제를 제공하기 위한 지수화는 관리되는 시스템의 개수뿐만 아니라 유지관리 사이클 및 유지관리 건수 등의 비율이 추가되어야 할 것 같음.
* 일반적으로 각 시스템 제공 업체별로 정기 및 수시로 유지보수를 해주고 있으며, 공식적인 스케쥴에 따라 관리되어야 효율적인 통제가 되고 있는지에 대한 의문이 생김.
* 유지관리 되고 있는 시스템의 비율을 확인하는데 좋을 것 같습니다. 하지만 공식적인, 스케줄이면 요구하는 조건이 다를 것 같습니다.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 각 조직의 유지관리 사이클에 대한 공통된 기준을 제시하기 어려움</td></tr>
<tr><td colspan="5">지표 9</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>유지관리</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보 시스템에 대해 주기적이고 시기적절한 유지관리 수행 및 효율적 통제를 제공해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{전체 시스템의 오류 발생건수}}{\text{전체 시스템 개수}\times\text{점검횟수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 오류의 중요도에 따라 지수화방법론의 가중치가 차등 적용되어야 하나, 현실적으로 측정이 애매해질 가능성 존재.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 점검횟수와 유지관리의 효율성과 연관성이 적음</td></tr>
<tr><td colspan="5">지표 10</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>정보보호 위험 제거</td></tr>
<tr><td>평가지표</td><td>시스템 및 정보 무결성</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보 시스템에 대한 신규 보안 위협에 대처하기 위하여 자동화된 패치 관리 시스템을 도입하여 운영해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{패치 관리 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">* 현재는 적정한 지수화 방법이라고 생각되지만, 점차 필수적으로 패치관리 프로그램, 보안 프로그램 등이 설치되고 있는 추세를 고려해야 함.
* 서버 진단 경험 상 패치관리 프로그램이 설치되었음에도 불구하고 서비스 유지를 위해 실제 패치를 진행치 않은 경우가 많았음. 실제 패치가 이루어지는 지에 대한 지표가 필요함.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 구현(S)</td><td>평가목적</td><td>위험 제거</td></tr>
<tr><td>평가지표</td><td>패치관리프로그램 설치비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보 시스템에 대한 신규 보안 위험에 대처하기 위하여 패치관리시스템을 도입하고 최신 패치를 유지해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{패치관리프로그램이설치된}\ PC\text{대수}}{\text{전체}\ PC\text{대수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 11</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>침해사고 대응</td></tr>
<tr><td>평가지표</td><td>긴급사태 대책</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 지속적인 서비스 운영을 위한 긴급사태 대책을 수립/관리하고 효율적으로 구현한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간긴급사태계획테스트를수행하는정보시스템의개수}}{\text{시스템목록에있는정보시스템의개수}}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 지속적인 서비스 운영을 위하여 긴급사태에 대응 테스트를 수행하는 정보시스템뿐만 아니라 긴급사태 발생 시 지원 가능한 여분의 정보시스템에 대해서도 고려되어야 할 것 같습니다.
* BCP / DRP 를 위해서 필요.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 구현(S)</td><td>평가목적</td><td>침해사고 대응</td></tr>
<tr><td>평가지표</td><td>긴급복구계획 테스트비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 지속적인 서비스 운영을 위하여 조직이 서비스 중인 자산 전반에 대한 긴급사태 대책을 수립/관리해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간긴급사태계획테스트수행대상시스템의개수}}{\text{정보자산에등록된시스템의개수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 12</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>침해사고 대응</td></tr>
<tr><td>평가지표</td><td>긴급사태 대책</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 지속적인 서비스 운영을 위한 긴급사태 대책을 수립/관리하고 효율적으로 구현한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{초기대응성공건수}}{\text{연간긴급사태발생건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* DDoS 등의 문제 발생 시, 신속한 업무 복구율 등을 평가하기 위한 중요한 벡터라고 판단됨
* 의미에 있어서는 지표의 내용이 적절하나 연간 긴급사태가 발생하는 건수가 실제로는 매우 적거나 없을 가능성이 높기 때문에 실효성이 없는 지표로 보입니다.“초기” 대응이라는 의미에 대해서도 정의가 필요합니다.
* 정확한 가이드가 없을 경우 그 범위가 정확하지 않음</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 복구 시간 및 긴급사태에 대한 기준 제시 미비.</td></tr>
<tr><td colspan="5">지표 13</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>침해사고 대응</td></tr>
<tr><td>평가지표</td><td>사건 보고</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 보안사고의 신속한 대응을 위해 사건보고 시스템을 운영하고, 보안 교육 및 모의 훈련을 통해 이를 점검해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{모의훈련횟수}}{\text{보안교육횟수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 보안 교육 및 모의 훈련을 하는 것을 확인해야 하는 것이지 모의 훈련 횟수와 보안 교육 횟수의 비율을 확인하는 것이 아닙니다. 일정 기간 내의 모의 훈련 시간이나 보안 교육 시간의 비율을 확인하는 것이 좋을 것 같습니다.</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>보안교육 및 모의훈련 시행비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 보안사고의 신속한 대응을 위해 보안 교육 및 모의 훈련을 실시해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간 보안교육 및 모의훈련 시행 횟수}}{\text{연간 보안교육 및 모의훈련 계획 횟수}})\times 100$</td></tr>
<tr><td colspan="5">지표 14</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>증명, 승인, 보안 평가</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 모든 정보 시스템에 요구되는 보안 증명 및 승인을 받아야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{구현 이전에 인가담당자에게 } CA \text{ 받은 신규 시스템의 개수}}{\text{전체 신규 시스템의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">-</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안관리</td></tr>
<tr><td>평가지표</td><td>보안평가 인증비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 모든 정보 시스템에 요구되는 보안 증명 및 승인을 받아야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{도입 이전에 인가담당자에게 } CA \text{ 받은 신규 시스템의 개수}}{\text{전체 신규 시스템의 개수}})\times 100$</td></tr>
<tr><td colspan="5">지표 15</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>증명, 승인, 보안 평가</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 모든 정보 시스템에 요구되는 보안 증명 및 승인을 받아야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{연간 발견된 비인가 시스템의 개수}}{\text{인가 받은 시스템의 개수}})]\times 100$</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 결과적으로 14번 항목과 동일</td></tr>
<tr><td colspan="5">지표 16</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 보유</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보통신망의 안전성 및 정보통신 설비 보호를 위해 정보보호 시스템을 설치/운영함으로써 네트워크 보안을 강화한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{전체 정보보호 시스템 도입 개수}}{\text{전체 서버의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 전체 서버개수 대비 정보보호시스템 개수에 대한 비율 보다 서버, 네트워크 장비 등 전체 시스템 규모를 파악하여 정보보호시스템 권고 기준에 얼마만큼 충족하는 지에 대한 지표 반영을 권함
* 서버 대비 정보보호 시스템 대비 정보보호 시스템 전체 시스템을 구성하는 규모 대비 정보보호 시스템의 적용을 확인하는 편이 좋을 것 같습니다.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>방화벽, IDS, IPS 도입개수</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보통신망의 안전성 및 정보통신 설비 보호를 위해 정보보호 시스템을 설치/운영함으로써 조직의 정보 자산을 보호한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{방화벽 or } IDS \text{ or } IPS \text{ 도입 개수}}{\text{전체 서버의 개수}})\times 100$</td></tr>
<tr><td colspan="5">지표 17</td></tr>
</table>

<table>
<tr><th colspan="6">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 보유</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">주요정보 전송시 비밀성과 무결성을 보장하는 보안서버구축 등의 조치를 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{보안서버의 개수}}{\text{전체서버의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">-</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td colspan="2">정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>보안서버 비율</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">주요정보 전송시 비밀성과 무결성을 보장하는 보안서버구축 등의 조치를 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{보안서버의 개수}}{\text{전체서버의 개수}})\times 100$</td></tr>
<tr><td colspan="6">지표 18</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 보유</td><td>지표성격</td><td colspan="2">후행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">조직은 급격한 트래픽 증가로 인한 네트워크 공격을 방어하기 위한 장비를 도입해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$[1-(\frac{\text{일일평균트래픽량}}{DDoS\text{방화벽의최대트래픽처리량}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 장비 도입의 유/무를 확인하는 것이 우선일 것이고 어느 정도의 트래픽을 처리할 수 있는지 확인하기 위해서는 방화벽의 (최대 트래픽 처리량) / (일일 평균 트래픽 처리량) 으로 100%의 지수가 아닌 상대지수를 활용하는 것이 좋을 것 같습니다.
* 지수화 방법론에서 방화벽 최대 트래픽 처리량에 대한 부분도 필요하지만, 최근 발생
하는 공격 형태는 회선 및 서버의 과부화는 거는 형태 등으로 복합적으로 발생하고 있으므로,이에 대한 추가적인 지표가 필요하다고 생각함.</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>수정후</td><td colspan="4">[제외] 실질적인 트래픽 공격을 막아내는 지수로는 부족함. 100점 만점으로 환산하기 위한 지수 개발이 필요</td></tr>
<tr><td colspan="5">지표 19</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>시스템 및 서비스 구입</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">아웃소싱 제공자가 조직으로부터 아웃소싱된 정보, 응용, 서비스를 보호하기 위해 적절한 보안 측정을 만족함을 보장한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$\left(\frac{\text{보안요구사항 및 명세를 포함하는 계약서의 개수}}{\text{시스템 및 서비스 구입 계약서의 전체 개수}}\right)\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 표준계약서에 보안요구사항이 명시되어 있다면 따로 측정할 필요성은 없어 보이나, 항목의 중요도를 고려하였을 때는 나름대로 의미 부여 가능.
* 모든 시스템 및 서비스가 보안과 관련된 것은 아니므로, 본 지수는 타당하지 않은 것으로 보임</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] ISMS 인증 지수로 대체 가능</td></tr>
<tr><td colspan="5">지표 20</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>시스템 및 서비스 구입</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">시스템은 유지관리를 통해 도입 계획 기간 내의 가용성을 보장해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$\left(\frac{\text{실제 운영중인 시스템의 개수}}{\text{시스템 및 서비스 구입 계약서의 전체 개수}}\right)\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 가용성 평가 측면으로는 좋은 항목이나 보안과는 연관성이 다소 떨어져 보임.
* (유지관리 계약이 맺어진 시스템 개수 / 운영중인 시스템 개수) X 100 실제 운영 중인 시스템 개수의 비율 보다 유지관리가 진행 중인 시스템 개수의 비율이 적절하다고 판단됨
* 가용성의 보장이란 실제 운영이 아니라 제대로 동작하느냐를 묻는 것입니다.</td></tr>
</table>

<table>
<tr><th colspan="6">후보 지표(조직분야)</th></tr>
<tr><td>수정후</td><td colspan="5">[제외] 가용성 부분 평가는 31번 항목으로 대체</td></tr>
<tr><td colspan="6">지표 21</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 도입</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">조직은 글로벌 선진 기업들의 Best Practice에 기반한 정보보호 관리 체계를 수립함으로써 조직의 신뢰도를 향상시킨다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$\left(\frac{ISMS\text{재인증횟수}}{(\frac{\text{현재년도}-\text{최초인증년도}}{3})}\right)\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 최초인증년도와 인증유지여부 확인만 되면 문제없음.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td colspan="2">정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 관리시스템 인증 비율</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">조직은 글로벌 선진 기업들의 Best Practice에 기반한 정보보호 관리 체계를 수립함으로써 조직의 신뢰도를 향상시킨다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$\left(\frac{ISMS\text{인증에 포함된 시스템 개수}}{\text{전체 시스템 개수}}\right)\times 100$</td></tr>
<tr><td colspan="6">지표 22</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">보안 관리</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 도입</td><td>지표성격</td><td colspan="2">후행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">조직의 정보 시스템을 위해서 행동규칙 및 보안 계획을 수립하고 이를 주기적으로 업데이트해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{행동규칙에 대해서명이후 시스템접근을 획득한사용자수}}{\text{전체 시스템접근자수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">* 절차나 보안 계획의 유/무가 우선이고 보안 계획서에 따른 증적의 유/무나 있어야 하는 증적의 수 대비 실제 있는 증적 수를 확인하는 것이 좋을 것 같습니다.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>보안서약 비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보 시스템을 위해서 행동규칙 및 보안 계획을 수립하고, 시스템 접근 이전에 보안서약을 받아야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{보안규정에 서명한 사용자 수}}{\text{전체 조직원 수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 23</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>설정 관리</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 시스템 개발 라이프 사이클을 통해 기본 설정을 수립하고, 조직 정보 시스템의 목록을 유지한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{자동화된 시스템 개발 라이프 사이클을 적용한 자산의 개수}}{\text{전체 정보자산의 개수}}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 자산을 보호하기 위해 자동화 시스템을 적용한 벡터가 안전성 평가 항목으로 보기에는 부적절하다고 판단됨
* 자동화되어 있다면 따로 지표화 시킬 필요는 없어 보임.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 자동화에 대한 기준 정의가 어려움</td></tr>
<tr><td colspan="5">지표 24</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>설정 관리</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 시스템 개발 라이프 사이클을 통해 기본 설정을 수립하고, 조직 정보 시스템의 목록을 유지한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{승인 및 구현된 설정 변경 건수}}{\text{자동화된 스캔으로 식별한 설정 변경 건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 설정 등의 변경을 승인 받았다고 안전하다고 말할 수 있는지? 또한, 자동화된 스캔이라는 전제 조건이 있음</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 자동화에 대한 기준 정의가 어려움</td></tr>
<tr><td colspan="5">지표 25</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>시스템 및 통신 보안</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 전자 정보 인프라의 적절한 보호를 위해 충분한 자원을 할당해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{암호학적 연산을 수행하는 모바일 컴퓨터 및 장치의 개수}}{\text{조직의 모바일 컴퓨터 및 장치의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 지수화에 있어 모바일 컴퓨터를 기반으로 비율을 정하는 것에 대한 이유를 알 수 없음. 시스템 및 통신 보안을 평가하기 위해 충분한 자원 할당과 모바일 컴퓨터의 연관성이 없어 보임.
* 통제목적과 지수화 방법론간의 관련성이 미약함 모바일 컴퓨터 및 장치의 개수가 분모로 반드시 해야 한다면, 분자를 변경함으로써 원하는 결과를 도출할 수 있을 것 같음.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 30번 항목과 목적이 유사함</td></tr>
<tr><td colspan="5">지표 26</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>시스템 및 통신 보안</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 전자 정보 인프라의 적절한 보호를 위해 충분한 자원을 할당해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{인증, 암호화, 부인방지 기능을 이용한 전자상거래 건수}}{\text{연간 전자상거래 건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 보안기능의 적용 비율을 확인하는 것은 좋지만 전자상거래가 모든 조직에 해당되는 것이 아니므로 대표하는 지표는 아닙니다.
* 전자상거래는 일부 조직에 국한된 벡터로 객관성 결여</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 암호화 통신을 목적으로 하는 17번, 34번, 39번 항목과 유사</td></tr>
<tr><td colspan="5">지표 27</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>접근 통제</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 정보 자산에 접근할 수 있는 엑세스 포인트에 대한 접근 통제를 수행해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{침입차단/탐지 시스템이 설치된 엑세스 포인트의 개수}}{\text{전체 엑세스 포인트의 개수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 암호화를 활성시켜 놓은 엑세스 포인트의 개수를 분자로 가져가는 것이 명확할 것으로 보임</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>네트워크 접근통제비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 정보 자산에 접근할 수 있는 엑세스 포인트에 대한 접근 통제를 수행해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{침입차단/탐지 시스템이 설치된 게이트웨이의 개수}}{\text{전체 게이트웨이의 개수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td colspan="5">지표 28</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>접근 통제</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 정보 자산에 접근할 수 있는 엑세스 포인트에 대한 접근 통제를 수행해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{비인가 접근이 획득된 엑세스 포인트의 개수}}{\text{전체 엑세스 포인트의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 앞에 평가 항목과 동일한 성격이라고 판단됨. 통합하는 게 적합함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 결과적으로 27번 항목과 유사함. 선행지표의 평가가 효율적임</td></tr>
<tr><td colspan="5">지표 29</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>물리적 환경</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보 자원의 적절한 보호를 보장하기 위해 물리적 보호 메커니즘과 정보보호 메커니즘을 통합한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{비인가출입을허가한물리적안전사고발생건수}}{\text{전체물리적안전사고발생건수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 비인가출입에 의한 물리적 안전사고 발생의 상대적인 비율을 알아보기 위한 것이니 해당 지표로는 안전하다/위험하다를 판단하기에는 부족합니다.
* 비인가 출입을 허가하여 안전사고가 발생했다면, 그 조직은 상황에 따라 이미 와해되었을 수 있음. 따라서 비인가출입이 발생한 건수를 분자로 가져가는 것이 타당할 것으로 생각됨. 비인가출입 발생은 출입 로그와 CCTV 등의 대조를 통해 손쉽게 밝혀낼 수 있기 때문</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 32번 항목으로 대체</td></tr>
<tr><td colspan="5">지표 30</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>물리적 환경</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 물리적 접속 통제를 위해서 무선 엑세스 포인트를 관리해야 하며, 적절한 수준의 보안설정을 유지해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{보안이 설정된 무선 엑세스 포인트 개수}}{\text{조직내의 전체 무선 엑세스 포인트 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 물리적 환경의 평가지표와. 통제목적에서 무선엑세스 포인트의 설정보안에 대한 것은 대표성이 부족하다고 판단</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>무선AP의 보안설정비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 무선 AP를 통한 내부 네트워크로의 비인가 접근을 방지하고, 도청을 방지하기 위하여 일정 수준 이상의 보안설정을 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{보안이 설정된 무선 엑세스 포인트 개수}}{\text{조직내의 전체 무선 엑세스 포인트 개수}})\times 100$</td></tr>
<tr><td colspan="5">지표 31</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>물리적 환경</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 네트워크의 가용성에 대한 중대한 영향을 미치는 회선에 대해 서비스의 가용성과 연속성을 보장할 수 있어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{이중화된 네트워크 장비의 대수}}{\text{전체 네트워크 장비의 대수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 모든 네트워크 장비에 대하여 이중화 시키는 것은 아니므로 이중화가 필요한 장비 수를 반영하는 것을 권함</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>네트워크 이중화비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 네트워크의 가용성에 대한 중대한 영향을 미치는 회선에 대해 서비스의 가용성과 연속성을 보장할 수 있어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{이중화된 링크 수}}{\text{전체 네트워크 장비의 대수}})\times 100$</td></tr>
<tr><td colspan="5">지표 32</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>물리적 환경</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보자산이 위치한 지역에 대해 인가된 자에 한하여 출입/접근할 수 있도록 관리해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{출입통제 시스템이 설치되지 않은 구역의 수}}{\text{전체 출입통제 구역의 개수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 특정 기준 설비의 설치율로 판단하는 것이 고려 필요.(이중화, CCTV, 통제구역의 출입문 수 등)</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>출입통제시스템 도입비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보자산이 위치한 지역에 대해 인가된 자에 한하여 출입/접근할 수 있도록 관리해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 출입통제시스템이 도입된 공공기관 수}}{\text{국가별 공공기관수}})\times 100$
$(\frac{\text{출입통제 시스템이 설치된 구역의 수}}{\text{전체 출입통제 구역의 개수}})\times 100$</td></tr>
<tr><td colspan="5">지표 33</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>물리적 환경</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보자산이 위치한 지역에 대해 인가된 자에 한하여 출입/접근할 수 있도록 관리해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{CCTV\text{가 설치되지 않은 구역의 수}}{\text{전체 출입통제 구역의 개수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 출입통제와 CCTV 관계가 대표성과는 무관
* 설문 항목 32번과 중복된다고 판단됨. 즉, 분모를 전체출입통제구역이라고 했는데, 앞에 지표란 뭐가 다른지? 아예, 조직 내에 물리적 보안은 CCTV 설치률을 평가하는 게 맞다고 판단됨</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 32번으로 대체</td></tr>
<tr><td colspan="5">지표 34</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>식별 및 인증</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">특정 등급 이상의 주요 정보 자산에 대해 사용자 및 시스템 인증 요구사항에 맞는 인증 및 암호화를 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{식별 및 인증이 이루어지는 자산의 수}}{\text{주요자산으로 분류된 자산의 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 통제목적에 언급된 주요 정보 자산에 대한 암호화 적용 여부가 반영되지 않음 이를 반영하거나 주요 정보 자산에 대한 암호화 지표가 추가되어야 함.
* 주요 자산으로 분류된 것이 식별된 것입니다.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>주요자산의 암호화비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">특정 등급 이사이의 주요 정보 자산에 대해 정보 노출을 방지하기 위하여 암호화를 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{암호화가 이루어지는 자산의 수}}{\text{조직의 주요자산으로 분류된 자산의 수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td colspan="5">지표 35</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>식별 및 인증</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">모든 시스템은 정보보호 정책에 따라 식별되고 인증되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{공유계정의개수}}{\text{전체사용자계정의개수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">*식별 및 인증을 제공하기 위해서는 전체 사용자 계정과 인증 성공/실패 횟수를 기반으로 지수화 하는 것이 더 나을 것 같습니다.
* 지수화에 있어 공유 계정 비율은 식별 및 인증과의 연관성이 떨어짐.
* 공유계정 외에도, 활성화 계정, 관리자 계정 등 여러 가지 유형의 계정에 대한 관리도 반영되어야 함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 계정관리 시스템이 설치되지 않은 경우, 데이터 수집이 어려울 것으로 판단</td></tr>
<tr><td colspan="5">지표 36</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>미디어 보호</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 미디어의 신뢰성 및 정보의 무결성 검증을 위해 조직이 정한 주기에 따라 백업 정보를 확인해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{백업정보의무결성점검횟수}}{\text{정보자산의백업수행횟수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 백업을 수행할 때마다 무결성 점검을 해야 한다면 맞는 지표이지만 일정한 주기에 따라 백업 정보를 확인해야 한다면 일정기간내 백업 정보의 무결성 점검 횟수를 확인해야 합니다.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 기본적으로 백업 시스템에서 백업 후 무결성 검사를 수행함.</td></tr>
<tr><td colspan="5">지표 37</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>미디어 보호</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">재사용을 위한 처리 및 배포 이전에 정보 시스템 미디어를 제거하거나 파괴해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{제거 절차 테스트를 통과한 미디어의 개수}}{\text{테스트를 거친 전체 미디어의 개수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 제거 절차 테스트를 통해 얻고자 하는 것이 ‘데이터의 완전 삭제 후 재사용 또는 저장매체의 폐기’ 라면, 본 지수화 방법론은 의미가 없음. 그 이유는, 본 지수로 얻을 수 있는 결론은 바꾸어 말하면,‘저장매체의 재활용 비율’이기 때문에, 이는 비용적인 측면과 연결되어 있는 것이지, 보안과 직결되는 내용이 아니기 때문.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외]</td></tr>
<tr><td colspan="5">지표 38</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>신기술 관리</td></tr>
<tr><td>평가지표</td><td>스마트폰 통제</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">업무 능률 개선을 위해 스마트워킹을 지원하는 경우, 스마트폰의 통제를 강화하여 정보자산에 대한 보안을 강화해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{스마트폰 보안통제 관련 예산}}{\text{스마트폰 활성화 지원 예산}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 스마트폰 활성화 지원예산보다는 조직의 IT전체 예산으로 산정하는 것이 효율적일 것 같음.
* 보안성 평가항목에 스마트폰 통제 항목 점수가 높다고 조직의 보안성이 높다고는 판단되지 않음
* 스마트폰도 인프라의 한 유형이므로, 좀 더 구체적인 지표화 필요.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 신기술 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 39</td></tr>
</table>

후보 지표(조직분야)				
수정전	평가분야	정보보호 기반	평가목적	신기술 관리
	평가지표	스마트폰 통제	지표성격	후행지표
	통제목적	조직 외부에서 조직 내부로 접속하는 사용자에 대한 기기 인증 및 사용자 인증은 물론, 암호화된 통신을 지원해야 한다.		
	지수화 방법론	$(\frac{\text{사용자 인증}(VPN)\text{을 통한 원격접근 이용자수}}{\text{전체 스마트폰을 이용한 원격접근 수}})\times 100$		
전문가의견	* 평가 항목과 비슷한 느낌이며, 사용자인증을 VPN으로 보기에는 어렵다고 판단됨. 요즘 대세가 조직 내에 DB에 접속하는 경우 이외에는 VPN 없이, 진짜 간략한 웹인증으로 접근하고 있음			
수정후	[제외] 구체적인 지수화를 위한 신기술 지표의 고도화 연구가 필요함			
지표 40				
수정전	평가분야	정보보호 기반	평가목적	신기술 관리
	평가지표	스마트폰 통제	지표성격	후행지표
	통제목적	조직 내부 정보의 유출을 방지하기 위하여 비인가된 스마트 폰의 내부 반입을 금지해야 한다.		
	지수화 방법론	$[1-(\frac{\text{비인가된 스마트폰 소지자수}}{\text{전체 스마트폰 이용자수}})]\times 100$		
전문가의견	* 스마트폰도 인프라의 한 유형이므로, 좀 더 구체적인 지표화 필요. * 비인가된 스마트폰 소지자의 수집이 불가할 것으로 보임. * 비인가된 스마트폰은 적발된 스마트폰을 의미하므로, 정확한 데이터 수집이 어려움			
수정후	[제외] 구체적인 지수화를 위한 신기술 지표의 고도화 연구가 필요함			
지표 41				

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>신기술 관리</td></tr>
<tr><td>평가지표</td><td>스마트 그리드 통제</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">스마트 그리드는 지속적인 전력 공급이 가능하도록 전력선 이중화나 우회 공급 경로를 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{조직 내의 전력 복구시간(분)}}{365\times1440})]\times100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 전력 복구률이 보안성하고 정확한 관계가 있는지 의문사항
* 전력을 복구해야 할 경우가 1년에 필요한 경우가 적을 수 있음
* 평가지표 - 통제목적 - 지수화 방법론 간의 관계가 불투명함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 신기술 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 42</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>개인정보보호</td></tr>
<tr><td>평가지표</td><td>개인정보보호</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">개인정보를 취급하는 조직은 개인정보 수집 및 이용시 그 사실을 고지하고 이용자의 동의를 얻어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\textit{OECD}\text{개인정보보호가이드라인을준수하는시스템의개수}}{\text{전체개인정를수집,처리,관리하는시스템의개수}})\times100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">개인정보를 취급하는 시스템의 개수를 카운트하는 게 적합한지? 지문과 같은 정보를 채취하는 것은 한정되어 있지만, 주민등록번호 등은 어느 시스템에서도 취급하는 게 가능하고, 사실, 개인정보를 가공, 저장, 유지하는 것은 단일 중앙 DB에서 처리하는 것으로 개인정보 안전성 평가를 위한 다른 벡터가 고려되어야 할 것 같음</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 43</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>개인정보보호</td></tr>
<tr><td>평가지표</td><td>개인정보보호</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">개인정보를 취급하는 조직은 개인정보 수집 및 이용시 그 사실을 고지하고 이용자의 동의를 얻어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{신고 및 적발 건수}}{\text{조직에 가입된 전체 회원수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 조직에 가입된 전체 회원 중, 통제목적에 따라 이용자 동의를 얻지 않은 회원이 가입되어 있는 것을 파악하기 위함이라면, 누가 신고를 할 것이며 누가 적발을 할 것인지 분명하지 않고, 약관 등의 이용자 동의 없이 회원 가입 절차가 이루어지는 조직은 거의 없으므로. 이 지수화 방법론에 따른 결과는 0 아니면, 100이 될 수밖에 없음</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 44</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보보호 수준을 높이기 위해서는 담당 업무의 직원, CEO, 일반 직원 모두가 정보보호의 중요성을 인식해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호가 중요하다고 인식하는 조직원의 수}}{\text{전체 조직원의 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 정보보호가 중요하다고 인식하는 조직원의 수는 문답 등의 설문을 통해 도출될 수 있는 객관성이 떨어지는 수치이므로, 이보다는 정보보호 관련 교육을 이수한 직원으로 변경하는 것이 나을 것으로 생각됨.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 45</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보보호 수준을 높이기 위해서는 담당 업무의 직원, CEO, 일반 직원 모두가 정보보호의 중요성을 인식해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간 일일보안점검 수행자의 수}}{\text{전체 조직원의 수} \times 365}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 전체 조직원이 1년 내 동일하지 않음. 매일 보안점검 수행자를 확인하기 위해서는 부하가 매우 큼 매달 또는 분기별 불시 보안점검을 수행하여 수행일 기준으로 보안점검 시 문제없는 확인하는 것이 명확함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 46</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 기본적인 보안 수준 확립을 위하여 모든 PC에 백신 프로그램을 설치해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{백신 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 단순한 백신 프로그램 설치 이외에 최신 버전으로 업데이트된 사항이 고려되어야 함.
* 매니지먼트 솔루션이 있을 경우 용이한 관리 가능.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>백신프로그램 설치비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 기본적인 보안 수준 확립을 위하여 모든 PC에 백신 프로그램을 설치해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{백신 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}}) \times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td colspan="5">지표 47</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 기본적인 보안 수준 확립을 위하여 신원 인증에 공인인증서를 이용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{공인인증서를 이용하는 조직원의 수}}{\text{전체 조직원의 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 조직에서 신원 인증에 공인인증서가 사용되는 경우는 크게 두 가지가 될 수 있음
1. 외부에서 VPN으로 내부망에 접근하는 경우
2. 내부 그룹웨어 이용 시, 인증서 사용 로그인 필수
본 지수화 방법론이 이용되려면, 상기 2번이 필수적인 전제조건이 되어야만 실효성을 가지기 때문에 범용적으로 적용되기 어려움</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 48</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 신속한 보안사고 대응을 위하여 조직원을 대상으로 보안 교육을 실시하여야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{해킹 및 바이러스 신고 건수}}{\text{전체 } PC\text{대수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 앞에서 언급된 스팸이나 취약점을 평가하는 항목들과 밀접한 관계가 있다고 판단됨
* 한 개의 PC에서 여러 번 사건이 발생하는 경우를 고려해야 함</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직 내의 신속한 보안사고 대응을 위하여 조직원을 대상으로 보안 교육을 실시하여야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{해킹 및 바이러스 신고 건수}}{\text{전체 } PC\text{대수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 49</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직원 및 고객의 개인 정보가 유출되지 않도록 적절한 조치를 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{개인정보침해신고건수}}{\text{전체조직원의수}}) \times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 1인당 1회의 신고를 하는 것은 아님
(국가정보보호지수, 국가 부분의 지표로 표준화 추진)</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 조직원 및 고객의 개인 정보가 유출되지 않도록 적절한 조치를 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{개인정보침해신고건수}}{\text{전체조직원의수}}) \times 100$</td></tr>
<tr><td colspan="5">지표 50</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 정보보호 업무만을 전담하는 정보보호 전문인력을 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호 전문인력의수}}{\text{정보통신 인력의수}}) \times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">* 조직의 정보보호 전문인력을 지수화하기 위해서는 정보통신 인력 수 대비보다는 조직의 인원 수 대비로 지수화 하는 것이 더 나을 것 같습니다.
* 전체 인원수 이외에 예산 및 규모, 실제로 업무에서 다루고 있는 자산 등도 고려하는 좋다고 판단됨</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>정보보호전문 인력비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 신속하고 효율적인 정보보호 업무 처리를 위해 정보보호 업무만을 전담하는 정보보호 전담 인력을 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호 전담 인력의 수}}{\text{전체 조직원의 수}})\times 100$</td></tr>
<tr><td colspan="5">지표 51</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 스팸 메일 수신 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{1계정당 수신되는 스팸메일 수}}{\text{1계정당 수신되는 전체 전자메일 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 1 계정당 수신되는 메일로 하게 되면, 이는 조직원의 메일을 확인할 수 있다는 것으로 프라이버시 침해 여지가 있음. 따라서 1계정이 아닌, 조직 전체의 것을 판단하는 것이 맞을 것으로 생각됨.
(국가정보보호지수, 국가 부분의 지표로 표준화 추진)</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 스팸 메일 수신 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{1계정당 수신되는 스팸메일 수}}{\text{1계정당 수신되는 전체 전자메일 수}})\times 100$</td></tr>
<tr><td colspan="5">지표 52</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 피싱사고 발생 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{조직 내의 피싱사고 발생 건수}}{\text{전체 피싱사고 발생 건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 전체피싱사고 발생건수의 출처를 명확히 제시해야함 예를들면, KISA에서 발표하는 연간 침해사고통계 건수 등을 활용 가능
* 국가를 대상으로할 경우, 데이터 수집을 담당하는 기관 필요 ex)apwg.org</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 데이터 수집 기관의 선정 문제</td></tr>
<tr><td colspan="5">지표 53</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 봇넷 감염 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{봇넷에 감염된 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 봇넷은 침해 피해 PC에 대한 대표 사례라고 볼 수는 있지만, 이렇게 개별적으로 평가하기 보다는 기준에 따라 통합하는 게 필요
* 국가를 대상으로할 경우, 데이터 수집을 담당하는 기관 필요 ex)shadowserver.org
[제외] 데이터 수집 기관의 선정 문제</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보화 역기능 수준</td></tr>
<tr><td>평가지표</td><td>봇넷 감염비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 정보자산을 유출을 가능성을 평가하기 위해 봇넷 감염비율을 측정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{봇넷에 감염된 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$</td></tr>
<tr><td colspan="5">지표 54</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 DDoS 공격 발생 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{서비스거부공격 발생일수}}{365})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 보안 관련 개별 벡터로 평가하기 보다는 통합하는 게 필요하고, 사실 DDoS를 평가할 때, 분명 일수도 중요하지만 피해 규모가 더 고려되어야 한다고 판단됨
* 해당 서비스거부공격에 대한 지표가 좋게 나올 경우 준비를 잘 해서 일 수도 있지만 주요 조직이 아니라서 공격시도가 없는 경우가 있을 수 있음
* 서비스 거부공격이 일 단위로 발생할 수 있지만, 짧은 시간에 종료되는 경우도 있기 때문에, 지수화 방법론의 데이터를 '시간'으로 바꾸면 좋을 것 같음
* 국가를 대상으로할 경우, 데이터 수집을 담당하는 기관 필요 ex)shadowserver.org
[제외] 데이터 수집 기관의 선정 문제</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보화 역기능 수준</td></tr>
<tr><td>평가지표</td><td>DDoS 피해 발생비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직이 제공하는 서비스의 중단을 발생시키는 서비스 거부 공격에 대한 대응 능력을 평가하기 위해 공격으로 인한 실제 서비스 중지시간을 측정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{실제서비스중지시간}}{\text{서비스거부공격발생시간}})\times 100$</td></tr>
<tr><td colspan="5">지표 55</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인식 및 훈련</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간보안교육을이수한보안인력의수}}{\text{전체보안인력의수}})\times 100$</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">-</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>보안인력의 교육비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간 보안교육을 이수한 보안인력의 수}}{\text{전체 보안인력의 수}})\times 100$</td></tr>
<tr><td colspan="5">지표 56</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인식 및 훈련</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국제 정보보호 자격증을 취득한 보안 인력의 수}}{\text{전체 보안 인력의 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 국제 정보보호 자격증이 객관화된 수치라고 할 수 있지만, 자격증을 가진 인원이 많다고 안전하다고 판단되지는 않음
* 보안자격증 취득 여부를 가지고 적절히 훈련되었다고 보기 힘듬. 또한, 국내에 도입된 국제정보보호 자격의 경우 대부분의 자격들이 학원만 다니면 단순 암기식으로 획득할 수 있으므로 실효성이 떨어짐</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>국제정보보호자격증 취득 비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호 자격증을 취득한 보안 인력의 수}}{\text{전체 보안 인력의 수}})\times 100$</td></tr>
<tr><td colspan="5">지표 57</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(조직분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인적 보안</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">조직은 각 조직원이 직위와 책임에 부합하는 보안 기준을 만족하는지 확인해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{신원조사를 마친 조직원의 수}}{\text{정보자산에 접근 가능한 조직원의 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 대부분 신규채용 시, 신원조사를 하게 되어 있을 것으로 판단되므로, 외부인력에 대한 항목으로 변경하는 방안 검토 필요
* 신원조사는 공공기관의 취업 또는 공공업무를 담당할 시 경찰청을 통해 수행하는 것이므로, 민간기업에 본 방법론을 적용하기에는 적절하지 않을 것으로 보임</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 58번 문항로 대체</td></tr>
<tr><td colspan="5">지표 58</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인적 보안</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">적격심사를 통과한 조직원의 경우라도 주요 자산에 대한 철저한 관리가 지속되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{보안 문제를 야기한 조직원의 수}}{\text{적격심사를 통과한 조직원의 수}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">보안문제를 야기했다고 해서 문제를 일부러 발생시킨 것이 아닌 실수인 경우가 있음. 때문에 문제를 일으킨 비율보다는 적격심사를 통과한 조직원 중 정보보호 교육 이수율을 확인하는 것이 좋음</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인적 보안</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">적격심사를 통과한 조직원의 경우라도 주요 자산에 대한 철저한 관리가 지속되어야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$[1-(\frac{\text{보안 문제를 야기한 조직원의 수}}{\text{적격심사를 통과한 조직원의 수}})]\times 100$</td></tr>
</table>

<table>
<tr><th colspan="6">후보 지표(조직분야)</th></tr>
<tr><td colspan="6">지표 59</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td colspan="2">정보보호 예산</td></tr>
<tr><td>평가지표</td><td>보안 예산</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">기업 정보 및 정보 시스템을 보호하기 위해 필요한 예산을 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{조직의 정보보호 예산}}{\text{조직의 전체 정보화 예산}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">-</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td colspan="2">정보보호 예산</td></tr>
<tr><td>평가지표</td><td>보안 예산 비율</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">기업 정보 및 정보 시스템을 보호하기 위해 필요한 예산을 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{조직의 정보보호 예산}}{\text{조직의 전체 정보화 예산}})\times 100$</td></tr>
<tr><td colspan="6">지표 60</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td colspan="2">정보보호 예산</td></tr>
<tr><td>평가지표</td><td>보안 예산</td><td>지표성격</td><td colspan="2">후행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">기업 정보 및 정보 시스템을 보호하기 위해 필요한 예산을 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$[1-(\frac{\text{역기능으로 인한 처리비용}}{\text{조직의 정보보호예산}})]\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 역기능으로 인한 처리 비용이 조직의 정보보호예산 안에서 모두 처리되지는 않음</td></tr>
</table>

후보 지표(조직분야)	
수정후	[제외] 59번 문항으로 대체

[표 11] 국가분야의 후보지표

후보 지표(국가분야)				
지표 1				
수정전	평가분야	정보보호 구현	평가목적	정보보호 위험 제거
	평가지표	취약점 관리	지표성격	후행지표
	통제목적	국가의 전반적인 보안 수준 향상을 위하여 최신 OS 패치를 설치하여야 한다.		
	지수화 방법론	$(\frac{\text{국가별 주요 } OS \text{ 취약점 패치 완료 건수의 합}}{\text{연간 발표된 주요 } OS \text{ 취약점 개수}}) \times 100$		
전문가의견	* (국가차원에서 조치 권고한 주요 취약점 개수/연간발표된 주요 OS 취약점 개수) * 국가별 주요 OS 취약점 패치 완료 건수의 합을 어떻게 구할 수 있는지?			
수정후	[제외] MS의 경우, OS별 패치율을 공개하고 있으나 다른 OS의 패치율도 고려해야 함.			
지표 2				
수정전	평가분야	정보보호 구현	평가목적	정보보호 위험 제거
	평가지표	유지 관리	지표성격	선행지표
	통제목적	해킹 사고의 국제적 대응을 위해 국제 차원이 해킹 대응 훈련에 참가하여 정보교류 및 상호협력을 맺고 있어야 한다.		
	지수화 방법론	$(\frac{\text{국제 보안 관련 컨퍼런스 참여 횟수}}{\text{최근 3년간 국제 보안 관련 컨퍼런스 개최 횟수}}) \times 100$		

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td>전문가의견</td><td colspan="4">*소규모 조직 및 기관에서는 국제보안관련 컨퍼런스 참석이 어려울 것으로 판단.(예산 및 인력 부족 등)
교육 지수 평가를 위해 필요한 항목이나 평가 벡터가 되는 컨퍼런스 선정에 대한 기준이 필요함
* (해당 국가의 국제 보안 관련 컨퍼런스 개최 횟수 / 전체 국제 보안 관련 컨퍼런스 개최 횟수)
* 참여한 횟수를 확인하면 인원이 나오기 때문에 최근3년간 참여한 국제 보안관련 컨퍼런스 횟수 / 최근 3년간 개최된 국제 보안관련 컨퍼런스 횟수 x 100
* 교육관련된 지표로 되어야 할 것으로 생각됨.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 19번, 20번 항목과 유사</td></tr>
<tr><td colspan="5">지표 3</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 구현</td><td>평가목적</td><td>침해사고 대응</td></tr>
<tr><td>평가지표</td><td>사건 보고</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가 차원의 신속한 보안사고 대응을 위하여 국민을 대상으로 보안 교육을 실시하여야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{연간 해킹 및 바이러스 신고 건수}}{\text{인구수}}) \times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 통제 목적은‘보안 교육’에 중점을 두고 있지만 지수화 방법론에서는‘연간 해킹 및 바이러스 신고 건수’를 다루고 있다. 이 부분에서는 연간 보안 교육 횟수에 대해서 지수화 시켜주면 더욱 효율적일 것 같다고 사료됨
* 연간 해킹 및 바이러스 발생건수는 신고+사전 및 자체조사의 형태로 이루어지므로, 분모를 인구수 보다는 ‘연간 해킹 및 바이러스 발생건수’로 하는 방안도 고려해 볼 수 있음</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 4</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 보유</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보통신망의 안전성 및 정보통신설비 보호를 위해 정보보호시스템을 설치/운영함으로써 네트워크 보안을 강화한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호 시스템의 개수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 지수 방법론에서 개별 PC에서 방확벽도 존재하고 있으며, 조직 내에 여러 개의 시스템이 존재할 수 있는데, 지금 지수로는 평가가 안될 것 같음
* 전국 정보보호시스템의 개수를 산정하는 것에는 무리수가 따르므로, 주요 IPS 업체가 보유한 시스템의 개수를 분모로 한다면 데이터를 산출하는데 더욱 효율적이고, 지표로서의 역할도 가능할 것으로 보임</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 5</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 시스템 보유</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">주요개인정보 전송시 비밀성과 무결성을 보장하는 보안서버구축 등의 조치를 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{보안서버의 수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">(국가망 보안서버 수 / 국가망 전체 시스템 수) 인구수는 적절치 않음
보안서버의 수 / 웹서버의 수</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 6</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>시스템 및 통신 보안</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">카드 거래 정보를 처리, 저장, 전송하는 가맹점 및 서비스 제공자는 데이터보안표준(PCI DSS)를 만족해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{PCIDSS\text{를 준수하는 가맹점 수}}{\text{국가별 가맹점 수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* PCIDSS가 더 활성화될 경우 도입 고려.
* 모든 가맹점이 PCIDSS를 준수해야 하는것음 아님, 우리나라의 경우 금감위에서 ‘전자금융업 등록 및 말소 현황’을 공개하고 있는데, 이를 활용하던지 해서 국가별 가맹점수의 범위를 명확히 하는 것이 필요함</td></tr>
<tr><td>수정후</td><td colspan="4">[제외]</td></tr>
<tr><td colspan="5">지표 7</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>접근 통제</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보 자산 및 정보 시스템을 보호/감시하기 위해 보안통제를 수행해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 공공기관 } CCTV\text{설치 대수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 공공기관과 인구수로 지수화하기에는 부족함.
* 정보자산 및 정보시스템에 대한 보호/감시를 위한 통제이므로, 각 기관별 특정 기준의 물리적 보안이 되어 있는지에 대한 여부로 판단하는 방안도 검토 필요.
* CCTV는 의무가 아닌 권고사항임 ※ 분모를 ‘공공기관이 설치한 CCTV 대수’로 하면 좀 더 명확할 의미가 될 것으로 판단됨</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>보안 관리</td></tr>
<tr><td>평가지표</td><td>출입통제시스템 도입비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 정보 자산 및 정보 시스템을 보호/감시하기 위해 보안통제를 주요 기관에 적용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 출입통제시스템이 도입된 공공기관 수}}{\text{국가별 공공기관수}})\times 100$</td></tr>
<tr><td colspan="5">지표 8</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 관리시스템 인증비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">기업들의 정보보호 관리체계 인증 현황을 파악하여 전반적인 국가의 정보보호 관리시스템 도입 현황을 파악한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 } ISO\,27001 \text{ 인증 건수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* ISO 27001은 정보보호관리체계의 국제 표준 규격이긴 하지만 국가 간 상호인정이 안 되어 있으므로 비교할 수 있는 지표는 아님. ISMS 관련 인증을 받은 기업 수 / 정보 처리 업무를 포함하는 기업 수 ISMS 관련 인증 : KISA의 ISMS, PIMS, G-ISMS, ISO/IEC 27001 등</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td>정보보호 시스템 도입</td></tr>
<tr><td>평가지표</td><td>정보보호 관리시스템 인증비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 조직이 구축한 ISMS에 대해 인증 현황을 파악하여 전반적인 국가의 ISMS의 관리 수준을 측정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 } ISMS \text{ 인증을 받은 기업 수}}{\text{국가별 전체 } IT\text{기업 수}})\times 100$</td></tr>
<tr><td colspan="5">지표 9</td></tr>
</table>

<table>
<tr><th colspan="6">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td colspan="2">정보보호 수준지수</td></tr>
<tr><td>평가지표</td><td>백신 보급률</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">국가는 안전한 인터넷 사용을 위하여 백신 프로그램 설치를 장려해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{백신프로그램이용자수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 국가차원의 조사가 가능한지
* 국가정보보지수의 방법론과 동일하지만, internetworldstats.com의 인구수 대신 인터넷 이용자수를 활용할 수 있음</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 기반(S/P)</td><td>평가목적</td><td colspan="2">정보보호 수준지수</td></tr>
<tr><td>평가지표</td><td>백신 보급률</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">국가는 안전한 인터넷 사용을 위하여 백신 프로그램 설치를 장려해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{백신프로그램이용자수}}{\text{인터넷이용자수}})\times 100$</td></tr>
<tr><td colspan="6">지표 10</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">정보보호 수준지수</td></tr>
<tr><td>평가지표</td><td>PKI 보급률</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">국가는 기본적인 보안 수준 확립을 위하여 신원 인증에 공인인증서를 이용해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{\text{공인인증서이용자수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 공인인증서 외에도 개인 정보 식별을 대처하는 I-PIN등 다른 방안도 고려 필요.
* 국가정보보지수의 방법론과 동일하지만, internetworldstats.com의 인구수 대신 인터넷 이용자수를 활용할 수 있음</td></tr>
<tr><td>수정후</td><td colspan="5">[제외] 국가정보보지수의 PKI 보급률 지수로 표준화 추진</td></tr>
</table>

<table>
<tr><th colspan="6">후보 지표(국가분야)</th></tr>
<tr><td colspan="6">지표 11</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">신기술 관리</td></tr>
<tr><td>평가지표</td><td>스마트그리드 통제</td><td>지표성격</td><td colspan="2">후행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">스마트 그리드는 지속적인 전력 공급이 가능하도록 전력선 이중화나 우회 공급 경로를 확보해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$[1-(\frac{\text{국가별 정전 복구시간(분)}}{365\times1440})\times100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 국가 차원에서 전력 복구는 중요한 벡터라고 판단되지만, 실제 복구 시간을 어떤 기준으로 산정할지 의문?
* 스마트그리드와 국가별 정전 복구시간은 관계가 없는 것으로 판단됩니다.</td></tr>
<tr><td>수정후</td><td colspan="5">[제외] 구체적인 지수화를 위한 신기술 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="6">지표 12</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 기반</td><td>평가목적</td><td colspan="2">개인정보보호</td></tr>
<tr><td>평가지표</td><td>개인정보보호</td><td>지표성격</td><td colspan="2">선행지표</td></tr>
<tr><td>통제목적</td><td colspan="4">개인정보의 유출에 대비하여 각 나라가 합의한 OECD의 통일된 개인정보보호지침을 준수해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="4">$(\frac{OECD\text{개인정보보호준수한기관수}}{\text{전체기업및공공기관수}})\times100$</td></tr>
<tr><td>전문가의견</td><td colspan="5">* 개인정보영향평가, G-ISMS 등 개인정보에 대한 통제 분야가 있는 인증을 받은 기관의 수 등을 고려해도 좋을 거 같음.
* 사용자들의 보안 인식분야와 관련되는 지표라고 판단됨</td></tr>
<tr><td>수정후</td><td colspan="5">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="6">지표 13</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 국민의 개인 정보가 유출되지 않도록 적절한 조치를 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{개인정보침해신고건수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 개인정보침해에 대한 기준 필요</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>개인정보보호</td></tr>
<tr><td>평가지표</td><td>개인정보침해 신고비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 인터넷에서의 개인정보침해 사고에 대응하기 위하여 개인정보침해 센터를 운영하고, 적절한 조치를 취해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{개인정보침해신고건수}}{\text{국가별인터넷사용자수}})\times 10000$</td></tr>
<tr><td colspan="5">지표 14</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">사회전반으로 정보화 역기능 심각한 수준에 이르고 있어 국민의 보안의식을 파악할 수 있는 지표가 필요하다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호가중요하다고인식하는이용자수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 국가별 인원이 많은 만큼 파악하기 어려울 것 같습니다. 설문을 통한다면 가능하나 중요하다는 인식도 파악해야 하나 정보보호 관련 정보에 대해 얼마나 알고 있는가의 파악도 필요할 것 같습니다.</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td colspan="5">지표 15</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 피싱사고 발생 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 피싱 사고 발생 건수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 피싱 사건으로 카운트할 수 있는 규모 산출이 필요</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 16</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 봇넷 감염 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 봇넷 감염 건수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 대부분이 1인/1PC를 기준으로 하는 것 같음. 또한, 실제 봇넷 감염 수치를 전 국민을 대상으로 카운트가 가능한지?</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 17</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 스팸 메일 수신 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 스팸 메일 발생 건수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 스팸메일수신은 이용자의 정보보호 의지와 상관없이(물론 스팸필터링시스템 설치여부에 따라 최종 이용자에게 수신여부는 다르지만) 국내 및 해외에서 발송될 수 있기 때문에 각 국가에서 스팸발송건수를 지표로 하는것이 각 국가의 정보보호수준을 측정하는 것이 될 것으로 생각함(예: 좀비PC가 많으면 스팸발송국 순위가 올라갈것이고, 적으면 순위로 떨어질것임)</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 국가정보보호지수 항목으로 표준화 추진</td></tr>
<tr><td colspan="5">지표 18</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>보안의식 수준</td></tr>
<tr><td>평가지표</td><td>정보화 역기능 수준</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보화 역기능 수준을 측정하기 위해 국가별 DDoS 발생 비율을 이용한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국가별 } DDoS \text{ 발생 건수}}{\text{전세계 } DDoS \text{ 발생 건수}})\times 100$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 정확한 카운트 수치 확보가 가능한 항목인지?
* 각 국가의 ISP내의 라우터에 Agent를 설치하여 데이터를 수집하는 shadowserver.org의 데이터를 활용할 수 있을 것임</td></tr>
<tr><td>수정후</td><td colspan="4">[제외] 구체적인 지수화를 위한 지표의 고도화 연구가 필요함</td></tr>
<tr><td colspan="5">지표 19</td></tr>
</table>

<table>
<tr><th colspan="5">후보 지표(국가분야)</th></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인식 및 훈련</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 정보보호 인력 양성을 위하여 전문 교육기관에 투자를 해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호관련교육기관수}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 교육기관의 수 보다는 정보보호 교육에 참여하는 참여인력이 고려되야 함.
* 정보보호 관련 학과 및 민간 교육 기관 등을 포함시키면 좋을 것 같습니다.</td></tr>
<tr><td rowspan="4">수정후</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준</td></tr>
<tr><td>평가지표</td><td>정보보호 교육기관 설립 비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가는 정보보호 인력 양성을 위하여 정보보호 전문기관을 설립해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{정보보호과정과목이개설된교육기관수}}{\textit{IT}\text{관련교육기관수}})\times 100$</td></tr>
<tr><td colspan="5">지표 20</td></tr>
<tr><td rowspan="4">수정전</td><td>평가분야</td><td>정보보호 환경</td><td>평가목적</td><td>정보보호 교육</td></tr>
<tr><td>평가지표</td><td>인식 및 훈련</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">국가 및 조직은 정보보호 정책수립 및 이행을 위한 전문인력을 보유해야 한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{국제정보보호자격증을취득한정보보호인력}}{\text{인구수}})\times 1000000$</td></tr>
<tr><td>전문가의견</td><td colspan="4">* 전문인력의 기준을 자격증으로 한정하는 것보다, 경력 및 교육 등도 고려 필요.</td></tr>
</table>

후보 지표(국가분야)				
수정후	평가분야	정보보호 환경(P)	평가목적	정보보호 수준
	평가지표	정보보호전문 인력비율	지표성격	후행지표
	통제목적	국가 및 조직은 정보보호 정책수립 및 이행을 위한 전문인력을 보유해야 한다.		
	지수화 방법론	$(\frac{\text{정보보호 자격증을 취득한 정보보호 인력 수}}{\text{국가별 } IT\text{관련 인력 수}}) \times 100000$		
지표 21				
수정전	평가분야	정보보호 환경	평가목적	정보보호 예산
	평가지표	보안 예산	지표성격	선행지표
	통제목적	국가의 정보화 예산 중 정보보호 분야에 대한 예산이 얼마로 책정되어 집행되고 있는지를 확인한다.		
	지수화 방법론	$(\frac{\text{정보보호 관련 국가예산}}{\text{인구수}}) \times 1000000$		
전문가의견	* 분모에 인구수가 아닌, 연간 총 예산 대비 보안 예산으로 평가해야 됨			
수정후	평가분야	정보보호 환경(P)	평가목적	정보보호 예산
	평가지표	보안 예산비율	지표성격	선행지표
	통제목적	국가의 정보화 예산 중 정보보호 분야에 대한 예상이 얼마로 책정되어 집행되고 있는지를 확인한다.		
	지수화 방법론	$(\frac{\text{정보보호 관련 국가예산}}{\text{국가 전체 예산}}) \times 100$		

[표 12] 국가분야 후보 지표에 포함시킨 국가정보보호지수

후보 지표(국가분야-국가정보보호지수)
지표 1

후보 지표(국가분야-국가정보보호지수)				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	백신 보급률	지표성격	선행지표
	통제목적	정보보호 기반수준은 정보보호 노력의 정도를 측정하는 지표로서 개인의 정보보호 기반수준을 측정하기 위해 백신 보급률, 패치 보급률, PKI 보급률을 측정한다.		
	지수화 방법론	$(\frac{\text{백신프로그램이용자수}}{\text{인터넷이용자수}})\times 100$		
지표 2				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	패치 보급률	지표성격	선행지표
	통제목적	정보보호 기반수준은 정보보호 노력의 정도를 측정하는 지표로서 개인의 정보보호 기반수준을 측정하기 위해 백신 보급률, 패치 보급률, PKI 보급률을 측정한다.		
	지수화 방법론	$(\frac{\text{패치설치수}}{\text{인터넷이용자수}})\times 100$		
지표 3				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	PKI 보급률	지표성격	선행지표
	통제목적	정보보호 기반수준은 정보보호 노력의 정도를 측정하는 지표로서 개인의 정보보호 기반수준을 측정하기 위해 백신 보급률, 패치 보급률, PKI 보급률을 측정한다.		
	지수화 방법론	$(\frac{\text{공인인증서이용자수}}{\text{인터넷이용자수}})\times 100$		
지표 4				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	Firewall 보급률	지표성격	선행지표
	통제목적	기업의 정보보호 기반수준을 측정하기위해 Firewall 보급률, IDS 보급률, 보안서버 보급률을 측정한다.		
	지수화 방법론	$(\frac{\textit{Firewall}\text{을사용하는기업체수}}{\text{기업체수}})\times 100$		

후보 지표(국가분야-국가정보보호지수)				
지표 5				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	IDS 보급률	지표성격	선행지표
	통제목적	기업의 정보보호 기반수준을 측정하기위해 Firewall 보급률, IDS 보급률, 보안서버 보급률을 측정한다.		
	지수화 방법론	$(\frac{IDS를\ 사용하는\ 기업체수}{기업체수})\times 100$		
지표 6				
국가정보보호지수	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	보안서버 보급률	지표성격	선행지표
	통제목적	기업의 정보보호 기반수준을 측정하기위해 Firewall 보급률, IDS 보급률, 보안서버 보급률을 측정한다.		
	지수화 방법론	$(\frac{국내\ 보안서버\ 판매대수}{인구수})\times 100000$		
지표 7				
국가정보보호지수	평가분야	정보보호 환경(P)	평가목적	정보보호 수준지수
	평가지표	정보보호 관련 예산 비율	지표성격	선행지표
	통제목적	정보보호환경수준은 정보보호예산비율, 전문인력, 국민의 정보보호의식수준을 측정한다.		
	지수화 방법론	$(\frac{정보보호\ 관련\ 국가예산}{정보화관련\ 국가예산})\times 100$		
지표 8				
국가정보보호지수	평가분야	정보보호 환경(P)	평가목적	정보보호 수준지수
	평가지표	정보보호 전문인력 비율	지표성격	선행지표
	통제목적	정보보호환경수준은 정보보호예산비율, 전문인력, 국민의 정보보호의식수준을 측정한다.		
	지수화 방법론	$(\frac{정보보호\ 전문인력}{정보화\ 전문인력})\times 100$		
지표 9				

<table>
<tr><th colspan="5">후보 지표(국가분야-국가정보보호지수)</th></tr>
<tr><td rowspan="4">국가정보보호지수</td><td>평가분야</td><td>정보보호 환경(P)</td><td>평가목적</td><td>정보보호 수준지수</td></tr>
<tr><td>평가지표</td><td>국민의 보안의식 수준비율</td><td>지표성격</td><td>선행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보보호환경수준은 정보보호예산비율, 전문인력, 국민의 정보보호의식수준을 측정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{5점 척도 필요 또는 매우 필요 응답자}}{\text{전제조사 대상자}})\times 100$</td></tr>
<tr><td colspan="5">지표 10</td></tr>
<tr><td rowspan="4">국가정보보호지수</td><td>평가분야</td><td>정보화역기능</td><td>평가목적</td><td>정보화 역기능 수준지수</td></tr>
<tr><td>평가지표</td><td>해킹·바이러스 신고비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보보호 역기능 수준은 해킹·바이러스 신고비율, 개인정보 침해 신고비율, 스팸메일 수신비율 등을 집계하여 추정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{해킹·바이러스 신고건수}}{\text{전체 } PC\text{보급대수}})\times 100$</td></tr>
<tr><td colspan="5">지표 11</td></tr>
<tr><td rowspan="4">국가정보보호지수</td><td>평가분야</td><td>정보화역기능</td><td>평가목적</td><td>정보화 역기능 수준지수</td></tr>
<tr><td>평가지표</td><td>개인정보 침해 신고비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보보호 역기능 수준은 해킹·바이러스 신고비율, 개인정보 침해 신고비율, 스팸메일 수신비율 등을 집계하여 추정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{개인정보침해 신고건수}}{\text{인터넷사용인구}})\times 100$</td></tr>
<tr><td colspan="5">지표 12</td></tr>
<tr><td rowspan="4">국가정보보호지수</td><td>평가분야</td><td>정보화역기능</td><td>평가목적</td><td>정보화 역기능 수준지수</td></tr>
<tr><td>평가지표</td><td>스팸메일 수신비율</td><td>지표성격</td><td>후행지표</td></tr>
<tr><td>통제목적</td><td colspan="3">정보보호 역기능 수준은 해킹·바이러스 신고비율, 개인정보 침해 신고비율, 스팸메일 수신비율 등을 집계하여 추정한다.</td></tr>
<tr><td>지수화 방법론</td><td colspan="3">$(\frac{\text{1계정당 수신되는 스팸메일 수}}{\text{1계정당 수신되는 전체 전자메일수}})\times 100$</td></tr>
</table>

제 4 절 사이버보안지수 2차 Draft 최종 지표 제안

현재 사이버보안지수 표준화는 조직 부분에 대해서만 표준화가 이루어지고 있으며, 조직의 보안 수준을 측정하는 지표와 지수화 방법론에 대한 내용을 담고 있다.

개발된 조직 지표를 ITU-T SG17 회의(12월 8일~17일, 스위스 제네바)에서 CSI development process의 Indicators for cybersecurity index에 추가되었다. 일부 지표가 조직에 적용하기 어려운 지표로 지적되었으나 조직에서 필요하지 않은 지표는 제외가 가능하다는 답변을 통하여 반대 없이 통과되었다. 이번 회의까지 X.csi 기고서는 Measurement implementiation, Methodolgy for Cybersecurity Index 항목을 제외한 부분의 내용이 합의가 되었다.

[그림 42] X.csi 목차

Scope 항목부터 Conventions 항목은 ITU 표준 문서 양식이고, 사이버보안지수에 대한

부분은 Cybersecurity index항목부터 Methodolgy for Cybersecurity Index 항목까지이다. 이 항목들에 대한 설명은 아래와 같다.

o Cybersecurity index: 사이버보안지수를 위한 일반적인 요구사항과 사이버보안지수 지표를 위한 요구사항 그리고 지표의 등급에 대한 설명이 포함되어 있다.

o CSI development process: 사이버보안지수의 지표 개발 단계를 설명하고 있으며, 사이버보안지수 지표를 포함할 예정이다.

o Annex A: Example of information security index and metrics: 이 항목에는 현재 국가정보보호지수의 지표와 함께 NIST의 SP 800-55 rev.1의 지표가 정보보호 지표의 예로 포함이 되어 있다.

[표 13] 표준에 제안된 후보 지표 (조직)

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
1	평가분야	정보보호 구현(P)	평가목적	위험 제거
	평가지표	취약점 조치비율	지표성격	후행지표
	통제목적	조직은 식별된 취약점들을 적시에 제거해야 한다.		
	지수화 방법론	$(\frac{\text{완화된 취약점의 개수}}{\text{식별된 취약점의 개수}})\times 100$		
2	평가분야	정보보호 구현(S)	평가목적	위험 제거
	평가지표	사고	지표성격	선행지표
	통제목적	조직은 부적절한 행동을 하는 사용자를 조사하기 위해 시스템 감사 로그를 유지해야 한다.		
	지수화 방법론	$(\frac{\text{감사로깅을 하는 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$		
3	평가분야	정보보호 구현(S)	평가목적	위험 제거
	평가지표	최신패치 설치비율	지표성격	선행지표
	통제목적	사용자 PC의 취약점을 완화하기 위하여, PC에는 보안 패치 프로그램이 설치되어야 한다.		

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
	지수화 방법론	$(\frac{\text{보안 패치 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$		
4	평가분야	정보보호 구현(S/P)	평가목적	침해사고 대응
	평가지표	보안사고 대응비율	지표성격	후행지표
	통제목적	조직은 모든 사고 분야의 보안사고를 적시에 보고해야 한다.		
	지수화 방법론	$(\frac{\text{적시에 보고된 사고의 수}}{\text{전체 보고된 사고의 수}})\times 100$		
5	평가분야	정보보호 기반(S)	평가목적	보안 관리
	평가지표	백신프로그램 설치비율	지표성격	선행지표
	통제목적	사용자 PC의 바이러스 감염을 줄이기 위해 PC에는 안티바이러스 프로그램이 설치되어야 한다.		
	지수화 방법론	$(\frac{\text{안티 바이러스 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}})\times 100$		
6	평가분야	정보보호 구현(S)	평가목적	보안관리
	평가지표	긴급복구계획 테스트비율	지표성격	선행지표
	통제목적	정보 시스템은 긴급복구계획 테스트를 수행해야 한다.		
	지수화 방법론	$(\frac{\text{연간긴급사태계획테스트수행대상시스템의 개수}}{\text{정보자산에 등록된 시스템의 개수}})\times 100$		
7	평가분야	정보보호 환경(P)	평가목적	보안관리
	평가지표	보안평가 승인비율	지표성격	후행지표
	통제목적	조직의 정보 시스템은 도입 이전에 증명 및 승인되어야 한다.		
	지수화 방법론	$(\frac{CA\text{받은 신규 시스템의 개수}}{\text{전체 신규 시스템의 개수}})\times 100$		
8	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	보안서약 비율	지표성격	선행지표
	통제목적	정보 시스템에 접근이 허가된 조직원은 조직의 정보 시스템에 접근 이전에 보안 서약을 해야 한다.		

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
	지수화 방법론	$(\frac{\text{행동규칙에서명후시스템에접근하는이용자수}}{\text{정보시스템에허가된이용자수}})\times 100$		
9	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	원격접근 통제 비율	지표성격	선행지표
	통제목적	조직은 조직의 내부 정보 자산을 보호하기 위하여 보호된 원격 접근을 제공하기 위한 방화벽이나 웹 방화벽을 설치해야 한다.		
	지수화 방법론	$(\frac{\text{방화벽 or 웹방화벽을이용하는원격접근포인트의수}}{\text{원격접근포인트의수}})\times 100$		
10	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	원격접근 통제비율	지표성격	선행지표
	통제목적	조직은 조직의 내부 자산을 보호하기 위하여 보호된 원격 접근을 제공하기 위한 IDS나 IPS를 설치해야 한다.		
	지수화 방법론	$(\frac{IDS \text{ or } IPS\text{를이용하는원격접근포인트의수}}{\text{원격접근포인트의수}})\times 100$		
11	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	보호된 무선AP비율	지표성격	선행지표
	통제목적	조직은 비인가 접근으로부터 내부 네트워크를 보호하기 위하여 보호된 무선 AP를 제공해야 한다.		
	지수화 방법론	$(\frac{\text{보안이설정된무선엑세스포인트개수}}{\text{조직내의전체무선엑세스포인트개수}})\times 100$		
12	평가분야	정보보호 구현(S)	평가목적	보안 관리
	평가지표	네트워크 이중화 비율	지표성격	선행지표
	통제목적	조직은 조직의 서비스에 대한 가용성과 연속성을 보장하기 위하여 주요 네트워크에 대한 이중화 링크를 구성해야 한다.		
	지수화 방법론	$(\frac{\text{이중화된링크수}}{\text{전체네트워크장비의대수}})\times 100$		
13	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	인사 보안 심사 비율	지표성격	선행지표
	통제목적	조직은 정보 및 정보 시스템에 인가된 사용자의 접속만을 허가해야 한다.		

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
	지수화 방법론	$(\frac{\text{신원조사를 마친 사용자 수}}{\text{전체 접근자 수}})\times 100$		
14	평가분야	정보보호 기반(S/P)	평가목적	개인정보보호
	평가지표	개인식별정보 보호비율	지표성격	선행지표
	통제목적	조직은 조직의 개인식별정보를 안전한 방법으로 보호해야 한다.		
	지수화 방법론	$(\frac{\text{보호되고 있는 개인 식별 정보의 수}}{\text{전체 개인 식별 정보의 수}})\times 100$		
15	평가분야	정보보호 기반(S/P)	평가목적	보안 관리
	평가지표	백업정보의 무결성 점검비율	지표성격	후행지표
	통제목적	조직은 백업 데이터에 대한 무결성 보장을 제공해야 한다.		
	지수화 방법론	$(\frac{\text{무결성이 보장되는 데이터의 합}}{\text{전체 백업 데이터의 합}})\times 100$		
16	평가분야	정보보호 기반(S/P)	평가목적	정보보호 시스템 도입
	평가지표	정보보호관리시스템의 범위 비율	지표성격	선행지표
	통제목적	조직의 정보보호 시스템은 ISMS 인증을 받아야 한다.		
	지수화 방법론	$\left(\frac{ISMS\text{인증이 포함하는 정보 시스템 수}}{\text{전체 정보 시스템의 수}}\right)\times 100$		
17	평가분야	정보보호 기반(S/P)	평가목적	정보보호 시스템 도입
	평가지표	보안서버 도입률	지표성격	선행지표
	통제목적	조직의 웹 사이트는 원격 접근을 위해 보안 터널을 이용해야 한다.		
	지수화 방법론	$(\frac{\text{보안서버를 이용하는 웹사이트 수}}{\text{전체 웹사이트 수}})\times 1000000$		
18	평가분야	정보보호 환경(P)	평가목적	정보보호 수준
	평가지표	스팸 수신 비율	지표성격	후행지표

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
	통제목적	조직은 조직원에게 발송되는 스팸을 차단하기 위한 스팸 필터를 이용해야 한다.		
	지수화 방법론	$(\frac{\text{일정량의 스팸메일을 수신한 조직원의 수}}{\text{전체 조직원의 수}}) \times 100$		
19	평가분야	정보보호 환경(P)	평가목적	정보보호 수준
	평가지표	이용자의 스팸메일 인식율	지표성격	후행지표
	통제목적	조직원은 출처를 알 수 없는 스팸메일을 열거나 첨부된 파일을 실행해서는 안 된다.		
	지수화 방법론	$(\frac{\text{스팸메일을 열거나 첨부된 파일을 실행한 조직원의 수}}{\text{전체 조직원의 수}}) \times 100$		
20	평가분야	정보보호 환경(P)	평가목적	정보보호 수준
	평가지표	보안교육 및 훈련 비율	지표성격	선행지표
	통제목적	조직원은 보안 사고에 적절히 대응하기 위해 보안훈련 및 교육을 이수해야 한다.		
	지수화 방법론	$(\frac{\text{보안훈련 및 교육을 완료한 조직원의 수}}{\text{전체 조직원의 수}}) \times 100$		
21	평가분야	Cybersecurity 역할 및 책임(P)	평가목적	정보보호 수준
	평가지표	정보보호 인력비율	지표성격	선행지표
	통제목적	조직은 보안인력을 채용하고 사이버보안 대응 인원 구성해야 한다.		
	지수화 방법론	$(\frac{\text{사이버보안 업무와 관련된 인력의 수}}{\text{전체 조직원의 수}}) \times 100$		
22	평가분야	정보보호 구현(S/P)	평가목적	정보화 역기능 수준
	평가지표	악성소프트웨어 감염 비율	지표성격	후행지표
	통제목적	조직원의 PC는 다양한 악성소프트웨어로부터 보호되어야 한다.		
	지수화 방법론	$(\frac{\text{악성소프트웨어에 감염된 } PC \text{대수}}{\text{전체 } PC \text{대수}}) \times 100$		

ITU-T SG17 제네바 회의(2010.12) X.csid에 제안된 후보 지표(조직분야)				
23	평가분야	정보보호 구현(P)	평가목적	정보화 역기능 수준
	평가지표	개인정보 노출비율	지표성격	후행지표
	통제목적	조직원의 개인정보는 노출되어서는 안 된다.		
	지수화 방법론	$(\frac{\text{개인정보노출경험이있는조직원의수}}{\text{전체조직원의수}})\times 100$		
24	평가분야	정보보호 기반(S/P)	평가목적	정보보호 수준지수
	평가지표	전자서명 이용비율	지표성격	선행지표
	통제목적	인증 및 식별을 이용할 경우, 조직원은 디지털 서명과 같은 강한 인증 방식을 이용해야 한다.		
	지수화 방법론	$(\frac{\text{전자인증서를발급받은조직원의수}}{\text{전체조직원의수}})\times 100$		
25	평가분야	정보보호 구현(S)	평가목적	정보화 역기능 수준
	평가지표	DDoS 측정	지표성격	후행지표
	통제목적	조직은 DoS 혹은 DDoS 공격으로부터 조직이 규정한 기간 동안 보호되어야 한다.		
	지수화 방법론	$(\frac{DDoS\text{공격으로실제서비스가중지된웹사이트의수}}{\text{웹사이트의수}})\times 100$		
26	평가분야	정보보호 구현(S)	평가목적	정보화 역기능 수준
	평가지표	봇넷 감염비율	지표성격	후행지표
	통제목적	조직은 봇넷 공격으로부터 보호되어야 한다.		
	지수화 방법론	$(\frac{\text{봇넷에감염된}PC\text{대수}}{\text{전체}PC\text{대수}})\times 100$		
27	평가분야	정보보호 환경(P)	평가목적	정보보호 예산
	평가지표	보안 예산 비율	지표성격	선행지표
	통제목적	기업은 조직은 사이버보안을 위한 예산을 지원해야 한다.		
	지수화 방법론	$(\frac{\text{조직의사이버보안예산}}{\text{조직의전체정보화예산}})\times 100$		

제 5 장 결 론

현재 ITU-T에서 진행하는 X.csi의 경우, 사이버 보안 지수와 관련하여 현재 글로벌 차원에서 합의된 지수가 없으며, 변화하는 기술반전 추이와 개도국이나 저개발국의 현황을 고려한 지수 개발이 요구되고 있으나 국제표준화 기구에서 표준화가 수행이 되고 있지 않기 때문에, 지수의 지표 데이터에 대한 신뢰성을 확보하면서 사이버보안 지수를 대표할 수 있는 지표 선정과 정보보호 정책의 집행 효과를 측정하기 위하여 한국의 염흥열(순천향대학교)와 송혜인(한국인터넷진흥원)이 제안하여 지난 SG17 회의(2010년 4월 7일~4월 16일) 사이버 보안 지수에 관한 가이드라인에 대한 신규 워크아이템 제안(A proposal for establishing a new work item on guidelines for Cybersecurity Index(CSI))으로 채택되었다. 이후 2010년 10월 라포쳐 회의를 거쳐, 2010년 12월에 개최 예정인 ITU-T SG17 회의에 개발된 사이버보안지수 지표가 포함된 기고서가 제출되었다.

사이버보안지수의 표준화를 통하여 기존 국내 주요 체계 및 지표를 통하여 표준화를 추진함으로써 국내 정보보호 환경 및 기반을 반영할 수 있는 국제표준 지표로 개발하였다. 그리하여 국내에서 활용되고 있는 지표를 반영하여 사이버보안지수를 개발하였기 때문에 데이터의 수집 및 측정에 유리하여 측정에 대한 용이성을 확보할 수 있다.

또한, 개발된 지수를 통해 집중 투자가 필요한 분야를 식별하고, 국가 정보보호 관련 예산의 확보와 중장기적인 정보보호 정책 수립 및 추진에 활용될 것으로 기대된다.

그리고 본 연구를 통하여 장기적으로 ITU로 하여금 향후에 국가별 정보보호 수준 현황을 파악하고, 이를 등급화 하는데 활용될 수 있을 것으로 보이며, 빠르게 변화하는 정보보호 이슈 및 개발도상국의 상황을 고려할 수 있는 신뢰성 있는 합의된 사이버 보안 지수를 개발할 수 있을 것으로 기대된다.

본 연구는 추후 주요 연구기관과 지속적인 협력을 토대로 개발된 지표의 고도화 연구를 진행해야할 것이다. 추가로 사이버보안 지수의 Use Case 연구가 진행되어야 할 것이다. 모

바일 및 클라우드 컴퓨팅 분야에 보안수준 평가지표 및 현재 개발된 지표가 포함하고 있지 못한 평가 영역에 대한 추가적인 지표 개발이 필요하다.

참고문헌

[1] ISO27001 Security, "Infosec Management Standards," http://www.iso27001security.com/
[2] 한국인터넷진흥원, “정보보호 관리체계 브로슈어”, 2010년 3월.
[3] 방송통신위원회, “개인정보보호관리체계(PIMS) 인증제 공청회,” 2010년 8월.
[4] 방송통신위원회, “개인정보보호관리체계(PIMS) 인증 심사항목 리스트,” 2010년 8월.
[5] ITU-T, “Proposal for the 4th revised text on ITU-T X.usnsec-1|ISO CD 29180: Security framework for ubiquitous sensor network,” http://www.itu.int/md/T09-SG 17-C-0125/en, Sep. 2009
[6] 국가사이버안전센터, “국가 사이버 안전 매뉴얼,” 2005년 10월.
[7] 행정안전부, “전자정부 정보보호관리체계 인증 등에 관한 지침,” 2010년 6월.
[8] 행정자치부, “개인정보보호수준 진단,” 2008년 4월.
[9] 한국인터넷진흥원, “공공기관 개인정보 영향평가 수행 안내서,” 2010년 3월.
[10] 한국인터넷진흥원, “정보보호 안전진단 해설서,” 2010년 3월.
[11] 한국인터넷진흥원, “정보보호 안전진단 업무 안내서,” 2010년 3월.
[12] 한국인터넷진흥원, “기업의 개인정보 영향평가 수행을 위한 안내서,” 2009년 1월.
[13] 정보통신산업진흥원, “eTRUST,” http://www.etrust.or.kr
[14] 한국정보보호진흥원, “국가 정보보호수준 평가지수 모델개발 및 활용에 관한 연구,” 2005년 12월.
[15] 한국정보통신진흥협회, “인터넷사이트 안전마크,” http://www.eprivacy.or.kr
[16] 한국정보통신진흥협회, “개인정보보호마크,” http://www.eprivacy.or.kr
[17] NIST, "Guide for Assessing the Security Controls in Federal Information Systems," Jul 2008.
[18] NIST, "Performance Measurement Guide for Information Security," Jul. 2008.
[19] NIST, "Recommended Security Controls for Federal Information Systems," Feb. 2005.
[20] BERR, "Information Security Breaches Survey 2008,," April 2008
[21] PricewaterhouseCoopers, Infosecurity Europe, "Information Security Breaches Survey 2010", April. 2010.
[22] Institute for Information Industry, http://web.iii.org.tw/
[23] 한국인터넷진흥원, “인증서 발급 현황,” http://isms.kisa.or.kr/isms/jsp/isms_2020.jsp
[24] 국가정보원, “국가정보보호백서,” 2009년 1월.
[25] NIST, "Guide to Developing Performance Metrics for Information Security," Jun. 2007.
[26] APWG, http://www.antiphishing.org
[27] Shadowserver, http://www.shadowserver.org/
[28] Homeland Security, "Primer Control Systems Cyber Security Framework and Technical Metrics," June, 2009.
[29] IATAC, "Measuring Cyber Security and Information Assurance," SOAR, May, 2009.
[30] ISO/IEC, http://www.iso.org

[부록 1] 과제 관련 언론 보도 기사

- 전자신문(2010-04-26): 사이버보안 지수, 국제 표준으로 개발

etnews.co.kr 전자신문 http://www.etnews.co.kr

사이버보안 지수, 국제 표준으로 개발

[2010-04-26]

스위스 제네바에서 열린 국제전기통신연합(ITU-T) 연구반 17(정보보호) 회의에서 '사이버보안 지수 가이드라인'을 새로운 표준화 항목으로 신설하고 향후 국제표준으로 개발하기로 합의한 것으로 알려졌다.

'사이버보안 지수'란 조직, 부문, 국가에 대한 보안 통제 이행 정도를 평가하고 정보보호 수준을 가늠하기 위한 평가 툴이라고 볼 수 있다. 이를 통해 수준이 미달하거나 추가적인 대응이 필요한 보안 분야를 식별하는데 활용될 수 있다.

사이버보안 지수 가이드라인 내용은 관리, 기술, 정책 측면에서 여러 지표들을 도출하고, 이들로부터 지수를 구하기 위한 방법론을 포함할 예정이다.

이번 국제 표준화 추진 합의는 현재 각 나라별로 다른 기준으로 평가되고 있는 사이버보안 지수를 국제 표준방식으로 개발해 동일한 잣대와 기준으로 평가할 수 있는 기반을 마련한 것을 의미한다. 특히 이번 가이드라인은 순천향대 엄흥열교수가 연구반 17 회의에 기고서를 제출해 프리너리에서 승인함으로서 이루어졌다.

엄흥열 순천향대 교수는 "이번 결과로 우리나라 국가정보보호 지수를 국제화하기 위한 토대를 마련했으며, 향후 인터넷진흥원 등 유관기관과 긴밀히 협력해 우리 실정이 반영된 국제 표준 사이버보안 지수를 개발하고자 한다"고 설명했다.

한편, 국내의 경우, 방송통신위원회와 국정원이 매년 우리나라 정보보호 수준 진전 정도를 평가해 '국가정보보호지수'로 발표하고 있으며, 미국 등 선진국도 정보보호 이행 정도와 수준을 평가해 차년도 정보보호 예산 수립시 반영하고 있다.

대표적인 국제 정보보호 지수는 세계경제포럼에서 매년 발표하는 보안 서버에 관한 것이 있으나, 전체 보안 수준을 측정하기에는 무리가 있는 것으로 알려져 있다. 따라서 이번 사이버보안 지수 가이드라인이 국제표준으로 신설되면 국내 정보보호 수준을 높이는데 기여할 것으로 기대되고 있다.

장윤정기자 linda@etnews.co.kr

출력하기 창닫기

- 보안 뉴스 (2010-09-16): 보안 기술의 국제 표준화로 경쟁력 강화에 일조할 것!

보안뉴스 미디어

"보안 기술의 국제 표준화로 경쟁력 강화에 일조할 것!"

2010-09-16

염흥열 순천향대학교 정보보호학과 교수

지난 2001년 순천향대학교에 처음으로 정보보호학과를 개설, 운영하고 있는 염흥열 교수는 지금까지 20년 동안 다양한 응용 보안 기술 연구와 후학양성에 매진하고 있다. 특히 국내 정보보호 수준 향상과 보안 기술 표준화를 위해 ITU-T(국제전기통신연합 전기통신표준화부문) 연구반 17의 부의장과 연구반 17/작업반 2의 의장으로 활동하고 있으며 ISO/IEC JTC 1 SC 27에서 네트워크 보안 국제표준 에디터로 활동하는 등 ITU-T와 ISO/IEC JTC 1에서 현재 개발 중인 10건의 국제표준 에디터로 활동하고 있다.

현재 순천향대학교에서 후학을 가르치고 있는데 주로 어떤 분야를 강의 하고 있는지. 순천향대학교에서 20년을 근무하고 있다. 특히 지난 2001년에 국내 최초로 학부에 정보보호학과를 개설하여 운영하고 있다. 학부과정에서 강의하는 과목은 인터넷보안, 방화벽, 네트워크 프로그램, 데이터통신, 컴퓨터 네트워크 등, 네트워크 보안 분야이다. 특히 석궭迷?과정의 경우, 무선 LAN 보안, 무선 네트워크 보안, 네트워크 보안 프로토콜 등이다.

한국인터넷진흥원(KISA)의 ISMS 인증위원장으로 활동하고 있는데. ISMS는 기업의 다양한 보안 환경과 보안 위협에 대처하기 위한 기술적, 물리적 보안 대책을 수립하여 시행하는 경영 프로세스이다. 한마디로 ISMS는 기업의 정보보호 수준을 한 단계 업그레이드 할 수 있는 중요한 툴이다. ISMS 인증은 ISMS를 수립 및 운영하고 있는 기업을 대상으로 정보통신망보호법에서 제시된 기준에 의거해 기업 ISMS 운영의 적절성과 타당성을 심사받고 심사를 통과한 기업에 ISMS 인증서를 부여하는 제도이다. 지난 3년간 최종 ISMS 인증 여부 타당성을 결정하는 한국 ISMS 인증위원회의 위원장으로 활동하고 있다.

현재 우리나라의 ISMS 인증 상황은 어떠한가. 지금까지 우리나라 나름대로 기준과 법제도에 근거해 적절하게 운영되어온 것도 인정되지만 ISMS 수준은 일본 등 선진국에 비해 아직 많이 미흡하다. 왜냐하면 한국인터넷진흥원의 ISMS 인증을 받은 기업의 수는 2010년 8월 현재 79개 정도이며 국제 ISMS 인증기업을 감안하면 국내 ISMS 인증기업은 185개이다. 일본의 경우 현재 3,572개 이상의 기업이 ISMS 인증을 받은 것으로 알려져 있다. 따라서 국내에서 ISMS 인증 기업의 수를 획기적으로 늘리기 위한 ISMS 활성화를 위해 다각적인 정부의 지원 정책이 방송통신위원회 차원에서 마련되고 일부는 시행되고 있으나 기업의 ISMS 중요성에 대한 인식제고가 필요하며 특히 교육, 의료, 금융 분야 기업에 대한 ISMS 인증을 적극적으로 권장할 필요가 있다고 본다.

우리나라 아이핀(I-PIN) 제도의 운영과 정착에도 그동안 많은 노력을 기울였는데. 지난 2005년도

에 아이핀(i-PIN)의 개념과 구조를 설정하기 위한 옛 정보통신부의 태스크포스 활동에 참여한 적이 있어서 아이핀 국내 운영 및 정착에 기여했다고 자부하며 아이핀의 발전과 확산에 남다른 애정이 있다. 지난 2008년 ITU-T 세계통신표준총회(WTSA)의 사이버보안 행사에서 한국의 아이핀을 발표해 중국 등으로부터 호평과 관심을 받은 바 있다. 아이핀은 한마디로 인터넷 상에서 주민등록번호를 대체하고 사용자 신원확인을 수행하는 한국형 아이디 관리 체계라고 볼 수 있다. 이러한 아이핀이 공공 및 정부, 모든 민간 분야에까지 모든 분야로 전면 확대 적용되어야 한다고 생각한다.

현재까지 아이핀(i-PIN) 제도가 제대로 정착되지 못한 이유는 무엇이라고 생각하는가. 현재 아이핀(i-PIN)이 직면한 문제는 아이핀을 구축하고 운영해야 할 기업의 문제와 사용자의 인식부족 문제로 구분할 수 있다. 아직 많은 기업이 관행적으로 주민등록번호를 이용해 회원가입을 받고 있다. 또한 기업의 아이핀 도입 의지가 부족한 실정이다. 따라서 기업은 주민등록번호 수집을 원천적으로 방지하면서 사용자의 신원을 확인할 수 있는 아이핀을 구축하여 서비스를 제공해야 할 것이다. 또한 사용자도 주민등록번호 등 자신의 개인정보를 필요 이상으로 인터넷 기업에게 주지 않아야 하며 주민등록번호를 이용해 회원 가입하지 말고 아이핀을 이용해 회원가입을 해야 한다.

최근 개인정보유출 사건이 이슈가 되고 있는데 각 기업의 개인정보보호 수준 강화를 위해서 해야 할 것은. 한마디로 기업의 개인정보 수집을 최소화하기 위한 노력과 수집된 개인정보의 안전한 처리와 보호가 요구된다. 기업은 자신이 지킬 수 있을 만큼만 개인정보를 사용자로부터 수집해야 한다. 예를 들어 아마존 등 외국 유명 사이트에 가입하기 위해서는 지극히 작은 수의 개인정보만을 제공하는 데 반해 우리나라는 필요치 않은 개인정보를 요구하고 있다.

적지 않은 기업이 개인정보 수집을 최소화하는 노력을 기울이고 있으나 대부분 국내 기업의 경우 아직도 많이 부족한 편이다. 또 기업의 개인정보도 표준화된 방법으로 안전하게 관리되어야 하며 개인정보관리 체계와 기준을 만족한 기업에 대해 국가에 의해 인증을 부여하는 것도 적절하다고 생각한다. 최근 방송통신위원회가 PIMS(Personal Information Management System, 개인정보관리체계) 제도를 2011년부터 시행한다고 발표한 바 있다. 이는 매우 바람직한 정책 방향이며 기업은 수집된 개인정보를 전사적 차원에서 전생명주기 동안 보호하는 관리체계 구축이 요구된다.

우리나라의 정보보호 현황과 수준을 평가한다면. 국가의 보안 수준은 국가, 기업, 개인 차원에서 평가될 수 있다. 먼저 정보보호에 투자가 되지 않은 상태에서 높은 정보보호 수준을 달성할 수 없다고 생각한다. 따라서 정보보호 수준을 높이기 위해 기업, 국민, 정부 차원의 활동이 필요하다고 생각한다. 세계경제포럼이 발표하고 있는 우리나라 정보보호 수준은 2009년 14위로 발표되었다. 그러나 기업, 정부, 국민 측면에서 정보보호강국으로 평가받기에는 아직 많이 부족하다.

정부의 정보기술 대비 정보보호 투자비는 미국의 경우 10% 내외가 되지만 우리나라는 2010년도에 8.2%(2,702억원)로 아직 선진국에 비해 아직 부족하다고 생각한다. 또한 방송통신위원회와 한국인터넷진흥원(KISA)이 국내 2,300개 사업체를 대상으로 조사한 2009년 기업 정보보호 실태에 따르면 정보보호 지출이 전혀 없는 기업이 63.6%, 정보화 투자 대비 5% 미만인 기업이 94%로 기업 대부분의 정보보호 투자가 미흡했다. 이를 보면 기업의 정보보호 투자는 많이 부족하다. 우리의 정보보호 수준을 획기적으로 개선하기 위한 사이버보안 법제도의 개선, 국민 의식수준 향상, 침해사고 예방 및 대응, 기업 및 정부의 정보보호 투자 및 대응 등의 활동이 요구된다. 특히 기

업이 기업 비즈니스 연속성 확보 차원에서 정보보호에 적극적으로 투자해야 한다.

현재 우리의 최대 보안 이슈는 무엇이며 이에 대한 대응방안은. 보안 이슈 중 현재 가장 문제가 되는 이슈는 DDoS 공격과 개인정보 유출 사건이라고 할 수 있다. 작년 7.7 DDoS 공격은 언제든지 다시 발생할 수 있다. 이 7.7 DDoS 공격 때보다 더 정교하고 발전된 봇넷이 나타나고 있다고 보고되고 있다. 또한 향후에는 인터넷전화, IPTV 서비스, 스마트그리드, 클라우드 컴퓨팅 서비스 또는 인프라에 대한 보안 위협과 이를 통한 개인정보의 유출 등 신규 보안 위협도 가까운 장래에 현실화 될 가능성이 있으며 특히 스마트폰을 이용하는 사용자가 급격히 증가함에 기인해 사용자 프라이버시 침해와 개인정보의 유출 등 다양한 보안 위협이 대두되고 있다.

이에 IT 제품 및 서비스 설계 단계에서 보안이 선행적으로 고려되고 삽입되어야 하며 설치 및 운영과정에서도 지속적으로 보안 위협이 평가되고 보안 대책을 마련되어야 하며 보안침해 사고에 사전 예방 체계와 신속하고 적절하게 대응 체계를 유지해야 한다. 물론 이를 위한 정보보호 조직의 구축은 당연한 것이다. 그리고 기업과 국민의 정보보호 수준을 제고하기 위한 기반을 마련하기 위해 국가 차원 정보보호 정책의 우선순위 부여와 각종 지원 정책 마련이 필요하다.

특히 최근 스마트폰과 SNS 보안 위협이 증가하고 있는데 이에 대한 의견은. 소셜 네트워크에서 가장 큰 보안 위협은 사용자의 위치에 대한 정보를 포함한 개인정보의 유출과 프라이버시 침해이다. 특히 사용자의 위치 정보에 대한 보호와 사용자의 위치정보보호 인식제고가 절대적으로 필요하다. 특히 쇼셜 네트워크를 통한 개인정보의 유출은 프라이버시 침해에와 함께 범죄 목적으로 활용될 가능성이 있으며 이미 범죄의 목적으로 활용될 수 있는 다양한 응용이 이미 존재하고 활용되고 있다고 알려지고 있다.

예를 들면 대표적인 쇼셜 네트워크 서비스인 페이스북(Facebook) 사용자의 개인정보와 위치정보 등을 분석해 사용자에 대한 범죄가 나타날 가능성이 매우 높다. 따라서 소셜 네트워크 서비스 제공자는 이러한 위협들에 대한 대비책을 마련해야 하며 이 대비책에 대한 글로벌 차원의 표준화된 합의가 필요하다. 특히 프라이버시 침해를 최소화할 수 있는 기술적, 관리적 대응 기법과 모범사례에 대한 연구를 시작해야 한다. 이러한 연구는 국내 단독 연구보다는 국제협력 연구형태로 수행되어야 한다. 또한 이용자 자신의 개인정보는 이용자 스스로 지켜야 하며 이에 대한 위협과 이의 침해사고 파급효과에 대해 이용자에게 알리는 인식제고가 필요하다.

요즘 주로 연구 하고 있는 분야는. 연구 분야는 무선네트워크 보안 프로토콜, 센서네트워크 보안, 공격자 역추적 기술, RFID 보안, IPTV 보안, 아이디 관리기술, 정보보호 수준 평가 지표 등의 다양한 응용 보안 기술을 연구하고 있다. 정보보호 기술에 바탕을 둔 법제도 등의 정책 연구도 수행하고 있다. 또한 네트워크 보안 및 응용 보안 분야에 대한 연구에 그치지 않고 연구결과를 국제표준화로 연결하고자 한다. 이를 위해 ITU-T(국제전기통신연합 전기통신표준화부문, International Telecommunication Union Telecommu nication Standardization Sector) 연구반 17의 부의장과 연구반 17/작업반 2의 의장으로 활동하고 있으며 ISO/IEC JTC 1 SC 27에서 네트워크보안 국제표준 에디터로 활동하는 등 ITU-T와 ISO/IEC JTC 1에서 현재 개발 중인 10건의 국제 표준 에디터로 활동하고 있다. 통상 에디터는 국제표준을 개발하고 문서화 작업을 수행하는 역할을 수행한다.

국가 정보보호 정책 및 규제와 연관된 국제 표준화도 매우 중요하다고 본다. 대표적으로 우리나라 국가정보보호지수를 ITU-T 국제 표준으로 개발하기 위한 ITU 권고 X.csi(사이버보안지수) 표준화 아이템을 지난 4월 ITU-T 연구반 17 회의에서 신설한 바 있고 현재는 에디터로 활동하고 있다.

우리나라 정보보호분야의 발전 방향은. 우리나라 정보보호분야는 정보보호 연구개발을 통한 기술수준 향상, 정보보호 인력양성, 정보보호 산업발전, 정보보호 법제도 향상 등 4가지 축이 적절하게 선순환적으로 연결되어야 발전할 수 있다고 생각한다. 현재 정보보호 인력은 전 세계 차원에서 부족하므로 인력양성을 위해 산업체를 포함한 관련 주체의 인력 양성을 위한 지원이 필요하며 정보보호 기술개발은 미국, 일본 등 선진국의 경우 가장 높은 우선순위를 두고 지원하고 있음을 감안해 우리도 우선순위를 높여야 할 것이며 정보보호 법제도 향상을 위한 노력도 꾸준히 필요하다.

특히 국내 정보보호 산업은 전년대비 9.2%(8,072억), 2014년까지 연평균 10.3% 정도의 성장세가 예측되는 유망 산업이다. 다만 150여개 가까운 정보보호 업체를 보유하고 있고 국내 정보보호 산업 규모는 아직 상대적으로 선진국에 비해 작은 규모이므로 지난 20여년간 습득한 경험과 노하우, 마케팅 전략을 통해 일본, 싱가폴 등 안정적 해외 시장을 적극 개척할 필요가 있다. 이를 위한 기반 조성은 정부의 역할이다.

앞으로의 계획은. 대학 교수의 기본 책무는 역시 후학 양성이다. 지난 2001년에 국내 최초로 학부과정에 정보보호학과를 신설했고 이를 통해 정보보호 분야의 이론과 실무를 겸비한 고급 인력 양성을 위해 노력할 생각이다. 또한 정보보호분야 국제 표준화 활동에 우선순위를 둘 것이다. 이를 통해 국내 보안 기술을 국제 표준화로 추진하여 국내 정보보호 산업과 기술의 국제 경쟁력을 강화하는데 일조하고 싶다.

최근 기억에 남는 일이 있다면. 최근 방송통신위원회가 개최한 '2010년도 해킹 방어 대회'에서 우리 학부 및 석사과정의 제자들로 구성된 '염흥열 교수의 제자'라는 팀이 우승을 차지한 바가 있다. 이 사실은 사전에 알지 못했고 대회가 끝나고 나중에야 알게됐다. 하지만 이러한 성과는 정보보호 이론뿐만 아니라 실무지식을 갖추지 않으면 달성할 수 없다고 생각하고 그들을 지도하는 교수의 입장에서 이번 해킹대회의 쾌거를 개인적으로는 매우 자랑스럽게 생각하고 있으며 기억에 남는 일이 됐다. 향후에도 이론 및 실무 기술을 겸비한 정보보호 공학도를 육성하여 각 분야에 공급함으로써 우리나라 정보보호 수준을 향상하는데 노력을 경주할 것이다.
<글/사진 : 김태형 기자(is21@boannews.com)>

[월간 정보보호21c 통권 제121호(info@boannews.com)]

- 디지털타임스(2010-10-27): 한국 정보보호지수 지표, 2012년 국제표준 된다

디지털타임스 뉴스인쇄

기사 주소: http://www.dt.co.kr/contents.html?article_no=2010102802010251746001

한국 정보보호지수 지표…2012년 국제표준 된다

ITU-T 회의서 주요사례 소개

김지선 기자 dubs45@dt.co.kr | 입력: 2010-10-27 23:20

2012년 국제표준 채택을 목표로 개발중인 세계 사이버보안지수에 우리나라 국가정보보호지수의 주요 지표가 반영된다.

27일 업계에 따르면, 이 달 중순 일본 도쿄에서 열린 국제전기통신연합(ITU-T) 연구반(SG)17(정보보호)회의에서 우리나라 국가정보보호지수의 주요 지표가 세계 사이버보안지수 부록으로 실려 주요 사례로 소개됐다. 부록은 본문과 같은 효력을 갖고 있으며, 외국 사례가 부록에 포함된 것은 우리나라가 유일하다.

현행 국가정보보호지수는 3개 영역 12개 항목으로 구성돼 있다. 백신, 패치, 방화벽 보급률 등으로 구성된 정보보호 기반영역, 정보보호 관련 예산비율 등 정보보호 환경 영역, 해킹, 바이러스 신고비율 등 정보화 역기능 영역으로 구분된다.

ITU-T가 추진중인 사이버보안지수는 각 국의 조직과 기업, 국가 등의 사이버보안 현황을 파악할 수 있도록 지수 평가방법을 구성할 계획이다. 이 지수는 사이버보안에 대한 글로벌 지수로 활용되며 보안 지수가 없는 개발도상국 등에게 유용한 지침서가 된다는 점에서 의미가 크다.

이에 따라 ITU-T는 지난 6개월간 공식 또는 이메일과 유선으로 회의를 해 왔고, 특히 우리나라의 국가정보보호지수에 대해 많은 관심을 보여왔다. 최근 일본에서 열린 회의에서 토니 러트코스키 ITU-T 연구반17 의장(미국)은 '한국의 국가정보보호지수는 각 국의 정책 입안자들에게 정보보호 분야 투자 등에 대한 동기를 부여하는데 좋은 사례로 꼽힌다'며 우리나라의 국가정보보호지수가 세계 사이버보안지수에 중요한 기틀이 될 수 있음을 언급했다.

우리나라 대표로 회의에 참석한 염흥열 순천향대 교수는 '미국, 영국, 일본 등 세계 주요 국가의 정보보호 분야 대표들이 참석한 회의에서 선진국들을 제치고 우리나라의 정보보호지수가 채택된 것은 우리나라의 정보보호 체계를 인정받았다는 점에서 의미가 크다'며 '다음 회의때 논의되는 세부 지표에도 우리나라 지표들이 들어갈 수 있도록 노력하겠다'고 말했다.

ITU-T 연구반 17은 12월경 다시 회의를 열고 사이버보안지수의 세부 지표 내용 등을 논의한다. 또 내년 4월과 9월 ITU-T 공식 회의에서 이 내용 등을 구체화하는 작업을 거쳐, 오는 2012년 초쯤 정식으로 국제 표준 채택을 한다는 계획이다.

김지선기자 dubs45@

출력시간: 2010-11-15 17:51:11

- 전자신문(2010-12-22): 국산 사이버보안지수 글로벌 표준으로 '우뚝'

etnews.co.kr 전자신문 http://www.etnews.co.kr

국산 사이버보안지수 글로벌 표준으로 `우뚝`

[2010-12-22]

국가의 정보보호 수준을 판단하는 잣대로서 우리나라가 제안한 사이버보안지수가 국제전기통신연합(ITU-T)에서 국제표준사이버보안지수로 사실상 채택, 국제 보안 무대에서 한국의 위상이 높아질 전망이다. ITU-T는 한 국가의 정보보호수준을 판단하는 지표로 세계경제포럼이 매년 발표하는 '보안서버 보급률'이 있지만 전반적인 수준을 측정하기에는 부족하다고 판단, 국제표준 사이버보안 지수 작성을 논의해왔다. 22일 정부에 따르면 지난 8일~17일 스위스 제네바에서 열린 국제전기통신연합(ITU-T) 연구반 17회의(정보보호)에서 국제표준사이버보안지수를 구성하는 27개의 세부 지표 중 우리나라가 제출한 12개의 세부 지표 모두가 채택됐다. 우리 정부는 백신 보급률, 패치 보급률, 방화벽 보급률, 좀비 PC감염률, 정보보호 예산 비율, 바이러스 신고비율 등 12개 항목을 ITU-T 17회의에 사이버보안 지수로 제출한 바 있다. 이번 ITU-T 17 회의에서 이같이 결정함에 따라 ITU-T는 내년 4월과 9월 잇달아 열리는 공식 회의에서 국제표준 보안지수를 다시 한번 검증하고 조정하는 단계를 거쳐, 오는 2012년 초 공식적으로 대외에 발표할 예정이다. 순천향대 염흥열 교수는 "국내 사이버보안 지수를 국제표준에 반영하는 성과를 거뒀을 뿐만 아니라 국제 보안 표준화 활동을 관장하는 협의체인 '보안협력회의(JCA on Security)' 신설도 우리가 주도해 국제 무대에서 한국의 위상이 보다 높아질 것"이라고 말했다.

장윤정기자 linda@etnews.co.kr

출력하기 창닫기

[부록 2] 전문가 설문조사 양식

2010년도 방송통신 정책연구용역사업

『국제표준 사이버보안지수 개발 및 방법론 연구』 관련 전문가 설문조사

안녕하십니까?

본 연구실에서는 금년도 방송통신위원회 정책연구용역 사업의 일환으로 정보통신산업진흥원과 함께 『국제표준 사이버보안지수 개발 및 방법론 연구』에 관한 연구를 수행 중에 있습니다. 국제표준 정보보호 평가지표 개발을 목적으로 개발한 지표들에 대한 적합성 판단 및 가중치 할당을 위하여 각계 전문가님들께 설문조사를 실시하려고 합니다. 바쁘시더라도 우리나라의 정보보호평가 지표의 반영을 위하여 귀하의 고견을 주시면 소중히 활용하겠습니다.

설문 응답시간에는 약 2~3시간이 소요될 것으로 예상됩니다. 유효한 응답해 주신 분들께는 소정의 자문료를 지급해드리도록 하겠습니다. 응답해 주신 설문내용과 응답자의 기본정보는 목적 외의 다른 용도로 사용하지 않을 것을 약속드립니다.

본 설문에 응해주신 전문가님의 소중한 고견에 다시 한 번 감사드립니다.

※ 본 설문지에 대한 의문사항이나 구성에 대한 문의 사항이 있으시면 언제든지 연락주시기 바랍니다.

책임 연구자 : 염 흥 열 (순천향대학교 일반대학원 정보보호학과)
연구원 : 여 돈 구, 이 동 희 (순천향대학교 일반대학원 정보보호학과 석사과정)
연락처 : 041) 530 - 1328, E-mail : h7ei@paran.com
주 소 : (336-745)충남 아산시 신창면 순천향대학교 멀티미디어관 M114호

2010년 10월

순천향대학교 일반대학원 정보보호학과 Cybersecurity Lab.

지표 적합성 및 가중치 설문 작성시 참조사항

□ 귀하께서는 저희 연구실에서 실시하는 『국제표준 사이버보안지수 개발 및 방법론 연구』를 위한 설문조사에 응해주신 것을 진심으로 감사드리며, 끝까지 참여하여 주시어 좋은 결과를 얻을 수 있도록 지도·편달하여 주실 것을 부탁드립니다.

□ 본 설문조사의 응답자 집단은 소수의 각계 전문가로 구성된 소집단(30명 내외)으로서 순천향대학교 정보보호대학원 석/박사 졸업생 및 한국인터넷진흥원에서 선별해주신 전문가입니다.

□ 본 설문조사는 단답형 및 서술형 설문지 조사로 이루어지며, 다수의 의견을 반영하는 표결(polling)방식으로 진행됩니다. 추가로, 설문지상의 설문에 대한 자유로운 의견 또한 수렴하여 공정성 있는 지표 개발에 반영할 계획입니다.

□ 본 연구실에서는 응답자 여러분께 설문 문항에 대하여 깊이 사고하신 연후에 진지하게 응답해주시기를 간절히 바라고 있습니다. 또한 새로운 문제를 제기하여 주시거나 새로운 대안을 탐색해 주시기를 간청드립니다.

□ 이 설문조사는 자문료 지급을 위하여 기명으로 실시되지만, 의견 수렴시 익명성을 보장합니다.

□ 만약, 귀하가 설문지의 특정 문항이 잘못되었다고 생각되시면 그 문항에 대한 수정 의견을 제안하실 수 있으며, 귀하가 수정한 문항에 대하여 응답하실 수도 있습니다.

□ 설문지는 e-mail을 통하여 배포되고 e-mail을 통해 수집될 것입니다만, 서면으로 작성하셨다면 우편을 이용하여 보내주시면 감사하겠습니다. (우편을 이용하실 경우, 정확한 전달을 위하여 사전에 연락을 주시면 감사하겠습니다.)

본 조사의 취지

1. 연구의 배경

o 정보통신분야에는 국제전기통신연합(ITU)의 DI(Development Index)와 세계경제포럼(WEF)의 NRI(Network Readiness Index) 등의 국제적인 평가 기준이 개발되어 있지만, 정보보호분야의 국제적인 사이버 보안 지수는 개발되지 않은 상태입니다.

o 또한, 현재 세계경제포럼과 세계경제협력기구(OECD)에서 시행하고 있는 보안 평가 지표는 보안 서버의 개수만을 이용하므로, 변화하는 정보보안 서비스와 각국의 정보보호 수준을 평가할 수 있는 지표로는 턱없이 부족한 실정입니다.

2. 연구의 목적

o 대부분의 국가에서 수집 가능한 보편적인 데이터를 기반으로 지표를 개발한다.

o 국가 차원의 정보보호 평가를 위하여 기존 정보보호 평가지표 중 대표성 있는 지표를 선정한다.

o 국내 정보보호 평가지표를 사이버 보안지수 모델에 최대한 반영한다.

o 정량적 평가가 가능하도록 정성적 평가지표를 정량적 평가지표로 변경한다.

3. 연구방법

o 국내외 정보보호 평가 지표 현황 분석
- 각 국가 및 표준화기구로 부터 다양한 지표들의 수집 및 비교 분석
- 수집한 지표를 토대로 각 지표의 분석

o 전문가 풀을 이용하여 지표의 정당성 평가 및 지표의 등급을 결정

o 정보보호 분야에서 글로벌하게 합의된 지표 선정
- 상기 연구를 통해 도출한 후보 지표를 바탕으로 ITU-T의 표준화 전문가회의를 통하여 국제화 표준 추진 예정

설문 응답 방법

□ 본 설문지의 질문항목에 대한 응답은 **(적당/부적당)** 혹은 **(필수/권고/선택/필요없음)** 중 한 가지를 선택을 하실 수 있습니다.

- **"적당"을 선택하신 경우,** 신뢰도를 1~9 까지 선택하실 수 있습니다.

1	2	3	4	5	6	7	8	9
매우낮음		낮음		보통		높음		매우높음

- **"부적당" 혹은 1~4점을 선택하신 경우,** 하단 여백에 질문항목 번호와 함께 의견을 기록하실 수 있습니다.

- **"필수/권고/선택/필요없음" 설문 항목**은 지표의 중요도를 평가하는 항목입니다. 중요도에 따라서 이후 표준화 추진시 국가의 정보보호평가 표준항목으로 추진할 계획입니다.

- **기타 의견**이 있으신 경우, 하단 여백에 자유롭게 의견을 기록하실 수 있습니다.

< 아래 표는 설문 응답의 예시입니다.>

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?	X	
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?	7	
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?	6	
④평가에 있어 본 지표를 "**필수/권고/선택/필요없음**"으로 구분한다면 어떻게 선택하시겠습니까?	필수	

위 설문 문항 중 1~4점 혹은 No를 선택하신 경우, 해당 항목 번호와 의견을 적어주시면 됩니다. (또한, 명칭 변경이나 기타 의견이 있으시면 간단하게 서술해주시기 바랍니다.)

(4) : 지수화에 있어 총 조직의 예산 비율을 반영하는 것이 좋을 것 같습니다.
- 일부 조직의 경우 총 조직 예산에 비해 정보화예산 비율 자체가 낮을 가능성이 있다. 이러한 경우 정보화대비 정보보호예산 비율은 높을 수 있지만 조직의 전체 예산 비율대비 정보보호예산 비율은 적정치에 미치지 못할 수 있습니다.

사이버 보안지수 모델 제안

제안하는 사이버 보안지수 모델은 조직 및 국가의 정보보호 수준을 평가하기 위해 한국정보보호지수에서 평가하고 있는 **평가분야**를 적용하였다. 각 분야에서는 2~4 가지의 **평가목적**을 수립하고, 평가목적을 달성하기 위한 **세부 평가지표**로 이루어져 있으며, 각 **세부 평가지표**는 가능하면 선행지표와 후행지표를 모두 포함하는 방향으로 구성하였으며, 세부 평가지표의 정보보호 목적, 측정 방법 및 출처는 다음 페이지에 첨부하였다.

설문 항목 (1)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	취약점 관리	지표성격	선행지표
통제목적	조직은 조직 내의 취약점을 식별하고, 식별된 취약점에 대한 적적한 조치를 해야 한다.		
지수화 방법론	$(\frac{\text{조치된 취약점의 개수}}{\text{식별된 취약점의 개수}}) \times 100$		
참조	SP800-53 RA-5:Vulnerability Scanning, SI-2:Flaw Remediation		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (2)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	감사 및 책임	지표성격	선행지표
통제목적	조직은 조직 내의 부적절한 활동을 모니터링, 분석, 조사를 위해 정보 시스템 감사기록을 생성, 보호, 보관해야 한다.		
지수화 방법론	$(\frac{\text{중앙에서 감사로깅이 가능한 전체 } PC\text{개수}}{\text{전체 } PC\text{개수}}) \times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (3)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	감사 및 책임	지표성격	후행지표
통제목적	조직은 조직 내의 부적절한 활동을 모니터링, 분석, 조사를 위해 정보 시스템 감사기록을 생성, 보호, 보관해야 한다.		
지수화 방법론	$[1-(\frac{\text{부적절한 활동이 탐지된 } PC\text{개수}}{\text{전체 } PC\text{개수}})]\times 100$		
참조	자체/SP800-53 AU:Audit Monitoring, Analysis, and Reporting		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (4)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	위협 평가	지표성격	선행지표
통제목적	조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.		
지수화 방법론	$(\frac{\text{업무연속성 계획에 반영된 위협의 개수}}{\text{위험분석을 통해 식별된 위협의 개수}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (5)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	위협 평가	지표성격	후행지표
통제목적	조직은 조직원에게 메일링 서비스에 대한 안전한 교육을 실시하고, 스팸 메일의 대응 능력을 평가한다.		
지수화 방법론	$[1-(\frac{\text{스팸메일을오픈한수}+\text{첨부파일을클릭한수}}{\text{전체조직원의수}})]\times 100$		
참조	Cyber Health Check		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (6)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	위협 평가	지표성격	후행지표
통제목적	조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.		
지수화 방법론	$(\frac{\text{스팸메일신고건수}}{\text{전체스팸메일발송건수}})\times 100$		
참조	자체/Cyber Health Check		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (7)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	위협 평가	지표성격	후행지표
통제목적	조직의 정보 시스템에 대한 위험분석을 주기적으로 수행하고, 결과를 정책에 반영한다.		
지수화 방법론	$(\frac{\text{업무 연속성 계획에 따라 조치된 취약점의 개수}}{\text{취약점 스캔을 통해 식별된 취약점의 개수}})\times 100$		
참조	자체/SP800-53 RA-5:Vulnerability Scanning, CA-5:Plan of Actions and Milestones, (POA&M(Plan of Actions and Milestones))		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (8)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	유지관리	지표성격	선행지표
통제목적	조직은 정보 시스템에 대해 주기적이고 시기적절한 유지관리 수행 및 효율적 통제를 제공해야 한다.		
지수화 방법론	$(\frac{\text{공식적인 유지관리 스케쥴에 따라 관리되는 시스템의 개수}}{\text{전체 시스템의 개수}})\times 100$		
참조	SP800-53 MA-2:Controlled Maintenance and MA-6:Timely Maintenance		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (9)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	유지관리	지표성격	후행지표
통제목적	조직은 정보 시스템에 대해 주기적이고 시기적절한 유지관리 수행 및 효율적 통제를 제공해야 한다.		
지수화 방법론	$[1-(\frac{\text{전체 시스템의 오류 발생 건수}}{\text{전체 시스템 개수} \times \text{점검 횟수}})] \times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (10)

지표구분	조직		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	시스템 및 정보 무결성	지표성격	선행지표
통제목적	조직은 정보 시스템에 대한 신규 보안 위협에 대처하기 위하여 자동화된 패치 관리 시스템을 도입하여 운영해야 한다.		
지수화 방법론	$(\frac{\text{패치 관리 프로그램이 설치된 } PC \text{대수}}{\text{전체 } PC \text{대수}}) \times 100$		
참조	자체/국가정보보호지수, 전자정부서비스 보안수준 실태조사, PIA, 정보보호안전진단, DHS-CSSP		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (11)

지표구분	조직		
평가분야	정보보호 구현	평가목적	침해사고 대응
평가지표	긴급사태 대책	지표성격	선행지표
통제목적	조직은 지속적인 서비스 운영을 위한 긴급사태 대책을 수립/관리하고 효율적으로 구현한다.		
지수화 방법론	$(\frac{\text{연간긴급사태계획테스트를수행하는정보시스템의개수}}{\text{시스템목록에있는정보시스템의개수}})\times 100$		
참조	SP800-53 CP-4:Contigency Plan Testing and Exercies		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (12)

지표구분	조직		
평가분야	정보보호 구현	평가목적	침해사고 대응
평가지표	긴급사태 대책	지표성격	후행지표
통제목적	조직은 지속적인 서비스 운영을 위한 긴급사태 대책을 수립/관리하고 효율적으로 구현한다.		
지수화 방법론	$(\frac{\text{초기대응성공건수}}{\text{연간긴급사태발생건수}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (13)

지표구분	조직		
평가분야	정보보호 구현	평가목적	침해사고 대응
평가지표	사건 보고	지표성격	후행지표
통제목적	조직은 보안사고의 신속한 대응을 위해 사건보고 시스템을 운영하고, 보안 교육 및 모의 훈련을 통해 이를 점검해야 한다.		
지수화 방법론	$(\frac{\text{모의훈련횟수}}{\text{보안교육횟수}})\times 100$		
참조	자체/ISMS, K-ISMS, G-ISMS, PIMS…		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (14)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	증명, 승인, 보안 평가	지표성격	선행지표
통제목적	조직은 조직 내의 모든 정보 시스템에 요구되는 보안 증명 및 승인을 받아야 한다.		
지수화 방법론	$(\frac{\text{구현이전에인가담당자에게}\ CA\ \text{받은신규시스템의개수}}{\text{전체신규시스템의개수}})\times 100$		
참조	SP800-53 CA(Certification, Accreditation, and Security Assessments)-6:Security Accreditation		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (15)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	증명, 승인, 보안 평가	지표성격	후행지표
통제목적	조직은 조직 내의 모든 정보 시스템에 요구되는 보안 증명 및 승인을 받아야 한다.		
지수화 방법론	$[1-(\frac{\text{연간 발견된 비인가 시스템의 개수}}{\text{인가 받은 시스템의 개수}})]\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (16)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 보유	지표성격	선행지표
통제목적	정보통신망의 안전성 및 정보통신 설비 보호를 위해 정보보호 시스템을 설치/운영함으로써 네트워크 보안을 강화한다.		
지수화 방법론	$(\frac{\text{전체 정보보호 시스템 도입 개수}}{\text{전체 서버의 개수}})\times 100$		
참조	정보보호 시스템 : 방화벽, IDS, IPS, 웹방화벽 자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (17)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 보유	지표성격	선행지표
통제목적	주요정보 전송시 비밀성과 무결성을 보장하는 보안서버구축 등의 조치를 적용해야 한다.		
지수화 방법론	$(\frac{\text{보안서버의 개수}}{\text{전체서버의 개수}})\times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (18)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 보유	지표성격	후행지표
통제목적	조직은 급격한 트레픽 증가로 인한 네트워크 공격을 방어하기 위한 장비를 도입해야 한다.		
지수화 방법론	$[1-(\frac{\text{일일평균트래픽량}}{DDoS\text{방화벽의최대트래픽처리량}})]\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (19)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	시스템 및 서비스 구입	지표성격	선행지표
통제목적	아웃소싱 제공자가 조직으로부터 아웃소싱된 정보, 응용, 서비스를 보호하기 위해 적절한 보안 측정을 만족함을 보장한다.		
지수화 방법론	$(\frac{\text{보안 요구사항 및 명세를 포함하는 계약서의 개수}}{\text{시스템 및 서비스 구입 계약서의 전체 개수}})\times 100$		
참조	SP800-53 SA:Acquisitions		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (20)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	시스템 및 서비스 구입	지표성격	후행지표
통제목적	시스템은 유지관리를 통해 도입 계획 기간 내의 가용성을 보장해야 한다.		
지수화 방법론	$(\frac{\text{실제 운영 중인 시스템의 개수}}{\text{시스템 및 서비스 구입 계약서의 전체 개수}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (21)

지표구분	조직		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 도입	지표성격	선행지표
통제목적	조직은 글로벌 선진 기업들의 Bast Practice에 기반한 정보보호 관리 체계를 수립함으로써 조직의 신뢰도를 향상시킨다.		
지수화 방법론	$\left(\frac{ISMS\text{재인증횟수}}{(\frac{\text{현재년도}-\text{최초인증년도}}{3})}\right)\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (22)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	정보보호 시스템 도입	지표성격	후행지표
통제목적	조직의 정보 시스템을 위해서 행동규칙 및 보안 계획을 수립하고 이를 주기적으로 업데이트해야 한다.		
지수화 방법론	$(\frac{\text{행동규칙에 대해 서명 이후 시스템 접근을 획득한 사용자 수}}{\text{전체 시스템 접근자 수}})\times 100$		
참조	SP800-53 PL-4:Rules of Behavior, AC-2:Account Management		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (23)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	설정 관리	지표성격	선행지표
통제목적	조직은 시스템 개발 라이프 사이클을 통해 기본 설정을 수립하고, 조직 정보 시스템의 목록을 유지한다.		
지수화 방법론	$(\frac{\text{자동화된 시스템 개발 라이프사이클을 적용한 자산의 개수}}{\text{전체 정보 자산의 개수}})\times 100$		
참조	자체/SP800-53 CM-2:Baseline Configuration and CM-3: Configuration Change Control		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (24)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	설정 관리	지표성격	후행지표
통제목적	조직은 시스템 개발 라이프 사이클을 통해 기본 설정을 수립하고, 조직 정보 시스템의 목록을 유지한다.		
지수화 방법론	$(\frac{\text{승인 및 구현된 설정 변경 건수}}{\text{자동화된 스캔으로 식별한 설정 변경 건수}})\times 100$		
참조	SP800-53 CM-2:Baseline Configuration and CM-3: Configuration Change Control		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (25)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	시스템 및 통신 보안	지표성격	선행지표
통제목적	조직은 전자 정보 인프라의 적절한 보호를 위해 충분한 자원을 할당해야 한다.		
지수화 방법론	$(\frac{\text{암호학적 연산을 수행하는 모바일 컴퓨터 및 장치의 개수}}{\text{조직의 모바일 컴퓨터 및 장치의 개수}})\times 100$		
참조	자체/SP800-53 SC-13:Use of Validate Cryptography		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (26)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	시스템 및 통신 보안	지표성격	후행지표
통제목적	조직은 전자 정보 인프라의 적절한 보호를 위해 충분한 자원을 할당해야 한다.		
지수화 방법론	$(\frac{\text{인증, 암호화, 부인방지 기능을 이용한 전자상거래 건수}}{\text{연간 전자상거래 건수}})\times 100$		
참조	자체/ISO 27001, K-ISMS, G-ISMS		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (27)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	접근 통제	지표성격	선행지표
통제목적	조직은 조직 내의 정보 자산에 접근할 수 있는 엑세스 포인트에 대한 접근 통제를 수행해야 한다.		
지수화 방법론	$[1-(\frac{\text{침입차단/탐지시스템이 설치된 엑세스 포인트의 개수}}{\text{전체 엑세스 포인트의 개수}})]\times 100$		
참조	자체/SP800-53 AC-17:Remote Access		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (28)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	접근 통제	지표성격	후행지표
통제목적	조직은 조직 내의 정보 자산에 접근할 수 있는 엑세스 포인트에 대한 접근 통제를 수행해야 한다.		
지수화 방법론	$(\frac{\text{비인가 접근이 획득된 엑세스 포인트의 개수}}{\text{전체 엑세스 포인트의 개수}})\times 100$		
참조	SP800-53 AC-17:Remote Access		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (29)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	물리적 환경	지표성격	후행지표
통제목적	조직의 정보 자원의 적절한 보호를 보장하기 위해 물리적 보호 메커니즘과 정보보호 메커니즘을 통합한다.		
지수화 방법론	$[1-(\frac{\text{비인가 출입을 허가한 물리적 안전사고 발생 건수}}{\text{전체 물리적 안전사고 발생 건수}})]\times 100$		
참조	SP800-53 PE-6:Monitoring Physical Access		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (30)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	물리적 환경	지표성격	선행지표
통제목적	조직은 물리적 접속 통제를 위해서 무선 엑세스 포인트를 관리해야 하며, 적절한 수준의 보안설정을 유지해야 한다.		
지수화 방법론	$(\frac{\text{보안이 설정된 무선 엑세스 포인트 개수}}{\text{조직내의 전체 무선 엑세스 포인트 개수}})\times 100$		
참조	자체/SP800-53A AC-17:Access Control		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (31)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	물리적 환경	지표성격	선행지표
통제목적	조직은 네트워크의 가용성에 대한 중대한 영향을 미치는 회선에 대해 서비스의 가용성과 연속성을 보장할 수 있어야 한다.		
지수화 방법론	$(\frac{\text{이중화된 네트워크 장비의 대수}}{\text{전체 네트워크 장비의 대수}}) \times 100$		
참조	네트워크 장비 : 라우터, DNS, DHCP, DB, 방화벽 등 정보보호 안전진단, 전자정부서비스 보안수준 실태조사		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (32)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	물리적 환경	지표성격	선행지표
통제목적	조직은 정보자산이 위치한 지역에 대해 인가된 자에 한하여 출입/접근할 수 있도록 관리해야 한다.		
지수화 방법론	$[1-(\frac{\text{출입통제 시스템이 설치되지 않은 구역의 수}}{\text{전체 출입통제 구역의 개수}})] \times 100$		
참조	자체/ISO 27001, K-ISMS< G-ISMS		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (33)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	물리적 환경	지표성격	선행지표
통제목적	조직은 정보자산이 위치한 지역에 대해 인가된 자에 한하여 출입/접근할 수 있도록 관리해야 한다.		
지수화 방법론	$[1-(\frac{CCTV\text{가 설치되지 않은 구역의 수}}{\text{전체 출입통제 구역의 개수}})]\times 100$		
참조	자체/ISO 27001, K-ISMS, G-ISMS		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (34)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	식별 및 인증	지표성격	선행지표
통제목적	특정 등급 이상의 주요 정보 자산에 대해 사용자 및 시스템 인증 요구사항에 맞는 인증 및 암호화를 적용해야 한다.		
지수화 방법론	$(\frac{\text{식별 및 인증이 이루어지는 자산의 수}}{\text{주요 자산으로 분류된 자산의 수}})\times 100$		
참조	자체/K-ISMS		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (35)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	식별 및 인증	지표성격	후행지표
통제목적	모든 시스템은 정보보호 정책에 따라 식별되고 인증되어야 한다.		
지수화 방법론	$[1-(\frac{\text{공유 계정의 개수}}{\text{전체 사용자 계정의 개수}})]\times 100$		
참조	자체/SP800-53 AC-2:Account Management, AC-3:Access Enforcement, IA-2:User Identification and Authentication		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (36)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	미디어 보호	지표성격	후행지표
통제목적	조직은 미디어의 신뢰성 및 정보의 무결성 검증을 위해 조직이 정한 주기에 따라 백업 정보를 확인해야 한다.		
지수화 방법론	$(\frac{\text{백업 정보의 무결성 점검 횟수}}{\text{정보 자산의 백업 수행 횟수}})\times 100$		
참조	자체/SP800-53A		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (37)

지표구분	조직		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	미디어 보호	지표성격	후행지표
통제목적	재사용을 위한 처리 및 배포 이전에 정보 시스템 미디어를 제거하거나 파괴해야 한다.		
지수화 방법론	$(\frac{\text{제거 절차 테스트를 통과한 미디어의 개수}}{\text{테스트를 거친 전체 미디어의 개수}})\times 100$		
참조	SP800-53 MP-6:Media Santization and Disposal		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (38)

지표구분	조직		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	선행지표
통제목적	업무 능률 개선을 위해 스마트워킹을 지원하는 경우, 스마트폰의 통제를 강화하여 정보자산에 대한 보안을 강화해야 한다.		
지수화 방법론	$(\frac{\text{스마트폰 보안통제 관련 예산}}{\text{스마트폰 활성화 지원 예산}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (39)

지표구분	조직		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	후행지표
통제목적	조직 외부에서 조직 내부로 접속하는 사용자에 대한 기기 인증 및 사용자 인증은 물론, 암화화된 통신을 지원해야 한다.		
지수화 방법론	$(\frac{\text{사용자 인증}(VPN)\text{을 통한 원격접근 이용자수}}{\text{전체 스마트폰을 이용한 원격접근 수}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (40)

지표구분	조직		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	후행지표
통제목적	조직 내부 정보의 유출을 방지하기 위하여 비인가된 스마트 폰의 내부 반입을 금지해야 한다.		
지수화 방법론	$[1-(\frac{\text{비인가된 스마트폰 소지자 수}}{\text{전체 스마트폰 이용자 수}})]\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (41)

지표구분	조직		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트 그리드 통제	지표성격	후행지표
통제목적	스마트 그리드는 지속적인 전력 공급이 가능하도록 전력선 이중화나 우회 공급 경로를 확보해야 한다.		
지수화 방법론	$[1-(\frac{\text{조직 내의 전력 복구시간(분)}}{365\times1440})]\times100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (42)

지표구분	조직		
평가분야	정보보호 기반	평가목적	개인정보보호
평가지표	개인정보보호	지표성격	선행지표
통제목적	개인정보를 취급하는 조직은 개인정보 수집 및 이용시 그 사실을 고지하고 이용자의 동의를 얻어야 한다.		
지수화 방법론	$(\frac{OECD\text{개인정보보호가이드라인을 준수하는 시스템의 개수}}{\text{전체 개인정를 수집, 처리, 관리하는 시스템의 개수}})\times100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (43)

지표구분	조직		
평가분야	정보보호 기반	평가목적	개인정보보호
평가지표	개인정보보호	지표성격	후행지표
통제목적	개인정보를 취급하는 조직은 개인정보 수집 및 이용시 그 사실을 고지하고 이용자의 동의를 얻어야 한다.		
지수화 방법론	$[1-(\frac{\text{신고 및 적발 건수}}{\text{조직에 가입된 전체 회원수}})]\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (44)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	선행지표
통제목적	조직의 정보보호 수준을 높이기 위해서는 담당 업무의 직원, CEO, 일반 직원 모두가 정보보호의 중요성을 인식해야 한다.		
지수화 방법론	$(\frac{\text{정보보호가 중요하다고 인식하는 조직원의 수}}{\text{전체 조직원의 수}})\times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (45)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	조직의 정보보호 수준을 높이기 위해서는 담당 업무의 직원, CEO, 일반 직원 모두가 정보보호의 중요성을 인식해야 한다.		
지수화 방법론	$(\frac{\text{연간 일일 보안 점검 수행자의 수}}{\text{전체 조직원의 수} \times 365}) \times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (46)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	선행지표
통제목적	조직은 기본적인 보안 수준 확립을 위하여 모든 PC에 백신 프로그램을 설치해야 한다.		
지수화 방법론	$(\frac{\text{백신 프로그램이 설치된 } PC\text{대수}}{\text{전체 } PC\text{대수}}) \times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (47)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	선행지표
통제목적	조직은 기본적인 보안 수준 확립을 위하여 신원 인증에 공인인증서를 이용해야 한다.		
지수화 방법론	$(\frac{\text{공인인증서를 이용하는 조직원의 수}}{\text{전체 조직원의 수}}) \times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (48)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	조직은 조직 내의 신속한 보안사고 대응을 위하여 조직원을 대상으로 보안 교육을 실시하여야 한다.		
지수화 방법론	$(\frac{\text{해킹 및 바이러스 신고 건수}}{\text{전체 } PC\text{대수}}) \times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (49)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	조직은 조직원 및 고객의 개인 정보가 유출되지 않도록 적절한 조치를 해야 한다.		
지수화 방법론	$(\frac{\text{개인정보침해신고건수}}{\text{전체조직원의수}})\times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (50)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	조직은 정보보호 업무만을 전담하는 정보보호 전문인력을 확보해야 한다.		
지수화 방법론	$(\frac{\text{정보보호전문인력의수}}{\text{정보통신인력의수}})\times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (51)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 스팸 메일 수신 비율을 이용한다.		
지수화 방법론	$(\frac{1계정당수신되는스팸메일수}{1계정당수신되는전체전자메일수})\times 100$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (52)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 피싱사고 발생 비율을 이용한다.		
지수화 방법론	$(\frac{조직내의피싱사고발생건수}{전체피싱사고발생건수})\times 100$		
참조	자체/apwg.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (53)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 봇넷 감염 비율을 이용한다.		
지수화 방법론	$(\frac{\text{봇넷에 감염된 } PC\text{대수}}{\text{전체 } PC\text{대수}}) \times 100$		
참조	자체/shadowserver.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (54)

지표구분	조직		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 DDoS 공격 발생 비율을 이용한다.		
지수화 방법론	$(\frac{\text{서비스거부공격 발생일수}}{365}) \times 100$		
참조	자체/shadowserver.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (55)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인식 및 훈련	지표성격	선행지표
통제목적	조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.		
지수화 방법론	$(\frac{\text{연간보안교육을이수한보안인력의수}}{\text{전체보안인력의수}})\times 100$		
참조	SP800-53 AT-3:Security Training		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (56)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인식 및 훈련	지표성격	후행지표
통제목적	조직의 보안 담당자들은 할당된 정보보호 관련 업무와 책임을 수행하기 위해 적절히 훈련되어야 한다.		
지수화 방법론	$(\frac{\text{국제정보보호자격증을취득한보안인력의수}}{\text{전체보안인력의수}})\times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (57)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인적 보안	지표성격	후행지표
통제목적	조직은 각 조직원이 직위와 책임에 부합하는 보안 기준을 만족하는지 확인해야 한다.		
지수화 방법론	$(\frac{\text{신원조사를 마친 조직원의 수}}{\text{정보자산에 접근 가능한 조직원의 수}})\times 100$		
참조	SP800-53 AC-2:Accout Management , PS-3:Personnel Screening		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (58)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인적 보안	지표성격	후행지표
통제목적	적격심사를 통과한 조직원의 경우라도 주요 자산에 대한 철저한 관리가 지속되어야 한다.		
지수화 방법론	$[1-(\frac{\text{보안문제를 야기한 조직원의 수}}{\text{적격심사를 통과한 조직원의 수}})]\times 100$		
참조	자체/ISMS, K-ISMS, G-ISMS, PIMS		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (59)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 예산
평가지표	보안 예산	지표성격	선행지표
통제목적	기업 정보 및 정보 시스템을 보호하기 위해 필요한 예산을 확보해야 한다.		
지수화 방법론	$(\frac{\text{조직의 정보보호 예산}}{\text{조직의 전체 정보화 예산}}) \times 100$		
참조	국가정보보호지수, NIST SP-800 55 rev.1 (SP-800 53 SA-2:Allocation of Resource)		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (60)

지표구분	조직		
평가분야	정보보호 환경	평가목적	정보보호 예산
평가지표	보안 예산	지표성격	후행지표
통제목적	기업 정보 및 정보 시스템을 보호하기 위해 필요한 예산을 확보해야 한다.		
지수화 방법론	$[1-(\frac{\text{역기능으로 인한 처리비용}}{\text{조직의 정보보호 예산}})] \times 100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (1)

지표구분	국가		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	취약점 관리	지표성격	후행지표
통제목적	국가의 전반적인 보안 수준 향상을 위하여 최신 OS 패치를 설치하여야 한다.		
지수화 방법론	$(\frac{\text{국가별 주요 } OS \text{ 취약점 패치 완료 건수의 합}}{\text{연간 발표된 주요 } OS \text{ 취약점 개수}}) \times 100$		
참조	자체/cert.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (2)

지표구분	국가		
평가분야	정보보호 구현	평가목적	정보보호 위험 제거
평가지표	유지 관리	지표성격	선행지표
통제목적	해킹 사고의 국제적 대응을 위해 국제 차원이 해킹 대응 훈련에 참가하여 정보교류 및 상호협력을 맺고 있어야 한다.		
지수화 방법론	$(\frac{\text{국제 보안 관련 컨퍼런스 참여 횟수}}{\text{최근 3년간 국제 보안 관련 컨퍼런스 개최 횟수}}) \times 100$		
참조	자체/first.org, cert.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (3)

지표구분	국가		
평가분야	정보보호 구현	평가목적	침해사고 대응
평가지표	사건 보고	지표성격	후행지표
통제목적	국가 차원의 신속한 보안사고 대응을 위하여 국민을 대상으로 보안 교육을 실시하여야 한다.		
지수화 방법론	$(\frac{\text{연간 해킹 및 바이러스 신고 건수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (4)

지표구분	국가		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 보유	지표성격	선행지표
통제목적	정보통신망의 안전성 및 정보통신설비 보호를 위해 정보보호시스템을 설치/운영함으로써 네트워크 보안을 강화한다.		
지수화 방법론	$(\frac{\text{정보보호 시스템의 개수}}{\text{인구수}}) \times 1000000$		
참조	정보보호 시스템 : 방화벽, IDS, IPS, 웹방화벽, DDoS 장비 자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (5)

지표구분	국가		
평가분야	정보보호 기반	평가목적	정보보호 시스템 도입
평가지표	정보보호 시스템 보유	지표성격	선행지표
통제목적	주요개인정보 전송시 비밀성과 무결성을 보장하는 보안서버구축 등의 조치를 적용해야 한다.		
지수화 방법론	$(\frac{\text{보안서버의 수}}{\text{인구수}})\times 1000000$		
참조	자체/oecd, wef, 국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (6)

지표구분	국가		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	시스템 및 통신 보안	지표성격	선행지표
통제목적	카드 거래 정보를 처리, 저장, 전송하는 가맹점 및 서비스 제공자는 데이터보안표준(PCI DSS)를 만족해야 한다.		
지수화 방법론	$(\frac{PCIDSS\text{를 준수하는 가맹점 수}}{\text{국가별 가맹점 수}})\times 100$		
참조	자체/신용카드사		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (7)

지표구분	국가		
평가분야	정보보호 기반	평가목적	보안 관리
평가지표	접근 통제	지표성격	선행지표
통제목적	정보 자산 및 정보 시스템을 보호/감시하기 위해 보안통제를 수행해야 한다.		
지수화 방법론	$(\frac{\text{국가별 공공기관 } CCTV \text{설치 대수}}{\text{인구수}}) \times 1000000$		
참조	자체/ISO 27001, K-ISMS, G-ISMS, 정보보호 안전진단, PIA		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (8)

지표구분	국가		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	선행지표
통제목적	기업들의 정보보호 관리체계 인증 현황을 파악하여 전반적인 국가의 정보보호 관리시스템 도입 현황을 파악한다.		
지수화 방법론	$(\frac{\text{국가별 } ISO\,27001 \text{ 인증 건수}}{\text{인구수}}) \times 1000000$		
참조	자체/ISO 27001		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (9)

지표구분	국가		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	선행지표
통제목적	국가는 안전한 인터넷 사용을 위하여 백신 프로그램 설치를 장려해야 한다.		
지수화 방법론	$(\frac{\text{백신프로그램이용자수}}{\text{인구수}})\times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (10)

지표구분	국가		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트폰 통제	지표성격	선행지표
통제목적	국가는 기본적인 보안 수준 확립을 위하여 신원 인증에 공인인증서를 이용해야 한다.		
지수화 방법론	$(\frac{\text{공인인증서이용자수}}{\text{인구수}})\times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (11)

지표구분	국가		
평가분야	정보보호 기반	평가목적	신기술 관리
평가지표	스마트그리드 통제	지표성격	후행지표
통제목적	스마트 그리드는 지속적인 전력 공급이 가능하도록 전력선 이중화나 우회 공급 경로를 확보해야 한다.		
지수화 방법론	$[1-(\frac{\text{국가별 정전 복구시간(분)}}{365\times1440})\times100$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (12)

지표구분	국가		
평가분야	정보보호 기반	평가목적	개인정보보호
평가지표	개인정보보호	지표성격	선행지표
통제목적	개인정보의 유출에 대비하여 각 나라가 합의한 OECD의 통일된 개인정보 보호지침을 준수해야 한다.		
지수화 방법론	$(\frac{OECD\text{개인정보보호준수한기관수}}{\text{전체기업 및 공공기관수}})\times100$		
참조	자체/oecd.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (13)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	국가는 국민의 개인 정보가 유출되지 않도록 적절한 조치를 해야 한다.		
지수화 방법론	$(\frac{\text{개인정보침해신고건수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (14)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보보호 수준	지표성격	후행지표
통제목적	사회전반으로 정보화 역기능 심각한 수준에 이르고 있어 국민의 보안의식을 파악할 수 있는 지표가 필요하다.		
지수화 방법론	$(\frac{\text{정보보호가중요하다고인식하는이용자수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (15)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 피싱사고 발생 비율을 이용한다.		
지수화 방법론	$(\frac{\text{국가별 피싱 사고 발생 건수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (16)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 봇넷 감염 비율을 이용한다.		
지수화 방법론	$(\frac{\text{국가별 봇넷 감염 건수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (17)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 스팸 메일 수신 비율을 이용한다.		
지수화 방법론	$(\frac{\text{국가별 스팸 메일 발생 건수}}{\text{인구수}}) \times 1000000$		
참조	자체/국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (18)

지표구분	국가		
평가분야	정보보호 환경	평가목적	보안의식 수준
평가지표	정보화 역기능 수준	지표성격	후행지표
통제목적	정보화 역기능 수준을 측정하기 위해 국가별 DDoS 발생 비율을 이용한다.		
지수화 방법론	$(\frac{\text{국가별 } DDoS \text{ 발생 건수}}{\text{전세계 } DDoS \text{ 발생 건수}}) \times 100$		
참조	자체/shadowserver.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (19)

지표구분	국가		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인식 및 훈련	지표성격	선행지표
통제목적	국가는 정보보호 인력 양성을 위하여 전문 교육기관에 투자를 해야 한다.		
지수화 방법론	$(\frac{\text{정보보호관련교육기관수}}{\text{인구수}})\times 1000000$		
참조	자체		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (20)

지표구분	국가		
평가분야	정보보호 환경	평가목적	정보보호 교육
평가지표	인식 및 훈련	지표성격	후행지표
통제목적	국가 및 조직은 정보보호 정책수립 및 이행을 위한 전문인력을 보유해야 한다.		
지수화 방법론	$(\frac{\text{국제정보보호자격증을취득한정보보호인력}}{\text{인구수}})\times 1000000$		
참조	자체/국가정보보호지수, cisa-isaca.org, cissp-isc2.org		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

설문 항목 (21)

지표구분	국가		
평가분야	정보보호 환경	평가목적	정보보호 예산
평가지표	보안 예산	지표성격	선행지표
통제목적	국가의 정보화 예산 중 정보보호 분야에 대한 예상이 얼마로 책정되어 집행되고 있는지를 확인한다.		
지수화 방법론	$(\frac{\text{정보보호관련국가예산}}{\text{인구수}}) \times 1000000$		
참조	국가정보보호지수		

설문 문항	적당	부적당
지표의 적합성 평가	1~9	X
①조직이나 각 국가에서 본 지표의 구현을 위해 **원시 데이터 수집이 가능한 지표**라고 생각하십니까?		
②본 지표가 **통제 영역**을 **대표할 수 있는 지표**라고 생각하십니까?		
③본 지표를 평가하기 위한 **지수화 방법**이 **적절**하다고 생각하십니까?		
④평가에 있어 본 지표를 **"필수/권고/선택/필요없음"** 으로 구분한다면 어떻게 선택하시겠습니까?		

[부록 3] Recommendation ITU-T X.csi: Guidelines for cybersecurity index

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 1332

English only

Original: English

Question(s): 4/17 Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source: Editor

Title: The 2nd revised text of Recommendation ITU-T X.csi: Guidelines for cybersecurity index

Summary

This TD is the 2nd revised text of Recommendation ITU-T X.csi which is an outcome document from the December 2010 SG17 meeting. It is based on discussion based on C345 and TD1157.

Contact: Heung Youl Youm
SoonChunhyang Univ.
Korea (Republic of)

Tel: +82 41 530 1328
Fax: +82 41 530 1494
Email: hyyoum@sch.ac.kr

draft Recommendation ITU-T X.csi

Guideline for cybersecurity index

1. Scope

The draft Recommendation is to provide a guideline to assist in the development, selection, and implementation of the measures or indicators that are basis to compute the CSI (Cybersecurity Index). To meet this objective, this draft recommendation provides a list of potential indicators and describes a methodology used in computing the CSI from indicators on its different steps.

2. References

The following ITU-T Recommendations and other references contain provisions that constitute the provisions of this Recommendation through referencing. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; thus, users of this Recommendation are encouraged to explore the possibility of applying the most recent editions of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly.

3. Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **Measurement**: Raw data that quantifies a single dimension of the thing to be measured. Raw data can be interchangeable with measurements.

3.1.2 **Metric**: Data processed from two or more measurements to demonstrate a significant correlation between them. It is interchangeable with an indicator.

3.1.3 **Measures**: Same as metrics

3.1.4 **Measurement**: The act of measuring

3.1.5 **Indicator**: It is interchangeable with metric.

3.1.6 security control : TBD

3.1 Terms defined in this Recommendation

3.2.1 Cybersecurity index : An index used to indicate the implementation of security controls as

defined which can be applied to information systems and cybersecurity programs and the state of cybersecurity in an organization or a community.

4 Abbreviations and acronyms

CVE Common vulnerability enumeration

CSI Cybersecurity Index

ICT Information and Communications Technology

IDS Intrusion Detection System

IPS Intrusion Prevention System

SSL Secure Socket Layer

TLS Transport Layer Security

WEF World Economic Forum

5 Conventions

<None>

6 Cybersecurity index

6.1 Introduction

Numerous efforts have been made to measure ICT performance, track progress, and evaluate the ICT effects for governments, operators, researchers, and industries in the use of ICT technology. Examples of these measures include the Development Index (DI) by International Telecommunication Union (ITU) and the Network Readiness Index (NRI) by World Economic Forum (WEF). However, there have been a few indices in the information security area, e.g. index on penetration of internet secure server which has been developed by WEF. However, it is only based on specific vendor's SSL or TLS certificates, resulting in lack of completeness which is required to cover all aspects of cybersecurity. The cybersecurity index can be computed from various indicators which are regarded as metrics to know the current state of performance of cybersecurity program and to evaluate the effectiveness and efficiency of security controls in an organization or a community.

6.2 General guidelines for cybersecurity index

This clause addresses general guidelines for cybersecurity index.

There may be need for some or all of the following;

- globally agreed-upon cybersecurity index,
- cybersecurity indicators that can be used to measure the current level of cyber security level or progress of the information security program in an organization or a community, especially for the developing countries,
- ensuring accuracy of raw data which are a basis to compute indicators,
- ensuring integrity of raw data which are a basis to compute indicators,
- indicators which can be used to help policy makers measure the performance of Information security policy and track progress of cybersecurity program, and
- considering fast changing ICT services and technologies and hacking technologies, when developing an indicator for a cybersecurity index.

6.3 Guidelines for selecting indicators for cybersecurity index

When selecting indicators, it may be necessary to select indicators to facilitate meeting goals and objectives of an organization or a community. In addition, the indicator should;

- measure major impact on performance results,
- measure aspects of cybersecurity in an organization or a community,
- be consisted of three types of indicators: system level, program level and both levels,
- measure progress of cybersecurity programs and implementation results of security controls in an organization and a community,
- measure progress in implementing cybersecurity programs, specific security controls, and associated cybersecurity policies and procedures,
- measure two aspects of security control implementation result in a security program: effectiveness and efficiency,
- measure the positive or negative impact of cybersecurity on an organization's mission or a community's common mission,
- measure status of progress and performance results applicable at the system level, the program level, or both levels, and
- measure positive and negative impact on the mission of an organization and a community and daily life of users.

Furthermore, the raw data should be accurate, reliable and collectible. In the whole measurement process, it is necessary to provide the integrity, privacy protection and availability of the raw data.

6.4 Classification of Indicators

There are three types of indicators: implementation, effectiveness/efficiency, and impact.

The implementation indicators are to demonstrate progress in implementing information security programs, specific security countermeasures, and associated security policies and procedures.

The effectiveness/efficiency indicators are to check if program-level processes and system-level security controls are implemented well, operating as intended, and satisfying the desired goals and objectives. They deal with two aspects of security control implementation results: the robustness of the result and timeliness of the result, i.e., the effectiveness addresses the robustness and the efficiency addresses the timeliness.

The impact indicators are to specify the impact of information security on mission of an organization or community. They are able to quantify the cost saving produced by information security program or through costs incurred from addressing information security incident, the degree of public trust obtained by the information security program, or other mission-related impacts of information security.

7 CSI development process

7.1 Introduction

A cybersecurity index should be regarded as a key toolkit which can be used to evaluate the performance of information security policy and figure out the current level of information security in an organization and a community. The following general steps could be applied to develop the global CSI;

- Identify the key indicators for construction of the index;
- Converting from absolute value to relative value;
- Converting the indicators to index value;
- Aggregate the index value;

8 Indicators for cybersecurity index

This clause describes various indicators which can be applicable to construct the cybersecurity index in an organization or a community. The indicators can be classified into three categories by the application level: mandatory indicator, recommended indicator, and optional indicator.

Indicator 1: Vulnerability management (program-level)

Field	Data
Indicator ID	Percentage of mitigated vulnerability
Goal	Organization should remove identified vulnerabilities on time.
Indicator	Percentage of vulnerabilities that have been mitigated within organizationally defined time frame.
Formula	$\left(\frac{Total\ number\ of\ vulnerabilities\ mitigated}{Total\ number\ of\ vulnerabilities\ identified}\right) \times 100$
Raw data	• The number of identified vulnerabilities during the time period • The number of mitigated vulnerabilities during the time period
Type	Effectiveness/**Efficiency**
Requirement level	Mandatory

Indicator 2: Audit (system-level)

Field	Data

Indicator ID	Percentage of PCs for which audit log is maintained
Goal	Organization should maintain system audit log to investigate inappropriate activities of users.
Indicator	Percentage of PCs for which audit log is maintained.
Formula	$\left(\frac{Total\ \ number\ \ of\ \ PCs\ \ with\ \ audit\ \ log}{Total\ \ number\ \ of\ \ PCs}\right) \times 100$
Raw data	• Number of PC for which audit log is maintained by a centralized log server or a PC • Total number of PC.
Type	Effectiveness/**Efficiency**
Requirement level	Mandatory

Indicator 3: Incident response (system-level and program level)

Field	Data
Indicator ID	Incident response
Goal	Organization should report incidents on time for every incident category.
Indicator	Percentage of incident reported within required time frame per applicable category
Formula	$\left(\frac{Number\ of\ incidents\ \ reported\ \ on\ time}{Total\ \ number\ of\ reported\ \ incidents}\right) \times 100$ for every category
Raw data	• Number of incidents reported within defined time frame • Total number of incident reported
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 4: Security patch program deployment (system-level)

Field	Data
Indicator ID	Security patch program
Goal	PCs should deploy security patch program for mitigating vulnerabilities of user's PCs.
Indicator	Percentage of PCs that deploys patch management system
Formula	$\left(\frac{Number\ \ of\ \ PCs\ employing\ \ security\ \ patch\ program}{Total\ \ number\ \ of\ \ PCs}\right) \times 100$
Raw data	• Total number of PCs deploying security patch program • Number of PCs
Type	**Effectiveness**/efficiency

Requirement level	Mandatory

Indicator 5: Antivirus program deployment (system-level)

Field	Data
Indicator ID	Antivirus program
Goal	PCs should deploy antivirus program for mitigating virus residing in user's PCs.
Indicator	Percentage of PCs that deploys antivirus program
Formula	$\left(\frac{Number\ of\ PCs\ employing\ \ antivirus\ program}{Total\ \ number\ of\ PCs}\right) \times 100$
Raw data	• Total number of PCs deploying s antivirus program • Number of PCs
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 6 Contingency planning (program-level)

Field	Data
Indicator ID	Contingency Plan Testing
Goal	Information system should conduct contingency plan testing.
Indicator	Percentage of information systems that have conducted contingency plan testing.
Formula	$\left(\frac{Number\ of\ information\ \ system\ \ that\ have\ conducted\ \ Contingency\ \ plan\ \ Testing}{Total\ \ number\ of\ information\ \ systems}\right) \times 100$
Raw data	• Number of information system that have conducted contingency plan testing
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 7: Security assessment (program-level)

Field	Data
Indicator ID	Percentage of information system with security assessment approval
Goal	Organization's information system should be certified and accredited prior to deployment
Indicator	Percentage of new information systems that have completed certification and accreditation prior to their deployment.
Formula	$\left(\frac{Number\ of\ information\ \ system\ s\ have\ been\ completed\ \ C\&A}{Total\ \ number\ of\ New\ System\ \ s}\right) \times 100$

Raw data	• Number of new information systems that have completed certification and accreditation
Type	**Effectiveness**/efficiency.
Requirement level	Mandatory

Indicator 8: Security pledge (program-level)

Field	Data
Indicator ID	Security pledge (rule of behaviour)
Goal	Employees who are authorized access to information systems should sign a security pledge before accessing to information system of an organization.
Indicator	Percentage of information system security personals who have signed security pledge
Formula	$\left(\frac{Number\ of\ personnels\ \ who\ are\ granted\ \ system\ \ access\ \ after\ \ signing\ \ rules\ \ of\ behavior}{Total\ \ number\ of\ personnels\ \ authoeized\ \ to\ access\ \ information\ \ system}\right) \times 100$
Raw data	• Number of employees who are granted system access after signing security pledge
Type	Implementation
Requirement level	Mandatory

Indicator 9: Remote access control (system/program)

Field	Data
Indicator ID	Protected remote access points
Goal	Organization should deploy firewall or web-application firewall to provide protected remote access in order to protect organization's internal assets.
Indicator	Percentage of protected remote access points
Formula	$\left(\frac{Number\ of\ remote\ \ access\ \ points\ \ that\ use\ \ firewall\ \ or\ web-apptation\ \ firewals}{Total\ \ number\ \ of\ remote\ \ access\ \ points}\right) \times 100$
Raw data	• Number of protected remote access points that use firewall or web-application firewalls.
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 10: Remote access control (system/program)

Field	Data

Indicator ID	Protected remote access points
Goal	Organization should deploy IDS or IPS to provide protected remote access in order to protect organization's internal assets.
Indicator	Percentage of protected remote access points
Formula	$\left(\frac{Number\ of\ remote\ access\ points\ that\ employ\ IDS\ or\ IPS}{Total\ number\ of\ remote\ access\ points}\right) \times 100$
Raw data	• Number of protected remote access points that uses IDS or IPS.
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 11: Wireless access control (system/program)

Field	Data
Indicator ID	Protected wireless access points
Goal	Organization should provide protected wireless access points to protect interior network from unauthorized access.
Indicator	Percentage of protected wireless access points
Formula	$\left(\frac{Number\ of\ protected\ wireless\ access\ point\ s}{Total\ number\ of\ Wireless\ access\ point\ s}\right) \times 100$
Raw data	Number of protected wireless access points
Type	**Effectiveness**/efficiency
Requirement level	Mandatory

Indicator 12: Link redundancy (system)

Field	Data
Indicator ID	Percentage of network link with redundancy
Goal	Organization should construct redundancy link of main network to guarantee the availability and continuity of organization's services.
Indicator	Percentage of network link with redundancy
Formula	$\left(\frac{Number\ of\ redundancy\ link\ s}{Total\ number\ of\ network\ device\ s}\right) \times 100$
Raw data	• Number of redundancy links for routers, DNS, DHCP, Firewall, or DB
Type	**Effectiveness**/efficiency
Requirement level	Recommended

Indicator 13: Personnel security (system-level/program-level)

Field	Data
Indicator ID	Personnel security screening
Goal	Organization should permit only authorized personnel to access to information and information system.
Indicator	Percentage of individuals screened before being granted access to organization's information and information systems.
Formula	$\frac{Number\ of\ individuals\ screened}{Total\ number\ of\ individuals\ with\ access} \times 100$
Raw data	• Number of individuals
Type	Implementation
Requirement level	Mandatory

Indicator 14: PII protection (system/program)

Field	Data
Indicator ID	Percentage of protected personal identifiable information
Goal	Organization should protect organization's personal identifiable information in a safe way.
Indicator	Percentage of protected personal identifiable information
Formula	$\left(\frac{Number\ of\ protected\ personal\ identifiable\ information}{Total\ number\ of\ personal\ identifiable\ information}\right) \times 100$
Raw data	• Number of protected personnel identifiable information
Type	**Effectiveness**/efficiency and i**mplementation**
Requirement level	Mandatory

Indicator 15: Back-up data protection (system/program)

Field	Data
Indicator ID	Rate of integrity inspection of backup data
Goal	Organization should provide integrity protection for the backup data
Indicator	Percentages of integrity-protected backup data
Formula	$\left(\frac{Amount\ of\ integrity\ -\ protected\ backup\ data}{Total\ amount\ of\ bakcup\ data}\right) \times 100$
Sampling	• Amount of integrated-protected backup data.
Type	**Effectiveness**/efficiency and i**mplementation**

Requirement level	Recommended

Indicator 16: Information Security management System Coverage (system/program)

Field	Data
Indicator ID	ISMS coverage
Goal	Organization's information system should be certified by ISMS.
Indicator	Percentage of information systems covered by the certified information security management system.
Formula	$\left(\frac{Number\ of\ information\ system\ s\ covered\ by\ certified\ ISMS}{Total\ number\ of\ information\ systems}\right) \times 100$
Raw data	Number of information systems covered by certified ISMS
Type	**Effectiveness**/efficiency and **implementation**
Requirement level	Mandatory

Indicator 17: Secure server deployment (system-level/program-level)

Field	Data
Indicator ID	Secure server deployment
Goal	Organization's web sites should use secure tunnel for remote access.
Indicator	Percentage of website that uses a secure tunnel, e.g. TLS, SSL, secure shell.
Formula	$\left(\frac{Number\ of\ web\ sites\ that\ use\ secure\ tunnel}{Total\ number\ of\ web\ sites}\right) \times 100$
Raw data	• Number of web sites that use secure channel • Total number of web sites
Type	**Effectiveness**/efficiency and **implementation**
Requirement level	Mandatory

Indicator 18: Spam receipt ratio (program)

Field	Data
Indicator ID	Spam Receipt Ratio
Goal	Organization should use the spam filter to block the spam mails to the employees.
Indicator	Percentage of employees that have received more than organization defined number of spam mails during the defined time frame.
Formula	$\left(\frac{Number\ of\ employees\ have\ received\ certain\ amount\ of\ spam\ mails}{Total\ number\ of\ employees}\right) \times 100$

Raw data	• Number of employees that received spam mails exceeding the organization defined numbers during the defined time frame.
Type	**Effectiveness**/efficiency and **implementation**
Requirement level	Mandatory

Indicator 19: Employee's awareness level for spam mails (program)

Field	Data
Indicator ID	User's awareness level for Spam
Goal	Users should not open the spam mail and attached file in the spam mail from unknown source.
Indicator	Percentage of employees who open the spam mail or attached file.
Formula	$\left(\frac{Number\ of\ employees\ \ who\ open\ \ spam\ \ or\ attached\ files}{Total\ \ number\ of\ employees}\right) \times 100$
Raw data	• Number of users who open the spam mail or attached files.
Type	**Effectiveness**/efficiency and **implementation**
Requirement level	Mandatory

Indicator 20: Awareness and training (program-level)

Field	Data
Indicator ID	Awareness and training
Goal	Organization's employees should complete security training and education in order to response to security incidents in proper way.
Indicator	Percentage of employees who have completed the security training and education during an organizationally defined time frame.
Formula	$\left(\frac{Number\ of\ employees\ \ that\ completed\ \ security\ \ training\ and\ education}{Total\ \ number\ of\ employees}\right) \times 100$
Raw data	• Number of employees that have completed training and education.
Type	Impact/Implementation
Requirement level	Mandatory

Indicator 21: Cybersecurity role and responsibility (program-level)

Field	Data
Indicator ID	Information security personnel
Goal	Organization should recruit and organization cybersecurity response team.

Indicator	Percentage of personnel that are related to information security.
Formula	$\left(\frac{Number\ of\ staffs\ \ that\ are\ related\ \ to\ cybersecurity\ \ activities}{Total\ \ number\ of\ IT\ staffss}\right) \times 100$
Raw data	• Number of staff that are related to cybersecurity activities
Type	Impact/Implementation
Requirement level	Mandatory

Indicator 22: Malware infection (program-level and system-level)

Field	Data
Indicator ID	Malware infected PCs
Goal	Employees' PCs should be protected from various malwares.
Indicator	Percentage of employees' computer that have been infected with virus or malware or compromised from attackers using hacking technologies to all computers.
Formula	$\left(\frac{Number\ of\ PCs\ that\ have\ been\ infected\ \ wth\ malware}{Total\ \ number\ of\ PCs}\right) \times 100$
Raw data	• Number of PCs that have been infected with virus or malware or compromised from attackers using hacking technologies to all computers.
Type	Impact and Effectiveness
Requirement level	Mandatory

Indicator 23: Personal information leakage (program-level)

Field	Data
Indicator ID	Personal information leakage
Goal	Employees' personal information should not be leakaged.
Indicator	Percentage of employees that have experienced leakage of personal information during a defined time frame.
Formula	$\left(\frac{Number\ of\ employees\ \ that\ have\ experienced\ \ personal\ \ information\ \ leakage}{Total\ \ number\ of\ employees}\right) \times 100$
Raw data	• Number of employees that have experienced leakage of personal information during a defined time frame.
Type	Impact
Requirement level	Mandatory

Indicator 24: Digital certificate usage (program-level and system-level)

Field	Data

Indicator ID	Digital certificate usage
Goal	When being authenticated and identified, employees should use strong authentication method such as digital certificates.
Indicator	Percentage of employees that have issued digital certificates from TTP for authentication, identification, and non-repudiation service.
Formula	$\left(\frac{Number\ of\ employees\ \ that\ have\ issued\ \ digital\ \ certificates}{Total\ \ number\ of\ employees}\right) \times 100$
Raw data	• Number of employees that have issued digital certificates during a defined time frame.
Type	Impact
Requirement level	Mandatory

Indicator 25: Bot infection (system-level)

Field	Data
Indicator ID	Percentage of PCs that are infected with Bot
Goal	Organization should be protected from bots attacks.
Indicator	Percentage of PCs that have been infected with bots in organization.
Formula	$\left(\frac{Number\ of\ PCs\ that\ have\ been\ infected\ with\ bot}{Total\ \ number\ of\ PCs}\right) \times 100$
Raw data	• Number of PCs that have been infected with bots.
Type	**Effectiveness**/Efficiency.
Requirement level	Recommended

Indicator 26: DDoS measures (system-level)

Field	*Data*
Indicator ID	*DDoS measure*
Goal	*Organization should protect information system against DDoS (or DoS) attacks during the organizationally defined time frame.*
Indicator	*Percentage of web sites that have been shut down from DDoS (DoS) attacks*
Formula	$\left(\frac{Number\ of\ web\ sites\ \ that\ have\ been\ \ shut\ down\ from\ \ DDoS\ attacks}{Total\ \ number\ of\ web\ sites}\right) \times 100$
Raw data	• *Number of web sites that have been shut down from DDoS attacks*
Type	***Effectiveness**/Efficiency*
Requirement level	Optional

Indicator 27: Security budget (program-level)

Field	*Data*
Indicator ID	*Percentage of organization's information security budget to ICT budget*
Goal	*Organization should provide resources for cybersecurity.*
Indicator	*Percentage of organization's information security budget to ICT budget*
Formula	$\left(\frac{Cybersecurity\ \ budget}{Total\ \ ICT\ \ budget}\right) \times 100$
Raw data	• *Amount of cybersecurity budget*
Type	***Impact***
Requirement level	Mandatory

9 Measurement implementation

10 Methodology for Cybersecurity Index

Annex A

Example of information security index and metrics

(This annex forms an integral part of this Recommendation)

This annex gives examples of use case of information security index and metrics which could be used to compute the cybersecurity index.

The National Information Security Index was developed and put in place since 2003 in Korea. Its aim is to evaluate the current state of performance of information security policy and security controls at the country level and help policy makers in identifying gaps between current level and desired target and developing the further information security policies. There are twelve possible indicators which can be grouped into three categories:

- Indicators for information security infrastructure;

  - ✓ Percentage of users deploying antivirus vaccine program s to Internet users.
  - ✓ Percentage of users deploying security patch programs to Internet users.
  - ✓ Percentage of users using public certificates to Internet users.
  - ✓ Percentage of enterprises deploying firewall to all enterprises.
  - ✓ Percentage of enterprises deploying IDS/IPS to all enterprise.
  - ✓ Number of secure servers deployed per a million people.

- Indicators for information security environment;

  - ✓ Percentage of amount of information security budget to ICT budget at the country level.
  - ✓ Percentage of employees involved for information security to ICT staffs at enterprise level.
  - ✓ Percentage of users with security awareness/training to Internet users.

- Indicators for negative impacts;

  - ✓ Percentage of user's computer infected with virus or malware or compromised from attackers using hacking technologies to all users computers.
  - ✓ Percentage of users who have experienced leakage of personal information to all users .
  - ✓ Percentage of users who have received SPAM mail to Internet users.

NIST published the Special Publication 800-55 Revision 1, *Performance Measurement Guide for information security*. It provides nineteen potential candidates of system level and program level metrics which can be grouped into those at following three levels;

- Metrics of system level

  - ✓ Access control
  - ✓ Audit and accountability

- ✓Identification and authentication
- ✓Maintenance
- ✓Risk assessment

- Metrics of program level

  - ✓ Security budget, vulnerability management,
  - ✓ Awareness and training
  - ✓ Certification, accreditation, and security assessments
  - ✓ Configuration management
  - ✓ Contingency planning
  - ✓ Physical environment

- Metrics of program level and system level

  - ✓ Incident response
  - ✓ Media protection
  - ✓ Planning
  - ✓ Personal security
  - ✓ System and communication acquisition
  - ✓ System and information integrity

Appendix I

Example of methodology

(This annex does not form an integral part of this Recommendation)

This appendix describes an example for the methodology used in ICT Development Index. This methodology includes principal components analysis (PCA) to eliminate indicators that have less influence on the index calculation.

Result of the Principal Components Analysis shows that raw data are highly correlated with other indicators and informs that some indicators are not essential to include in a particular category. In other words, Principal components analysis (PCA) will be carried out to analyse raw data, to explore whether the different dimensions are statistically well-balanced and to reveal how different indicators are associated and change in relation to each other.

I.1 Principal Components Analysis (PCA) The main objective of running multivariate analysis, such as Principal Components Analysis (PCA), is to analyse carefully the underlying nature of the data used in the index. PCA is a multivariate analysis tool for reducing multidimensional data sets to lower dimensions for analysis. It is done by calculating combinations of the underlying data that contains most of the information. PCA is applied to explore whether the different dimensions are statistically well-balanced and to reveal how different indicators are associated and change in relation to each other. PCA helps in determining the most important indicators to be included in each of the sub-indices by identifying those that are statistically "similar".

This type of analysis is important for reducing the number of variables (and achieving the goal of having a rather simple index) while retaining as much of the original information as possible. PCA is performed for ICT access, use and skills indicators using the Statistical Package for the Social Sciences (SPSS). Those characteristics of the data set (variables) that contributed most to its variance are retained, by keeping principal components, which usually contain the most important aspects of the data.

Before running the statistical analyses, the countries to be included in the index were defined based on data availability. The data set was prepared and cleaned, to avoid including missing data.

Before running the PCA, Bartlett's test of sphericity is performed to find out whether the indicators initially chosen are correlated. Results confirmed that some of the indicators are indeed correlated, hence the need of performing PCA. PCA involves the examination of the correlation matrix and the extraction of the principal components. The results/outputs derived from PCA include three main elements: eigenvalues, the percent (%) of variance explained in each component and the rotated component loadings. Eigenvalues represent the relative importance of the components – components with high eigenvalues and which explain the maximum variance are retained.

I.2 Weighting and aggregation

In choosing the weights, the results of the Principal Components Analysis (PCA) were taken into consideration. As explained above, PCA identifies the relative importance of the indicators selected in each category. It assigns a relative weight to each indicator.

The results derived from the PCA are particularly the component loadings (derived using varimax rotation). The weights are computed by performing the following steps in "For further details on the methodology", OECD and European commission 2008:

- The component loadings were squared and divided by the share of variance explained by the component.

- The results were then multiplied by the ratio of the variance explained by the component and total variance. These results are then associated as the participation (weights) of each variable in the total components taken into account.

- The derived weights were rescaled to sum up to 100 (to increase comparability).

The three steps are performed for the access, use and skills sub-indices.

The respective weights derived from the PCA helped in identifying the relative importance of each indicator. Although not directly applied to the indicators, they provided guidance on assigning the weights. Since no major differences were found among weights in each category, and in order to keep the methodology as simple as possible, it was decided to assign the same weight to indicators in the same category.

I.3 Calculating the idex

Sub-indices are computed by summing up the weighted values of the indicators included in the respective category. The values of the sub-indices are calculated by Formula of each measure. The sub-index value iscalculated by taking the simple average (using equal weights) of the normalized indicator values. For the final index computation, sub-indices of 3 categories are given certain per cent weight each. The final index value was then computed by summing up the weighted sub-indices.

I.4 Sensitivity analysis

Sensitivity analysis was carried out to investigate the robustness of the index results, in terms of the relative position in the overall ranking, using different combinations of methods and techniques to compute the index.

Potential sources of variation or uncertainty can be attributed to different processes employed in the computation of the index including the selection of individual indicators, the imputation of missing values, weighting and aggregation.

The tests computed the possible index values and country rankings for different combinations of the processes mentioned above. Results show that while the computed index values change, the overall message remains the same. The index was found to be extremely robust to different methodologies – with the exception of some countries, particularly countries in the "high" group.

The relative position of countries included in the "high" group can change somewhat depending on the methodology used. Therefore, conclusions based on the ranking of these countries should be made with caution. On the contrary, the relative position of countries included in the "middle" and "low" groups is in no way affected by the methods or techniques applied. Countries in these groups ranked similar in all index computations (using different methodologies). This confirms the results conveyed by the X.csi.

1. 본 연구보고서는 방송통신위원회의 출연금 등으로 수행한 방송통신정책연구용역사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 방송통신위원회 방송통신정책연구용역사업의 연구결과임을 밝혀야 합니다.