Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.973

개인정보영향평가의 문제점과 개선방안*

최 영 희,[1†] 한 근 희[2‡]
[1]건국대학교 정보통신대학원, [2]고려대학교 정보보호대학원

Problems and Improvement of Privacy Impact Assessment*

Young-hee Choi,[1†] Keun-hee Han[2‡]
[1]Graduate School of Information and Communications, Konkuk University,
[2]Graduate School of Information Security, Korea University

요 약

정보시스템에 수집·이용되는 개인정보에 대한 개인정보영향평가가 법적 근거에 의해 시행된 지 2016년으로 6년차가 된다. 이에 ITSM(Information Technology Service Management)의 3대 구성요소를 기준으로 운영상의 문제점을 분석하였다. 다양한 개인정보 처리시스템에 대한 평가자로써의 역할을 수행하면서 product에 해당하는 평가 보고서의 품질 향상 방안에 대해 주된 고민을 하였고, 평가 수행 시 적용하는 보고서의 형식적 타당성을 갖추기 위한 개선안을 평가 단계별 산출물 4종을 기준으로 제시하였다. 다음으로 people에 해당하는 평가수행자에게 요구되는 능력을 GRC(Governance, Risk, Compliance)로 인식하여 개선안을 제시하였고, process인 제도 운영에 관한 개선안도 부가하였다. 2011년 개인정보보호법 제정 시 명시한, 개인정보영향평가 완료 기한인 2016년 이후에도 실효성 있는 평가제도로 정착하기 위해서는 평가자·평가기관과 주관기관이 협력하여 평가제도를 완성해가야 할 것이다.

ABSTRACT

It's been almost 6 years since PIA was implemented based on legislation. So I analyzed problems of PIA from the perspective of ITSM 3 elements. I mainly took account of quality improvement of the report when I assessed systems processing personal informations. So, I propose in terms of logical validity improvement of assessment report. The improvements on 4 different outputs for each phase are many cases that I assessed systems processing personal informations. And I propose improvements on qualified assessors having capability of GRC and on process for managing the assessment system. To settle down PIA system as the reasonable and effective assessment system even after 2016, the statutory deadline for completion of PIA, assessors and appointed assessment firms and authorities should cooperate to complete the assessment system.

Keywords: privacy, Privacy Impact Assessment, personal information, human rights to information

I. 서 론

1.1 한국의 개인정보 현황

한국에서의 개인정보보호 현황에 대해 살펴보자면, 시스템의 개인정보에 관한 최초 문제제기는 2003년 NEIS 시스템 구축 사업 시 대량의 학생정보를 중앙 시스템에 수집·저장하는 문제를 놓고 전교조를 비롯한 시민사회단체들이 국가인권위원회에 진정하였다[1]. 이후 2005년 기업의 PIA가이드라인이 배포되었으며, 2008년 업무담당자 대상 PIA전문교육이 시행된 바 있다. 2011년에 이르러 개인정보보호법이

Received(04. 11. 2016), Modified(06. 21. 2016), Accepted(08. 01. 2016)
* "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2016-H8501610120001002)
† 주저자, solemnity02@gmail.com
‡ 교신저자, khhan@formal.korea.ac.kr(Corresponding author)

제정되었고, 이 때 비로소 법적 근거를 기반으로 PIA전문가 교육과 함께 평가가 시작되었다[2]. PIA 시장모형[1)][3]은 두 가지 변수(전담기구의 평가기관 면허권, 평가기관 선정의 주체)에 따라 아래 (Table 1.)과 같이 4가지 유형이 도출되며 한국은 '수요자 다수의 불완전경쟁 시장모형'을 채택하여 현재까지 제도를 운영하고 있다.

국외의 동향을 살펴보면, 개인정보 보호에 관한 가장 오래된 정책은 캐나다에서 1990년대에 제정된 'Privacy By Design'이며, 이는 7대 기본원칙을 준수한다면 개인정보 생명주기(life cycle)에 걸쳐 이용자의 프라이버시와 데이터를 보호하는 기술 및 정책을 안전하게 적용할 수 있다고 주장한다. 그리고 미국은 DHS에서 시행하는 PIA, 일본은 1999년에 제정된 'JIS Q 15001'이 있다. 특히, 일본은 EU지침 25조에 국제적으로 대응하기 위해 이를 제정하였다. 이외에 개인정보보호와 관련된 국제표준으로는 1980년 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'이 최초이며, ISO/IEC 표준[4]에서는 ISO29134(PIA methodology)가 현재 작업중이다. 이외에 29100, 29101, 29190, 29191, 금융에 관한 표준으로 ISO22307 등이 규정되어 있다.

Table 1. market model of PIA

		main agent of selecting assessment institution (consumer)	
		licensee (consumer majority)	main agent (consumer 1person)
main agent's assessment institution license (provider)	Yes (provider minority)	A (imperfectly competitive market model of majority consumer)	B (imperfectly competitive market model of 1person consumer)
	No (provider majority)	C (perfectly competitive market model of majority consumer)	D (perfectly competitive market model of 1person consumer)

1.2 ITSM 3대 구성요소 관점의 개선방안 수립

IT Governance란 기업의 전략과 목표에 부합함으로써 리소스와 프로세스를 통제·관리하기 위한 체계이며, 이 중 IT 서비스를 최상의 상태로 유지하기 위한 활동이 ITSM이다. 즉 ITSM은 합리적인 비용범위 내에서 합의된 품질 수준의 서비스를 제공할 수 있도록 프로세스, 자원, 기술을 종합적으로 관리하기 위한 IT 관리체계를 만드는 것을 지원한다. 이를 위한 3대 구성요소로 product는 도구 혹은 솔루션을 의미한다. 다음으로 people은 기술과 능력을 갖춘 인재에게 Role을 배정하거나 인력이나 조직에게 업무에 적합한 교육을 수행하는 것을 포함한다. 그리고 process는 IT서비스를 제공하고 지원하는 과정이다.

업무처리에 사용하기 위해 정보처리시스템에서 보유·이용하는 개인정보를 보호하는 활동은 이제 기업의 경쟁력 강화를 위해 반드시 수행해야하는 업무이다. 이에 상기 3P 요소(Product, People, Process)의 관점으로 PIA 평가체계를 분석하여 product에는 평가 도구 자체인 PIA 평가체계를, people에는 평가수행 인력을, process에는 평가제도 운영 프로세스를 대응시켜 평가제도에 대한 메타평가를 수행하고 개선안을 제안하였다(Table 2.).

Table 2. structure of the paper

3P of ITSM	3P of PIA	the focus of analysis
Product	assessment report	formal validity
People	assessor	long/medium/short term plans for manpower
Process	system management	Role of senior management

II. PIA 평가보고서의 문제점과 개선방안

2.1 평가보고서에 적용되는 논증의 성격

논증은 연역과 귀납의 두 가지 방법이 있으며, 주장과 근거의 관계가 얼마나 탄탄한지를 진단하는 도구로써 논증을 사용한다. PIA 평가보고서에서 다루고자 하는 것은 평가 전제의 참이 결과의 참을 증명하는 연역논증의 성격을 가진다. 아래 (Table 3.)을 보면, 연역논증에서 '타당하다'라고 평가할 수 있는 세 가지 경우가 있으며, 다음 단계인 내용의 건전성까지 검토하는 과정을 거쳐야 최종적으로 전제와 결론이 모두 참인 결론에 도달하게 된다.

이를 개인정보 영향평가에 적용하여 저자는 타당성

1) 진보네트워크센터의 '정보인권과 개인정보 사전영향평가' 보고서에 수록된 표 인용

Table 3. validity and integrity of the deductive argument

	premises	conclusion	validity	integrity
①	true	true	○	○
②	true	false	×	×
③	false	true	○	×
④	false	false	○	×

과 건전성을 다음과 같이 분류하였다. 형식적 타당성이란[5] 최종 평가결과가 제3자의 입장에서 용인될 수 있는 전제로부터 시작하여 평가의 각 과정이 연역적 논증을 만족하는 것이다. 주로 평가보고서에서 범위설정과 업무분류, 위탁·제3자 제공 등 개인정보 현황분석 시 사용하는 논리체계에 해당하며, 평가항목 점검 이전 단계까지로 이해하였다. 그리고 내용의 건전성이란, 영향평가에서는 주로 평가항목의 점검에 국한하여 관리적·기술적 내용을 분야별 전문지식에 기반하여 평가하는 것으로 이해하였다.

다양한 개인정보 처리 시스템을 대상으로 평가를 수행하면서 적용한 개선방안을, 영향평가 수행 단계별 산출물 4종을 기준으로 제시하였다. 평가도구의 조건인 타당도, 신뢰도, 객관도, 실용도[2] 향상을 고려하였고, 특히 형식적 타당성[6][3]을 염두에 두고 논리적 일관성 측면의 개선안을 제시한다. 아래(Table 3.)에서 ③,④의 경우를 예방하기 위해 전제의 올바른 수립을 돕기 위한 도구로써 4가지 산출물을 아래와 같이 검토하였다.

2.2 개인정보취급업무표

2.2.1 개인정보 범위선정에 관한 명확한 기준 제시

산출물 중 '개인정보 취급 업무표'는, 평가대상시스템에서 처리하는 개인정보항목을 표기하도록 하고 있다. 이는 평가대상 범위설정에 대한 근거자료이다. 그러나 평가자별로 표기하는 개인정보의 정도가 상이하여 제3자 입장에서 개인정보로 정의하는 기준 파악이 모호하여 범위설정에 관한 명확한 이해가 어렵다. 현재 수행사례를 보면, 평가항목에서 명시한 개인정보 항목이 개인정보취급업무표나 개인정보흐름도에 나타나고 있지 않아 보고서 전체의 일관성이 결여된 경우가 있다. 그리고 민감정보 여부에 대해 평가자마다 다른 개념정의를 가지고 있어, A기관 영향평가에서는 민감정보로 분류한 개인정보 항목이 연계기관인 B기관 평가보고서에서는 누락되는 등의 문제가 발생하고 있다.

대안으로 '개인정보 영향평가 수행안내서'의 개인정보 영향도 등급표에서 구분하는 3단계 깊이 '등급〉등급내 세분류〉개인정보 종류'까지 표기하는 방법을 사용한다면 평가에서 정의하는 명확한 개인정보의 범위를 이해하기 쉽다(Table 4.). 혹은 평가대상 기관의 내부 법률지원팀과 협의하여 개인정보의 범위를 정의하고 이후, 관련 근거를 첨부하여 객관성을 높일 수 있다.

그리고 단일 시스템을 여러 기관이 공동 관리하는 경우, 세부 업무에 대한 평가의 범위를 명확히 설정하여 제3자 제공 유무를 판단하여야 한다(Fig.1.).

2.2.2 평가 업무단위 분류 근거 제시

평가 업무단위는 개인정보취급업무표, 개인정보흐름표, 개인정보흐름도, 평가항목표의 '평가단위'로서 평가 보고서 각 산출물간 일관성이 필요하다. 그러나 업무분류 근거가 명확하지 않거나 동일 보고서 내에서도 업무단위의 개수나 명칭의 일관성이 결여되는 경우가 자주 발생하고 있다.

동일한 시스템(혹은 업무)이라 하더라도 평가자에 따라 업무단위 분류가 상이할 수 있으나, 평가자가 정의한 업무단위에 대해 대상시스템의 사이트맵이나 메뉴구성도 등 평가 업무단위 분류 근거 제시해야 한다. 개인정보 취급업무표에서 '별첨' 등의 형태로 근거를 제시하는 등 논리적 기준을 수립해야 업무 분류에 대한 이해가 명확해지고 보고서가 설득력을 가질 수 있다(Fig.2.).

그리고 특정 시스템별 독특한 개발 방법론이나 특성을 가지고 있는 경우, 표준 산출물 형식 이외에도 시스템 이해를 도울 수 있는 부가적인 자료를 작성하는 융통성을 부가하여 평가보고서의 품질향상을 위해 노력해야 한다. 수행 사례 중 AOP(Aspect Oriented Programming)[4]관점으로 시스템의 업

2) - 타당도:측정하고자 하는 변인을 검사가 제대로 측정하였는지에 대한 정도를 의미하며, 신뢰도 확보를 위한 필요조건임.
- 객관도:채점자에 따라 점수가 얼마나 일관성이 있는지의 정도를 의미하며, 평가 신뢰도 확보의 전제조건임.

3) 건전한 논증이 되기 위해서는 형식적 타당성이 선행되어야 다음 단계인 내용의 건전성 검토로 진행하게 됨.

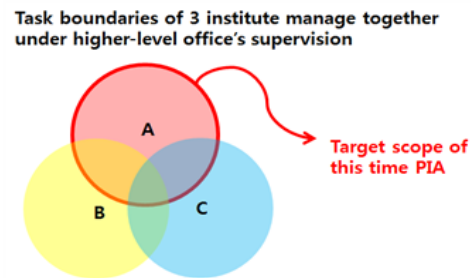
4) 객체지향의 다음 단계를 이어가는 새로운 방법론으로서,

Table 4. case on table handling privacy_items

menu	the existence of personal information	CRUD	critical personal informations		
			1-class degree	2-class degree	3-class degree
1.school register					
information modification	○	C	unique identifiable information(resident registration number), financial information(name of bank, account number, account holder)	unique identifiable information(name, ID picture, address, phone number, e-mail)	limited self identifiable information(student ID number)
students information query	○	R	unique identifiable information(resident registration number), financial information(name of bank, account number, account holder)	unique identifiable information(name, ID picture, address, phone number, e-mail), personal relevant information(family composition, reward, certificate, school register change, timetable, grade)	limited self identifiable information(student ID number)
check borrowing an umbrella	○	R	unique identifiable information(resident registration number)	unique identifiable information(name, address)	limited self identifiable information(student ID number)
2.class					

A institution ABC system Privacy Impact Assessment the table handling privacy

※ A system is developed and managed by 3 institutes in common



- At this time PIA, ordering agency is A. So tasks that B and C institutes manage exclude from boundary of PIA.
- In case of tasks managed by A and B institutes in common, it's not offering to third party but A's tasks that A offers informations to B.
- To without ommission investigate the whole flow of privacy including interagency linking of ABC system that 3 institutes manage together, I recommand that after this assesment, you assess intensively interagency link focusing on personal information under higher-level office's as ordering agency.

Fig. 1. case on table handling privacy_relative organization

기존의 프로그래밍 방법론으로 해결할 수 없었던 여러 모듈에 속성상 걸치게 되는 횡단 관심사(cross-cutting)를 모듈화 하여 코드 혼합과 코드 산재의 문제를 해결함.

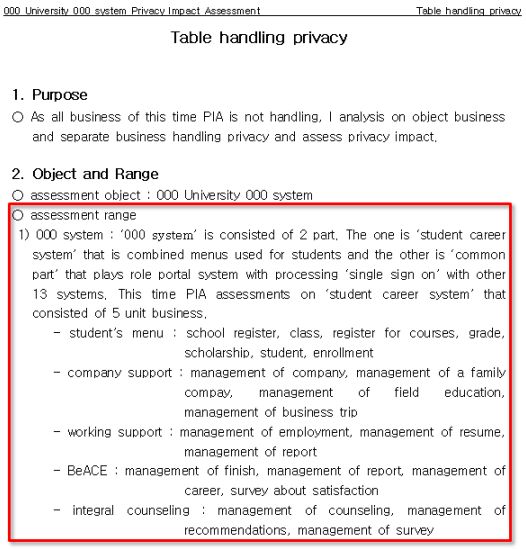

000 University 000 system Privacy Impact Assessment Table handling privacy

Table handling privacy

1. Purpose

○ As all business of this time PIA is not handling, I analysis on object business and separate business handling privacy and assess privacy impact.

2. Object and Range

○ assessment object : 000 University 000 system

○ assessment range

1) 000 system : '000 system' is consisted of 2 part. The one is 'student career system' that is combined menus used for students and the other is 'common part' that plays role portal system with processing 'single sign on' with other 13 systems. This time PIA assessments on 'student career system' that consisted of 5 unit business.

- student's menu : school register, class, register for courses, grade, scholarship, student, enrollment
- company support : management of company, management of a family compay, management of field education, management of business trip
- working support : management of employment, management of resume, management of report
- BeACE : management of finish, management of report, management of career, survey about satisfaction
- integral counseling : management of counseling, management of recommendations, management of survey

Fig. 2. case on table handling privacy_task

무 프로세스와 메뉴구성도가 고안된 경우, 개인정보 취급업무표에서 AOP맥락에 따라 개인정보 생명주기를 구분함으로써 개인정보의 흐름을 이해하기 쉽게 안내하였다. (Table 5.)는 메뉴구조도 12개 처리단계를 법정분류기준인 A, B, C의 업무로 구분하고, 각 처리단계별 개인정보주체(마스킹 처리를 위해 동물이름으로 대체함)와 개인정보처리단계(수집, 이용제공, 파기)여부를 구분하였다.

2.3 개인정보 흐름표/흐름도

내부연계의 경우, 별도 표기하도록 개인정보흐름도 작성단계에서 안내하고 있으나, 대부분의 평가보고서에서 누락되고 있다. 외부연계의 경우, 누락되고 있거나 가능한 모든 외부연계를 표현하고 있지 않다. 특히 개인정보흐름도 산출물의 경우, 평가 결과를 생명주기에 따라 한 눈에 이해하기 용이하도록 지원하는 산출물 형식이지만 일부 평가자의 경우 다수의 항목 표기를 누락하고 있다.

평가 단계별 도출되는 각 산출물 간 표현 방식만 상이할 뿐 동일한 내용을 포함하고 있으므로, 최종 개인정보 흐름표·흐름도에는 평가대상 시스템의 '개인정보 내부/외부연계 시스템'과 '수집 서식'등을 명시하여 시스템 간의 상관관계를 한눈에 파악할 수 있어야 한다(Fig.3.).

2.4 평가항목 점검표

신규 기준 78개 평가항목 평가 시(이행/부분이행/미이행/해당없음), 평가기준이 평가수행 기관이나 평가자에 따라 상이하므로 다른 평가자에 의한 시스템 결과가 보고서 검토자 입장에서는 평가결과를 상호 비교할 수 있는 근거가 취약하고 논리적 설득력이 부족하다. 대안으로써 (Table 6.)의 경우, (개정 이전 114개 평가항목에서) 항목 평가 수행 전 평가자가 수립한 평가기준을 명시하여 평가기준의 이해를 돕는다. 평가 평가항목 3, 4장 실행항목의 경우, 1장(대상기관에 관한 정책)이나 2장(대상시스템에 관한 정책)규정이 수립되어 있다면, 부분이행은 있을 수 있으나 미이행 항목이 도출되는 않는 평가 기준을 적용하였음을 안내한다.

Table 5. case on table handling privacy_AOP

	step 1	step 2	step 3	step 4	step 5	step 6	step 7	step 8	step 9	step 10	step 11	step 12
A		○	○		○	○	○	○	○	○	○	○
B		○	○		○	○			○		○	○
C	○	○	○	○	○	○			○	○	○	○
owner of personal information	-tiger -lion	-elephant -sparrow	-frog	-cat	-mouse		-giraffe -monkey -donkey			-camel		
personal information life cycle	collection	collection	use	use	use	use	use	use	collection/offering	collection	use	use

Table 6. case on assessment item checklist

evidence about assessment		Yes	Partial	No	Not applicable
inside policy and evidence of design/operation		○	-	-	-
inside policy or evidence of design/ operation	inside policy	-	○	-	-
	evidence of design/ operation	○ some items that doesn`t mentioned about relevant inside-policy at checklist chapter1(targer organization), chapter2(targer system).	○ some items that mentioned about relevant inside-policy at checklist chapter1(targer organization), chapter2(targer system) but doesn`t have concrete policy.	-	-
no both inside policy and evidence		-	-	○	-
irrelevant to target system		-	-	-	○

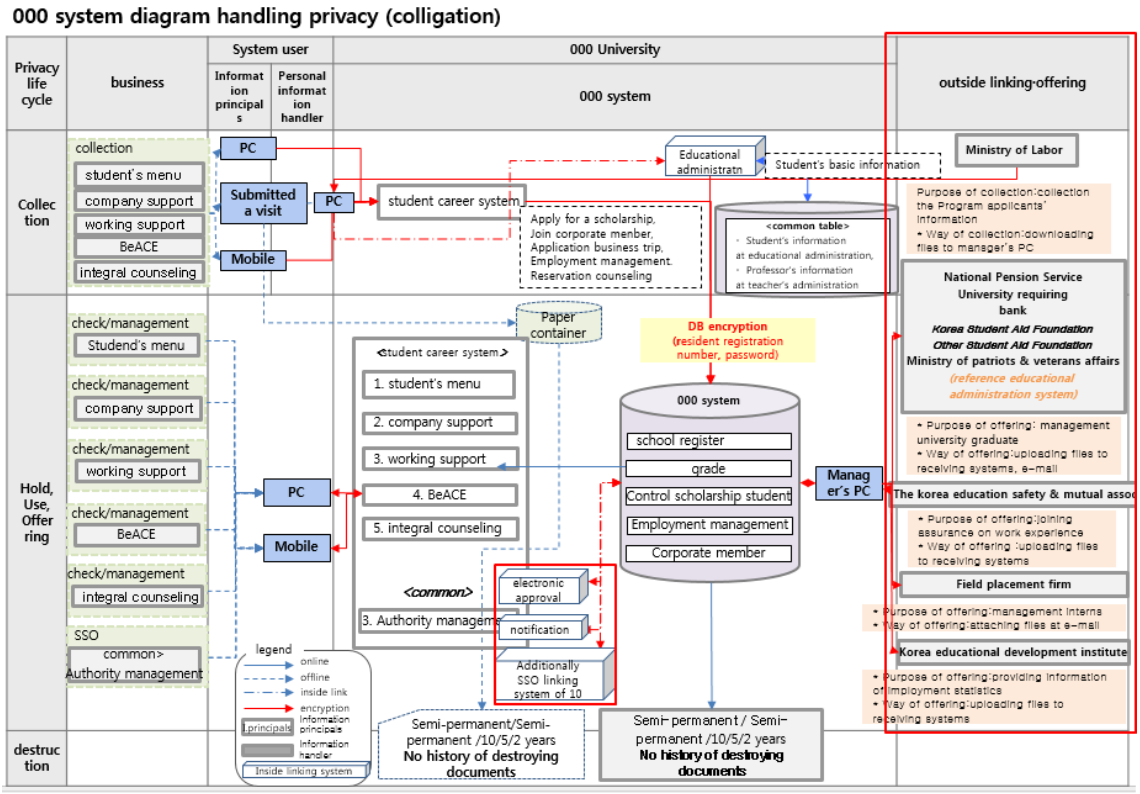


Fig. 3. case on diagram handling privacy

2.5 결과보고서

평가 수행기관에 따라 위험도 평가 시 DoA(Degree of Assurance) 수준을 산정하는 경우도 있으나 일부 보고서는 누락하는 경우도 있다. 수행가이드에는 명시되어 있지 않으나, 유사 인증체계(PIMS, ISMS)등에서 점검항목으로 포함되어있어 차후 유사인증 획득이 필요한 경우 DOA 산정 업무를 별도 수행하여야 하므로 PIA에서도 필수 항목 이외 선택항목의 범위에서 명시화 한다면 보고서의 실용성을 향상시킬 수 있다.

III. 제도운영의 문제점과 개선방안

2장에서는 ITSM 3P 중에서 product에 해당하는 평가 산출물의 형식적 타당도 확보를 위한 개선안을 제안하였다. 3장에서는 평가 보고서 품질 향상을 위해 people에 해당하는 평가 수행인력과 process에 해당하는 제도 운영에 관한 개선안을 제안한다.

3.1 평가인력 관점

현재 발주되고 있는 일부 제안요청서에서는 평가인력의 SW기술자 등급별 가점이 명시되거나 유사 단가가 제안된다면 SW기술자 등급이 높은 경우 낙찰이 되고 있다. 그러나 영향평가 업무수행에 필요한 소양이나 보고서 품질과 SW기술자 등급 간의 정적 상관관계에 대한 선행 연구나 근거 없이 이루어지고 있어 품질향상에 대한 기대가 쉽지 않다. 미국의 교육학자 블룸이 제시한 7단계 사고력(Table 7.)[8]에 비교하자면, 현재의 인력 평가는 주로 기초정신과정에 해당하는 인지능력 즉, IT와 법률에 관한 내용을 측정하고 있다. 또한 영향평가 수행가이드는 평가체계에 관한 큰 틀만 제시하고 있으며 이외의 형식적 타당성이나 내용의 건전성[6]에 대해서는 평가기관이나 평가자에 의존한 자율성을 부여하고 있다.

선행연구 사례로서 김이랑의 '개인정보영향평가 자격기준의 문제분석과 개선방안 연구'[7]에서는 CPPG[5], ISA[6]와 함께 평가 목적과 대상, 업무, 지식, 기능, 평가기준, 검정과목을 기준으로 비교하고 있다. 이에 따른 PIA 자격체계의 개선방안으로서는, 전문자격수립, 모듈별 추가운영, CIPP[7]유사 전문자격 모듈화를 제시하고 있다.

Table 7. categorization of educational objectives on cognitive domain by Bloom

basal mental process	knowledge	memory	- knowledge on indivisual and detailed thought - knowledge on way and means - knowledge on universal and abstract thought
	intellectual skill	comprehension	- comprehension of the meaning - translation - extrapolation / interpolation
higher mental process		application	- application of abstract idea - application of way and principle - application of theory and system
		analysis	- analysis of element - analysis of relationship - analysis of organizing principle
		synthesis	- design of a unique communication - design of planning and execution procedure - derivation of abstract relationships
		evaluation	- judgment by internal criterion - judgment by external criterion

그러나 개인정보 영향평가 수행자에게는 GRC (Governance, Risk, Compliance) 관점에 부합하는 융합 학문적 소양이 필요하다. (Fig.4.)는 GRC 역량을 인체에 비유하여 표현하였다. 한국에서 개인정보영향평가의 필요성은 1장에서 언급했듯이 시스템 상에 이용되는 개인정보에 관한 인권의 문제에서 대두되었다. 그러므로 인권을 우선으로 염두에 두고 이를 보호하기 위한 목적으로 평가 전략을 수립해야한다. 업무처리에서 인권보호를 실천하기 위해 방

5) CPPG:한국CPO포럼에서 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 평가하여 개인정보관리사 자격을 인증하기 위한 목적으로 2009년부터 운영됨.

6) ISA:한국정보화진흥원에서 국가 정보화사업에 대한 감리체계 확립과 실제 정보시스템 분야의 감리 전문 인력 확보를 위해 2000년부터 국가공인민간자격으로 운영됨.

7) CIPP:각 국가 법제의 특수성을 반영하여 미국(US), 캐나다(C), 유럽(E)등으로 구분되어 있고, 정부와 공공영역(G)에 특수화되거나, 정보시스템전문가(IT)들을 위해 별도로 구분되어 있다. 미국은 법률적·정책적 내용들을 중심으로 하는 CIPP/US와 기술적인 부분에 초점을 맞추고 있는 CIPP/IT를 별도로 운영함.

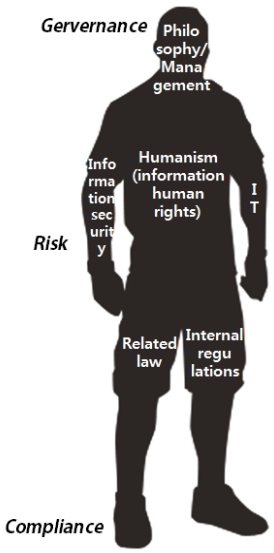


Fig. 4. GRC on PIA

향을 설정하고 인도하기 위해 의무사항으로써 관련 법률을 규정하고 이를 기반으로 각 기관에서는 최적화 된 내부규정을 수립하고 있다. 시스템에서 개인정보 보호를 준수하기 위하여 정보보안과 IT는 구체적인 실행을 수행하며 정보보안부서는 기존 IT운영의 기반위에서 보다 특화되어 주도적인 역할을 수행하여야 한다.

Governace에 해당하는 소양은 논증의 검증에 있어서 타당성과 관련되며, Risk와 Compliance 소양은 IT와 법률에 관한 내용의 건전성에 해당한다고 볼 수 있다.

3.1.1 장기적 인력양성 방안

이를 기반으로 평가 인력을 통한 품질 개선안을 도출하자면, 장기적인 방안으로서 논리적 사고나 고등정신과정 계발을 유도하여 타 학계에서 고등인지능력(논리추론, 상황판단 등) 함양을 유도하는 유사 인력체계를 갖춰나가야 한다. 선행 연구 사례로서, 이은경이 '인문학과 정보과학기술의 학제간 연구 교육현황과 활성화방안'[9]에서 제시한 대안을 수용하여 대학의 정보보안 학과에서는 정보보호 컨설팅 역량 강화를 위한 맞춤형 인문학 교과목을 운영하거나 IT학과에서는 논리적 교양과목을 포함하는 학제간 융합교육으로 인력을 양성할 수 있다. 이는 현재의 인력 평가내용에서 누락된 Governance 소양을 보완해 줄 수 있는 방안이 되며, 블룸이 제시한 7단계 사고력 체계에서도 고등정신능력인 분석·종합·평가의 능력을 갖출 장기적인 시간을 확보하게 되어 적합한 인력양성을 위한 적절한 시기가 될 수 있다.

3.1.2 중기적 인력양성 방안

보다 중기적인 방안으로는 선행연구 사례인 김이랑이 제시한 개선안과 절충하여 현재의 인력선발 제도의 평가지표에 공통모듈 등으로 'PSAT(Public Service Aptitude Test)'와 같은 영역을 추가 운영하는 방안이 있다. 이는 고등인지능력 측정의 평가도구로써 타당도와 신뢰도는 여영서[10], 김기원[11] 등 다양한 선행연구를 통해 검증된 바 있다. 이와 같은 고등 인지능력을 겸비한 평가자에 의해 다양한 형태의 시스템에 관한 형식적 타당성도 갖춘 평가 보고서를 기대할 수 있다.

3.1.3 단기적 인력양성 방안

단기적인 방안으로, 이미 선발된 수행 인력에 대해서는 IT와 법률에 대한 계속 교육이 수반되어 급변하는 IT기술과 법률 분야에서 내용적 건전성을 유지하여야 한다. 그리고 기술 기반의 특급 인력을 투입하여, 현재 내용의 충실도 면에서 미흡한 보안 기술 분야의 품질을 향상시켜야 한다.

부가하여 사회적 측면에서 평가 시 투입되는 인력을 본다면, 개인정보영향평가는 공공기관을 대상으로 수행하고 있으므로 공공기관의 청년 일자리 창출정책과 일관된 방향을 추구하여, 사업 발주 시에 초·중급을 모두 포함하는 피라미드식 팀 구성에 가점을 부여하는 방안이 있다. 이는 국가 전체의 제도와 맥락을 같이하는 방안으로써 상급 관리기관이 인력을 통제할 수 있는 범위이다. 또한 평가 수행 시 필요한 능력인 GRC 역량과 인력예산 ROI(Return On Investment)의 차원에서도 합리적인 인력 배치가 된다.

3.2 상급 관리기관의 역할

ITSM의 3P 중 process에 관한 부분으로는, 제도를 운영하는 상급 관리기관의 역할에 대해 개선안을 제시한다.

3.2.1 평가 결과에 대한 품질 검토

현재 운영되는 시장모형(수요자 다수의 불완전경쟁 시장모형)에 따르면, 개인정보보호위원회가 관리의 책임을 가지고 있으므로 역할과 책임(R&R)을 인식하고 적극적으로 제도의 process를 개선하기 위해 노력하여야 한다. 실행 방안으로서는 행정자치부에 등록되는 개인정보영향평가 결과보고서의 품질검토를 수행하여 평가기관이나 평가자에게 피드백 하는 과정이 마련되어야 한다. 차후 기관 재지정 시, 감점을 부여하거나 수행인력 자격갱신 시에 객관적으로 반영하여 품질 향상을 제도적으로 유도하는 등 적극 개입해야 한다.

3.2.2 사업기간 대비 비용

'개인정보영향평가 대가산정 참고사항 (2014.03.10.)'[12]를 제시하고는 있으나 현재 사업 수주의 경우 평균 시스템 당 3천만원으로 가격이 결정되며 최저가 입찰로 수행되고 있는 실정이다. 혹은 개발업체의 하도급에 의해 수행되는 경우도 있다. 발주기관에서는 평가 수행자체에만 의미를 두고 있으며, 상급관리기관에서도 수행사의 보고서 품질관리에 관대한 면이 있다. 결과, 시스템별 특성에 따라 세분화해야 할 업무단위가 그룹핑되어 평가가 수행되는 등의 문제가 발생하며 보고서의 품질이 평가대상 기관이나 평가업체에서 비중 있게 다루어지고 있지 않다. 개선책으로 발주/수주의 과정에서 개발사 하도급이 금지되고, 비용 산정에 관한 근거 문서를 첨부하도록 하여 사업범위와 기간 대비 적절한 대가를 지불하여 평가의 날림 수행을 예방하고 품질이 향상된 평가가 정착하도록 관리하여야 한다.

3.2.3 연계된 공공기관의 개인정보 관리 기준 상이

평가기관이 대학교인 경우, '개인정보파일 표준목록'과, '대학 기록물 보존기간 책정기준 가이드' 등을 참고하고 있다. 그러나 대학 상급기관인 교육부에서 안내하는 가이드의 내용과 상충하는 등 개인정보 관리에 대한 기준이 불일치하는 문제가 발생하며, 대학교는 관리기관인 교육부 정책을 따르게 되므로 컨설팅에서 제시하는 개인정보 관리 가이드가 무용한 경우가 발생한다. 상급 기관들 간의 공통 업무에 대한 top-down 방식으로 일관된 개인정보 관리기준을 정비한 안내가 불가능하다면, Bottom-up 방식으로 개인정보영향평가 결과 등을 반영하여 연계된 공공기관 등의 개인정보에 관한 관리기준을 점검하여 일관성 있는 개인정보 관리기준을 수립해가야 한다.

IV. 결 론

개인정보 영향평가 수행자로서 다양한 시스템을 평가하면서 평가의 논리적 타당성을 수립하기 위한 개선방안을 모색하였다. ITSM의 핵심은 특정 업무에 국한되어 있는 각종 IT 인프라를 제반 업무에 효율적으로 활용해 투자효과도 극대화시키면서 최신 IT기술을 빠르게 받아들일 수 있게 하는 것이다. IT 서비스의 일부인 PIA 역시 동일한 프레임으로 평가체계를 조망할 수 있다. 결론을 요약하면 아래 (Table 8.)과 같이 정리된다.

후속 연구로는 유사 정보보안 컨설팅(ISMS,

Table 8. summary of conclusion

structure of contents		improvement plan
assessment report [formal validity]	assessment report (Product)	• Considering the characteristics of consulting services, I studied reasonable development of deductive logic. • Applying to 4 outputs of PIA, I suggest methods that prevent omission of assessment range and improve objectivity of assessing items.
system management	assessor (People) [integrity of contents]	• I defined the competency for assessment wort is GRC(Governance, Risk, Compliance). • For that, I suggest the improvement plan in the long/medium/shot term.
	system management (Process)	• I suggest the role of the Personal Information Protection Commission that is management agency of PIA, • I propose quality review of the report, prevention poor business execution, and consistent policy-making between interagency.

PIMS 등)에도 동일하게 적용되는 연역추론의 타당한 전개과정을 검토하여, PIA체계에 도입하거나 개선해야 할 사안들을 수용할 필요가 있다. 그리고 본 논문에서 언급한 다양한 문제점들(학제간 융합교육, 평가인력 편성 등)에 대해 다양한 이해관계자와 관련 전문가의 의견을 수렴하여 평가제도의 객관성과 실용성을 확보해가야 할 것이다.

미래에는 무인자동차, 인공지능 등 새로운 기술이 등장하고 이를 제어하기 위한 새로운 법령이 제정되는 등 개인정보를 취급하게 될 산업의 범위는 지속적으로 확장될 것이다. 현재 공공기관을 의무대상으로 하는 PIA는 주로 'web site'의 범위에 한정되어 수행되고 있으나, 평가체계의 논리적 타당성을 건전하게 수립한다면 향후 다양한 신기술 분야에서 개인정보가 활용되더라도 평가의 대상만 확장될 뿐 용이하게 개인정보 보호체계를 적용할 수 있을 것이다.

References

[1] Keo-hyeon Lee, "Thesis on the violation of information human rights and the development of the issue:centering onf NEIS," master's thesis, the department of civil society organizations graduate school of ngo Sungkonghoe University, Feb. 2006.

[2] Jin-man Heo, Chang-woo Woo and Jung-ho Park, "Development of Privacy Impact Assessment Tool," The Korean Association of Computer Education journal, 15(2), pp. 3, Mar. 2012.

[3] Network Center studied progress, "Information Human Rights and Privacy Impact Assessment," Panel discussion on civil society organizations, pp. 22-24, Nov. 2004.

[4] Dae-ha Park, "International Standardization Trend on Information Security and Personal Information Security," Korean Institute of Information Security & Criptology, 23(4), pp. 47-52, Aug. 2013.

[5] Kwang-soo Kim, Logic and critical thinking:chapter 3 validity, Company philosophy and reality, Sep. 1995.

[6] Chung-gyoo Woo, "Cultivating Critical Thinking Power Through Formal Logic and PSAT/LEET Sample Questions," Culture collection of writings, 5, pp. 50-80, Dec. 2011.

[7] E-rang Kim, Mi-na Shim and Jong-in Lim, "A Study in the Improvement and Analysis Problem of Privacy Impact Assessment Qualification Criteria," master's thesis, the department of information security graduate school of Korea University, pp. 6-15, Feb. 2013

[8] Young-jung Kim, "PSAT and Bloom's Classification of Thinking," KOREAN SOCIETY OF CIVIL ENGINEERS journal, 53(7), pp. 89-94, July. 2005.

[9] Eun-kyeng Lee, Young-soo Yook, Mal-rae Lee and KwansSoo, Lee, "current state of education and ativation plan on interdisciplinary research of humanities and information technology," Korea Council of Humanities Social Research Institute A series of humanities and Policy Resarch, Mar. 2006.

[10] Yeong-seo Yeo, "LEET and Logical Thinking Ability-comparing LEET, LSAT, PSAT," DAE-DONG Philosophical Society, 43, pp. 262-274, June. 2008.

[11] Ki-won Kim, "Validity of PSAT(Public Service Aptitude Test)," Korean Journal of Counseling and Psychotherapy, pp. 252-253, 2008.

[12] National Information society Agency, "Reference price calculation on PIA," Mar. 2014.

〈저자소개〉

최 영 희 (Young-Hee Choi) 정회원
2003년 2월: 부산외국어대학교 전자컴퓨터공학부 컴퓨터공학과 졸업
2016년 8월: 건국대학교 정보통신대학원 정보보안 공학석사
현재: ㈜씨에이에스 개인정보사업부문 선임컨설턴트
〈관심분야〉 개인정보보호, 정보보호관리체계

한 근 희 (Keun-Hee Han) 종신회원
서울과학기술대학교 컴퓨터공학과 졸업
한양대학교 과학대학원 공학석사
고려대학교 대학원 이학박사
현재: 고려대학교 정보보호대학원 산학교수
〈관심분야〉 소프트웨어 보증, 시큐어코딩, 정보보호관리체계, 개인정보보호, 클라우드 컴퓨팅보안, 스마트 의료보안, 스마트 공장/제조 보안 등