정 보 보 호 학 회 지
제28권 제6호, 2018. 12

국제표준에 따른 정보보호관리체계 전문가 인증 방안

오 경 희*

요 약

2017년 국제 정보보호관리체계 전문가에 대한 자격 기준인 ISO/IEC 27021 표준이 발표되었다. 이 기준을 만족하는 ISMS 전문가를 인증하기 위해서는 인증스킴과 인증기관으로 이루어지는 인증체계가 필요하지만, 국내의 인증 체계는 ISO에서 인정하는 사람에 대한 인증 요구사항을 만족하기 어렵다.

이 논문에서는 ISO/IEC 27021의 요건을 만족하는 인증된 ISMS 전문가를 배출하기 위해 필요한 사항들을 살펴보고 인증 스킴의 개발 방법과 전문가 인증 방안을 검토한다

Ⅰ. 서 론

2017년 국제 정보보호관리체계(Information Security Management System, ISMS)를 수집, 구현, 유지, 개선하는 업무를 수행하는 전문가에 대한 자격 기준인 ISO/IEC 27021[1] 표준이 발표되었다. 이 표준은 ISMS 표준 시리즈를 개발하는 ISO/IEC JTC 1/SC 27 WG 1에서 개발되었다.

ISMS 인증심사를 수행하는 심사원 자격에 대한 기준은 ISMS 인증 기관에 대한 요구사항을 정의하는 ISO/IEC 27006에 포함되어 있다. 그러나 인증심사원에게는 결과를 평가하는 지식과 기량은 요구되지만 ISMS 체계를 수립하고 운영하기 위한 지식과 기량은 요구되지 않고 있다.

시장에서는 전세계적으로 고급의 정보보호 인력의 수요가 높아지고 있었으며 특히 ISO/IEC 27001에 따른 정보보호관리체계를 수립, 구축, 운영, 개선하기 위해서는 좀 더 경영시스템의 수립 및 운영에 관한 조직적, 인적, 업무적 측면에 대한 이해가 강조되어야 한다는 요구가 높았다. ISO/IEC 27021은 이러한 요구를 만족시키기 위하여 개발되었다.

그러나 ISO/IEC 27021 표준은 ISMS 전문가에 대한 자격 기준만을 명시하고 있으며, 이러한 기준을 만족하는 전문가를 배출하기 위해서는 이 기준에 따라 전문가를 인증하는 인증 기관과, 그 인증기관에서 활용하기 위한 인증 기준이 필요하다. 이 논문에서는 이러한 요구사항을 검토하고, 국제 표준에 따른 정보보호관리전문가를 배출하기 위한 방안을 설명한다.

Ⅱ. 정보보호관리체계 전문가 자격 요건 표준

2.1. 개발 경과

2012년 스웨덴의 정보보호관리 전문가에 대한 인증제도 수립이 발표되었고, 이에 여러 국가에서 심사원이 아닌 실무 전문가의 인증 필요성에 공감함으로써 정보보호관리 전문가의 국제 인증(International Certification of Information Security Management Specialists)에 관한 연구기간(study period, SP)이 개시되었다.

이 SP는 스웨덴, 한국, 일본의 주도로 1년간 진행되어 정보보호 전문가에 대한 기존의 국제 자격제도 및 표준 현황을 조사하고 ISO/IEC 27000 시리즈에 기초하여 정보보호관리체계를 구축, 운영하기 위한 전문가 자격제도가 필요한지의 여부를 조사하였다.

2013년 ISO/IEC 27021 개발이 결의되고 SP에서 라포처로 활동한 한국의 오 경희, 일본의 Yonoske

1) SC27 심의위원회는 이전에는 information security management system을 "정보보안경영시스템"으로 번역하였으나 2018년부터 국내 법의 용어를 따라 "정보보호관리체계"로 통일하기로 결정하였음. 이에 따라 기존 ISMS 표준을 개정 중에 있음

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(정보보안경영전문가 자격기준 국제표준화)

* TCA 서비스 대표 (khoh@tcaservices.kr)

Harada와 영국의 Andreas Fuchsberger가 에디터로 임명되었다. 그러나 ISO/IEC JTC 1의 승인 단계에서 IEC가 인증 스킴의 소유권 문제 및 표준 개발 권한에 관한 문제를 제기함으로써 1년간 SP가 연장되었다.

연장된 SP 과정에서는 ISO와 IEC 각각에서 인증제도를 담당하는 기구인 CASCO (Committee on conformity assessment)와 CAB (Conformity assessment body)이 참여하여, 이러한 신규 인증 제도가 만들어진다면 어떤 기구가 소유권을 가지고 인증 제도를 운영할 것인지, 인증 관련 표준 개발에서 ISO/IEC JTC 1 SC 27/WG 1의 작업 권한은 어떤 것인지에 관한 논의가 이루어졌다.

최초의 제안은 ISO/IEC 27006과 같은, 정보보호 전문가를 인증하기 위한 요구사항을 개발하는 것이었다. 그러나 이러한 요구사항은 인증 스킴을 구성하는 것이며, 인증 스킴은 인증기관 또는 인정기관이 개발/참조해야 하는 문서로서 ISO 적합성 평가 표준의 중립성 원칙을 위배한다는 점이 지적되었다.

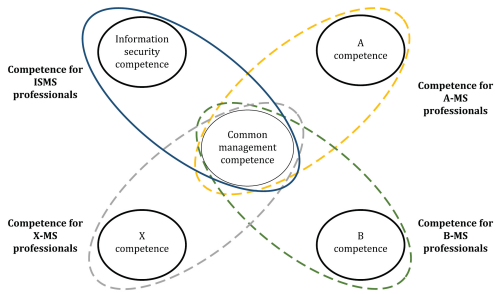
ISO의 적합성 평가 위원회인 CASCO가 2012년 발행한 적합성 평가 표준의 개발자 안내서[2]에서는 표준 개발자는 “중립 원칙(Neutral principal)”에 따라 제1자(제조자 또는 공급자), 제2자(사용자 또는 구매자), 제3자(인증기관과 같은 독립 기관) 모두에게 적용될 수 있는 문서를 개발해야 한다고 규정하고 있다. 이에 따르면 제3자 기관이 주로 참조하게 되는 인증 스킴에 관한 문서는 SC 27의 개발 권한 범위를 넘어서는 것이다. 이에 따라 SC 27에서는 인증 스킴에 대한 문제는 ISO/CASCO와 IEC/CAB, 또는 각 국의 인증체계의 결정사항으로 남겨 두고, 제1자, 2자, 3자가 모두 활용할 수 있는 내용을 선정하여 “정보보호관리체계 전문가 자격 요건”으로 범위를 변경하였다.

이 표준에서 규정하는 정보보호관리체계 전문가의 자격 요구사항은 제1자인 전문가 및 전문가 양성 교육기관에서도, 제2자인 정부기관, 보안 전문회사, 보안직원을 채용하고자 하는 수요기관 등에서도, 그리고 제3자인 전문가를 인증하기 위한 인증기관과 그 인증기관을 인정하는 인정기관에서 모두 활용할 수 있어 ISO Directive의 중립원칙을 만족할 수 있다.

2.2. 표준의 내용

ISO 표준에서 자격(competence)이란 “의도한 결과를 성취하기 위해 지식과 기량(skill)을 적용하는 능력”이라고 정의하고 있다.[3]

ISMS 전문가가 보유해야 할 자격은 환경, 품질, 의료 등 모든 분야의 관리체계에 공통적으로 필요한 업무 관리 관련 자격(business management competence)과 정보보호 분야의 업무 수행을 위한 자격(information security competence)으로 나누어 질 수 있다. ISO/IEC 27021 표준에서는 5장에서 업무 관리 자격을, 6장에서는 정보보호 자격을 설명하고 있다. (그림 1)은 ISO 표준에서 각 분야별 자격의 구성을 보여준다. [표 1]은 업무 관리 자격의 항목을, [표 2]는 정보보호 자격의 항목



〔그림 1〕 분야별 관리체계 전문가 자격 구성〔1〕

〔표 1〕 ISO/IEC 27021 업무 관리 자격

번호	자격 명
1	리더십
2	의사소통
3	사업전략과 ISMS
4	조직 설계, 문화, 행동 및 이해관계자 관리
5	프로세스 설계 및 조직의 변화 관리
6	인적자원, 팀 및 개인 관리
7	위험 관리
8	자원 관리
9	정보시스템 아키텍처
10	프로젝트 및 포트폴리오 관리
11	공급자 관리
12	문제 관리

을 보여준다.

각각의 세부적인 자격은 의도한 결과, 필요한 지식, 필요한 기량의 측면에서 자격을 서술하는 구조를 갖는다. 또한 이 자격은 ISMS를 수립, 구축, 운영, 개선하는 전문가를 위한 것이기 때문에, 각 자격마다 ISO/IEC 27001 세부 조항과의 연결성을 명시하고 있다.

부록에서는 ISMS 지식 체계(body of knowledge) 개발의 일환으로써 각 항목 별 지식 키워드를 제공하고 있다.

〔표 2〕 ISO/IEC 27021 정보보호 자격

번호	자격 명	번호	세부 자격
1	정보보호	1	정보보안 거버넌스
		2	조직의 상황
2	정보보호 계획	1	ISMS 범위
		2	정보보호 위험 평가 및 처리
3	정보보호 운영	1	정보보호 인식, 교육 및 훈련
		2	문서화
4	정보보호 성과평가	1	ISMS 모니터링, 측정, 분석 및 평가
		2	ISMS 감사
		3	경영진 검토
5	정보보호 개선	1	지속적 개선
		2	기술 추세 및 개발

Ⅲ. 국제 정보보호관리 전문가 배출 방안

3.1. ISO 인정 체계

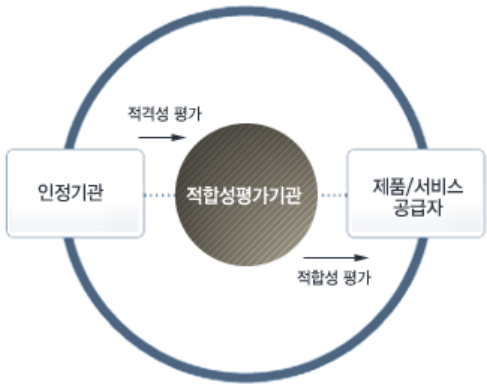
정보보호관리 전문가의 자격 요건은 마련되었으나 이 국제 표준에서 요구하는 자격을 갖춘 전문가를 배출하기 위해서는 인증 기관(Certification body)이 필요하다. ISO는 국가 별로 인정기관을 두고, 인정기관(Accreditation body)이 인증을 제공하는 인증기관을 인정하고 사후 관리를 수행하는 체계를 가지고 있다.

인증은 ISO 규격에서는 “적합성 평가(comformity assessment)”라는 용어로 표현되는데, 제품, 프로세스, 사람 또는 기관에 대한 규정된 요구사항 충족 여부를 실증하는 활동을 말하며, 시험, 검사, 제품 인증, 관리체계 인증, 사람에 대한 자격 인증 등을 포함한다. 이에 따라 인증 기관을 “적합성 평가 기관”, 인증 제도를 “적합성 평가 제도”라고 표현하기도 한다.

인정 기관은 적합성 평가 기관(시험소, 제품 인증 기관, 관리체계 인증 기관, 자격 인증 기관)이 국제 규격 또는 기준에 적합하게 운영되고 있는지를 평가하여 확인하고, 사후관리를 통하여 관리·감독한다. 즉 인증 제도의 신뢰성을 유지하고 보장하는 역할을 수행한다. 일반적으로 인정기관은 각 국 정부가 지정한다.

적합성 평가 기관은 제품, 프로세스, 서비스, 기관, 사람 등의 적합성 평가 대상에 대하여 국제규격 또는 기준이 규정한 요구사항에 적합한지를 평가하고 실증해 주는 기관이다. 규정된 요구사항의 적용대상이 관리체계인 경우 관리체계 인증, 사람인 경우 자격 인증이라고 부른다.

(그림 2)는 인정 기관과 “적합성평가기관‘으로 표현된 인증 기관의 관계를 보여주고 있다.[4]



〔그림 2〕 인정기관과 인증기관〔4〕

국내에서는 산업통상자원부 산하에 한국인정지원센터(Korea Accreditation Board, KAB)가 경영시스템 인증 및 자격인증 분야의 인정기관으로 활동하고 있다. 또한 경우에 따라서는 연수기관을 두어 자격 대상자에 대한 교육을 수행하도록 하고 있다.

3.2. ISO 인정 기준

자격인증기관에 대한 인정규격은 ISO/IEC 17024 적합성 평가 - 사람에 대한 인증을 제공하는 기관에 대한 일반 요구사항 (Conformity assessment - General requirements for bodies operating certification of persons[5]에서 정의하고 있다. [표 3]은 ISO 17024의 구조를 보이고 있다.

〔표 3〕 ISO 17024 구조

장	제목	절	소제목
1	범위		
2	참조 표준		
3	용어정의		
4	일반 요구사항	4.1	법적 문제
		4.2	인증에 대한 결정의 책임
		4.3	공평성 관리
		4.4	재정 및 법적 책임
5	구조적 요구사항	5.1	관리 및 조직 구조
		5.2	훈련에 관한 인증기관의 구조
6	자원 요구사항	6.1	일반 직원 요구사항
		6.2	인증 활동에 관련된 직원
		6.3	외주
		6.4	기타 자원
7	기록 및 정보 요구사항	7.1	응시자, 후보자 및 인증된 인력의 기록
		7.2	공개 정보
		7.3	기밀성
		7.4	보안
8	인증 스킴		
9	인증 프로세스 요구사항	9.1	응시 프로세스
		9.2	평가 프로세스
		9.3	시험 프로세스
		9.4	인증의 결정
		9.5	보류, 철회 또는 인증 범위의 축소
		9.6	재인증 프로세스
		9.7	인증서, 로고, 마크의 이용
		9.8	인증 결정에 대한 불복
		9.9	불만처리
10	관리체계 요구사항	10.1	일반
		10.2	일반 관리체계 요구사항
부록 A(정보성)		사람에 대한 인증 기관 및 그 인증 활동에 대한 원칙	

특히 ISO/IEC 17024의 8장에서는 각 인증의 범주에 대한 인증 스킴을 요구하고 있다. 인증 스킴은 다음과 같은 요소를 포함해야 한다.

a) 인증의 범위
b) 직무 및 업무 설명
c) 필요한 자격
d) 능력(필요한 경우)
e) 전제 요건 (필요한 경우)
f) 윤리 강령 (필요한 경우)

또한 인증 스킴은 다음과 같은 인증 프로세스 요구사항을 포함해야 한다.

a) 초기 인증과 재인증에 관한 기준
b) 최초 인증 및 재인증의 평가 방법
c) 감독 방법 및 기준(필요한 경우)
d) 인증의 보류 및 취소 기준
e) 인증의 범위 또는 수준의 변경 기준(필요한 경우)

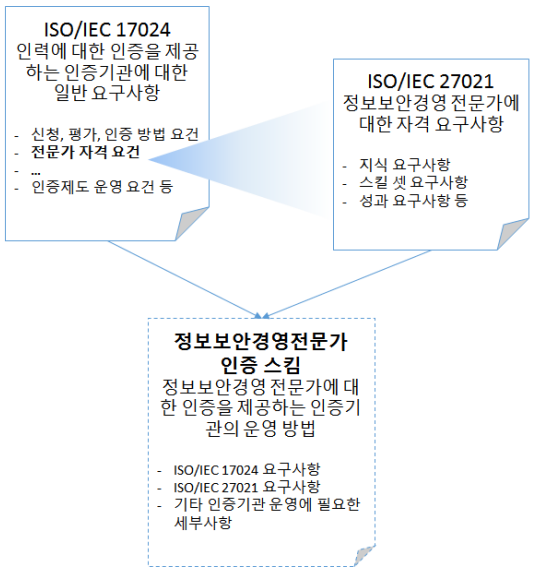
또한 인증기관은 인증 스킴의 개발과 검토 시

a) 적절한 전문가들의 참여
b) 공정한 구조
c) 필요한 경우, 전제조건과 자격요건
d) 평가 메커니즘과 자격 요건과의 연계
e) 직무 또는 실무 분석의 수행 및 갱신을 포함하여야 하며, 이를 확인할 수 있도록 문서화해야 한다.

또한 인증 스킴을 지속적이고 체계적으로 검토, 검증해야 한다.

즉, 위에서 보듯이 전문가의 자격은 ISO 17024에서 요구하는 한 요소이며, ISO/IEC 27021이 정의하고 있는 것은 정보보호관리체계 전문가를 인증하기 위한 전체 인증 스킴의 일부이다. 물론 이 자격 요건은 전제 조건 및 평가와 연계되어야 한다.

(그림 3)은 이러한 관련 표준의 관계를 보여준다.



〔그림 3〕 정보보호관리 전문가 인증 스킴을 위한 관련 표준의 관계

한편 ISO/CASCO와 IEC/CAB은 이 표준이 발행된 후 관련 업계의 반응에 기초하여 스킴 개발을 결정하기로 결정한 바 있다. IEC/CAB은 2016년 운영회의에서 신속한 적합성 수요 대응을 위해 CAB 체계를 전면 개편하고, 사이버 보안 분야 적합성 평가 대응을 위한 작업그룹(WG 17)을 신설하여 필요시 ISO/IEC 27021 관련 인증 스킴을 개시하려고 하고 있다.

3.3. 국내 인증 및 인정 체계와 ISO 체계의 차이

우리나라의 경우 정보보안 기사/산업 기사 자격이 존재하며, 정보보호기술사제도를 시행하려는 노력이 있었으나 중단된 바 있다.[6] 이러한 국내의 기존 자격 제도는 현재의 국제적인 인력에 대한 자격 기준이 요구하고 있는 직무분석, 재인증 등의 요구사항을 포함하고 있지 않아서 일반적인 국내 자격 제도는 ISO 17024 요건을 만족하지 못한다.

일본의 자격 제도 역시 우리나라와 마찬가지로 재인증을 요구하지 않고 있으므로 ISO 17024에 따른 국제 인증을 받을 수 없다. 일본은 자신들이 운영하고 있는 정보보안 기술사 자격을 이 표준에 따라 국제 인증을 받게 하는 것을 목표로 ISO/IEC 27021 개발에 적극적으로 참여하였으며 연구기간 동안 재인증을 포함하지 않는 “qualification” 개념을 신규 자격 표준에 도입하기 위하여 노력하였으나, 무산된 바 있다.

한편 우리의 기존의 정보보안 기사/산업 기사 자격의 내용은 ISO/IEC 27021 표준의 업무경영 자격을 모두 만족시키지는 못한다.

우리나라는 본 과제의 수립 및 진행과정에 적극적으로 참여하면서 2016년 초 발표된 ‘정보보호관리·운영‘ 국가직무능력표준[7]의 내용을 포함하도록 기고하였으며 대부분이 받아들여졌다. 그러나 국가직무능력표준 역시 ISO/IEC 27021 표준의 요구사항을 모두 포함하지는 못하고 있다.

3.4. 정보보호관리체계 전문가 배출을 위한 방안

ISO 17024 인증을 받은 기관의 경우 정보보호관리 전문가 자격을 포함하는 인증 스킴을 개발하여 운영하면 된다. ISACA의 CISA, ISC2의 CISSP 등 일부 국제 자격은 이미 ISO 17024에 따라 적격성을 평가 받은 제도들이다. 이들은 자신들이 제공하는 인증이 ISO/IEC 27021의 요건을 포함하고 있다는 것을 보이기만 하면 된다.

현재 이들의 지식체(Body of knowledge)는 각 기관이 자체적으로 개발한 것으로서 ISO/IEC 27021이 요구하는 정보보안 자격은 상당 부분 포함하고 있으나 업무 관리 자격에 포함된 사항들은 일부 미흡할 수 있다. 이들은 ISO/IEC 27021의 자격을 기존의 내용에 매핑하고 미흡한 사항들은 자신들의 지식 체계에 새롭게 포함시키는 작업이 필요할 것이다.

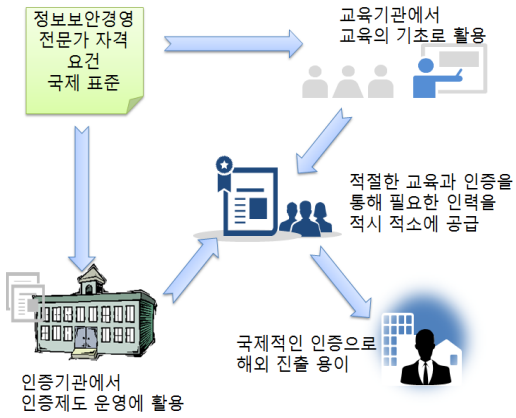
한편 ISO 17024 인증을 받지 못한 조직이 ISO/IEC 27021 표준에 따른 전문가 인증을 제공하기 위해서는 2가지 방안이 가능하다. 첫째는 ISO/IEC 27021 자격 내용을 포함하는 인증을 자체 선언하는 것이고, 다른 하나는 ISO/IEC 27021 및 17024의 요구사항을 포함하는 새로운 자격제도를 만들고 ISO의 인증을 받는 것이다.

이 두 방안은 각각 장단점이 있으므로 이해당사자들의 논의와 고려가 진행되어야 한다. 특히, 국내에서의 진행은 앞 절에서 설명한 ISO/CASCO와 IEC/CAB의 인증 스킴 개발에 관한 국제 동향을 검토하고 반영하면서 이루어져야 할 것이다.

국제 표준화 기구 수준에서 인증 스킴을 개발한다면 각 인증기관이 개별적으로 인증 스킴을 개발할 필요 없이 여기서 개발된 인증 스킴을 채택하여 운영하면 된다. 이 경우 국제 인증 체계가 더 단일화되면서 국제적인 정보보호관리 전문가 인증이 이루어질 수 있다. 물론 인증 기관은 자신의 인증 스킴을 개발하여 운영할 수 있으며 ISO 인정도 받을 수 있지만, 이미 시장을 확보한 자격이 아니라면 표준화 기관이 개발된 인증 스킴을 따르는 쪽이 더 유리할 것이다.

첫 번째 방안은 ISO로부터 객관적인 인증을 받지는 못하지만 기존 운영 중인 자격 요건을 대조하여 포함 여부를 확인하고 필요한 경우 자격 요건을 확장함으로써 우리의 자격이 ISO/IEC 27021에서 요구하는 자격을 모두 포함하고 있다고 주장하는 것이다. 이것은 현재의 자격 제도를 크게 수정하지 않고 좀 더 용이하지만 제3자에 의한 객관적인 적합성 평가를 거치지 않아 그 주장의 신뢰성을 보장하기 어려운 단점이 있다.

두 번째 방안은 객관적인 보증을 얻을 수 있지만 그 실현에 여러 가지 어려움이 있다. ISO/IEC 27021에서 요구하는 자격을 포함하는 인증 스킴을 개발해야 하며,



〔그림 4〕 ISO/IEC 27021 활용 방안

3.2절에서 설명한 바와 같이 ISO 17024에서 요구하는 여러 기준을 만족하도록 인증 기관을 운영해야 한다. 또한 주기적으로 ISO 인정기관의 심사와 사후관리를 받아야 하며 이에 따른 비용이 수반된다.

2013년 미래창조과학부는 정보보호 산업발전 종합대책의 일환으로 정보보안기술사 자격 도입을 추진한 바 있으나 시장 규모의 제한으로 인해 도입되지 않은 경험이 있다. 따라서 새로운 인증 기관을 수립하는 것은 재정적 어려움이 예측된다.

현재 보안 인력 시장에서는 기존의 국내·국제 보안 자격증이 활용되고 있으며, ISMS에 관해서는 인증심사원 자격이 활용되고 있다. 이러한 자격들이 실제 ISMS의 수립·운영 과정에 필요한 능력을 포괄하지 못하고 경영진의 업무를 충분히 지원하지 못한다고 보고있으나 자격증 자체에 대한 회의가 높은 것으로 보인다.

한편 자격 인증을 제공하지는 못하더라도 이 표준을 활용하여 국제 정보보호관리체계 전문가를 위한 교육 훈련을 제공하는 것은 가능하다. 교육 훈련기관들은 ISO/IEC 27021에서 요구하는 지식 내용을 제공하고, 지식과 기량을 발휘하여 각 자격에서 요구되는 결과를 달성하기 위한 훈련 과정을 개발할 수 있다. 이러한 과정과 ISO/IEC 27021의 지식과 기량을 매핑함으로써 교육 훈련의 질과 효과를 높이고 시장에서 차별화를 꾀할 수 있다. 이러한 교육 훈련은 제3자 인증은 받지 못하더라도 시장에서 필요로 하는 전문가 양성에는 큰 도움이 될 것이다.

Ⅳ. 결 론

ISO/IEC 27021을 개발한 SC 27의 전문가들은 정보보호관리 전문가들의 가장 큰 현안은 경영진의 관점에서 정보보호관리체계의 효과를 제시하고 지속적으로 보안에 투자할 수 있도록 경영진을 이끄는 것이라고 보았다.

국내외적으로 컨설턴트 또는 정보보호 관리 담당자 또는 책임자를 고용하고자 하는 조직에서 경험되는 문제점은 시장에서 사용되고 있는 전문 자격증을 획득한 인력을 고용하더라도 이들이 조직의 비즈니스를 이해하지 못하고, 경영진에게 정보보호의 필요성을 설득하는 데 한계가 있다는 점이다. 이러한 문제를 해결하기 위해서는 정보보호에 관한 전문 지식 뿐만 아니라 일반적인 업무 및 관리에 대한 이해와 지식, 의사소통 기량이 필요하다.

현재 시장의 정보보호 전문가 자격 제도들은 이러한 관리체계의 수립과 운영에 관한 실무를 수행하기 위한 지식과 기량, 결과물을 만들어내기 위해 소통하고 협력하는 과정보다는 정보보호를 위한 기술적 지식이나 정해진 양식에 따른 산출물을 평가하는 데 더 치우쳐 있다는 문제가 있다.

ISO/IEC 27021 정보보호관리 전문가 자격 요건 국제 표준은 정보보호 전문가들과 이들을 필요로 하는 수요자들에게 조직 내외에서 정보보호관리체계 수립·운영에 필요한 실제적인 능력을 식별하도록 하기 위해 개발되었다.

이를 가장 적절하게 활용하는 방법은 교육 훈련 기관에서는 이 기준에 따라 교육 훈련을 제공하고, 인증기관에서는 이를 활용하여 인증 스킴을 수립하고 전문가를 인증함으로써 검증된 전문가들을 필요한 수요기관이 선택할 수 있도록 제공하는 것이다.

국내 보안 전문가들은 국제 자격을 취득하기 위해 시험 및 자격 유지 비용을 지출하고 있어 이에 따른 국부 유출이 상당한 수준으로 평가되고 있다. 이러한 기존 국제 자격들이 ISO/IEC 27021 국제 표준을 따르는 국제 정보보호관리 전문가 자격으로 인정된다면 ISMS를 운영하는 수요 기관들에게는 국제 자격 취득자에 대한 선호 경향을 더 높일 수 있으며 외화 유출 측면에서 볼 때 아쉬운 부분이다.

최근에는 국내 기업들의 해외 지사 수립 등 국제 진

출이 활발하고 이에 따라 한 기업의 정보보호관리체계 범위가 해외로 확장 연결되는 경우들이 발생하고 있다. 이러한 활동들을 통해 해외 경험을 쌓고 국제 표준에 따라 적합성이 인증된 전문가들이 국제 시장에 진출하게 된다면 개인적으로나 국가적으로나 큰 이득이 될 것이다.

ISO 승인을 받는 정보보호관리 전문가 인증제도를 운영하는 것은 국내 정보보호 인력 시장의 규모 또는 관리상의 불편으로 인한 어려움이 예상된다. 그러나 이러한 어려움이 해소되지 못한다면 장기적으로는 해외 자격제도와의 선호 격차가 더 커질 수 있고, 그만큼 경제적 기회도 축소될 수 있다. 전극적인 고려가 필요한 시점이다.

참 고 문 헌

[1] ISO/IEC 27021:2017 Competence requirements for information security management systems professionals, ISO, 2017.

[2] ISO/CASCO, Conformity assessment for standards writers : Do's and dont's, ISO, 2012.

[3] ISO/IEC 17024:2012 Conformity assessment -- General requirements for bodies operating certification of persons, ISO, Dec. 2012.

[4] 한국인정지원센터, https://www.kab.or.kr/sys_guide/?CodeFlag=0001

[5] ISO/IEC 17024:2012 Conformity assessment -- General requirements for bodies operating certification of persons, ISO, Dec. 2012.

[6] 디지털타임스, 2016, "정보보안기술사 자격증 연내 도입 '불투명'", 2016. 11. 02

[7] 한국산업인력공단, 국가직무능력표준 직무명: 정보보호관리·운영, 2016. 02

〈저 자 소 개〉

오 경 희 (Kyeong Hee Oh)

1988년 8월 : 서강대학교 전산과 학사
1992년 2월 : KAIST 전산과 석사
2012년~현재 : TCA서비스 대표
2010년~현재 : 산업표준심의회 정보보호기술(ISO/SC27) 전문위원
2016년~현재: 산업표준심의회 표준회의 의원
2017년~현재 : 산업표준심의회 블록체인(ISO/TC 307) 전문위원
2013년~2017년 : ITU-T SG17 Q3 Associate rapportuer
2017년~현재: ITU-T SG17 Q14 Corapportuer
관심분야 : 정보보호관리, 블록체인, 아키텍처, IT 감사, 거버넌스, 통제