

금융보안 리스크 기반의 IT도급 정책 연구

최창래,[†] 윤장호, 이경호[‡]
고려대학교 정보보호대학원

A Study on IT Outsourcing Policy Based on Operational Risks of Financial Industries

Chang-Lai Choi,[†] Jang-Ho Yun, Kyung-Ho Lee[‡]
Korea University, Graduate School of Information Security

요약

2011년 대형 금융 사고가 연달아 발생하자 정부는 인력, 조직, 예산을 포함한 전자금융감독 규정 전면 개정을 발표했다. 규정에 주요 내용은 전자금융거래법 대상 기업들은 전체 직원의 5%를 IT인력으로 채용하고, IT인력의 5%는 보안인력으로, 또 IT예산의 7%는 정보보호 예산으로 편성하게 하는 내용이었다. 본 연구는 전자금융감독 규정 전면 개정에 따른 금융보안 리스크 기반의 IT도급 정책 결정 방안에 대해 연구하였다. 외주인력 문제를 해결하기 위한 정책 결정 Flow를 제공하고 IT 업무 분류 시 프로그램 품질 향상을 위한 개선 방안과 사례 연구를 통해 외주 인력의 효율적 운영 정책을 제시하고자 한다.

ABSTRACT

For the continuous financial incidents occurred in 2011, Korean government has announced the amendment on electronic finance supervision regulation including human resources, organization and budget. The major part of the regulation is mainly focused on human resources and budget. It states that company has to employ at least 5 percent of IT staff out of total staff, and at least 5 percent of security staff in IT staff employment number. Budget for security should be at least 7 percent of total IT budgets. This paper studies IT outsourcing policy based on operational risks of financial industries caused by amendment of regulation. This paper provides the policy decision procedure for resolving the 3rd party problems and suggests the effective operation policy to 3rd party for the program quality improvement and case studies at the IT task classification.

Keywords: Electronic Financial supervision regulatory, IT Outsourcing Policy, Operational Risks

1. 서론

2011년 4월12일 N사는 해킹 피해로 인터넷 뱅킹 및 자동화기기(ATM) 등의 주요 금융서비스가 전면 중단 되었다. 관련 사태로 인해 금융기관은 물론 국내 공공기관, 대기업, 중소기업에 대한 보안 문제는 필수 불가결한 운영 요소가 되었다.

이에 대한 정부 대책으로 전자금융감독 규정 개정 시행 및 금융회사 정보기술(IT부문) 보호업무 모범규정 개정 시행에 따라 금융기관 IT인력은 총 임직원수의 5% 이상을 IT인력으로 확보해야 하며, 정보보호 인력은 IT인력의 5% 이상을 보안인력으로 확보해야 한다(단, 외부 IT인력은 금융회사 내부 IT인력 범위 내에서 인정). 또한, IT예산의 7%를 IT보안 예산으로 확보해야 한다[1][5][6].

전자금융 업무는 IT기술 발전이 급속히 진행되는 여건상 외주 인력 업무가 상당부분 차지하고 있으나,

접수일(2014년 5월 9일), 게재확정일(2014년 7월 10일)

[†] 교신저자. cclking@korea.ac.kr

[‡] 교신저자. kevinlee@korea.ac.kr(Corresponding author)

외주 인력에 대한 내부통제 및 관리 소홀로 금융사고가 빈번하게 발생하고 있다. 국내 전자금융거래는 급격히 증가하여 전자금융 이용 비중이 2013년 12월 기준으로 87.8%에 이르고 있다.

인터넷 가입자 수는 9,459만 명(중복합산), 모바일뱅킹 고객 수는 4,993만명(중복합산)이며, 거래금액은 일평균 33조 6,751억 원이다. 이러한 전자금융 규모는 점차 증가하고 있으나 카드 등 금융회사의 정보통신(IT)부문 인력 상당수를 외부에 의존하고 있다(7).

Table 1.은 금융회사 IT부문 외주인력 현황(13.6월말)이다. 외주인력 비율 증가는 더 강력한 내부통제와 프로세스가 필요하여 내부 관리 인력이 더욱 필요 해진다(8).

Table 1. The status of the outsourcing in financial IT group (2013.6)
(Unit : Persons)

Division	Internal personnel	Outsourcing personnel	Rate of outsourcing personnel
Bank	3,702	2,081	56.2%
Securities	1,872	881	47.1%
Insurance	2,146	2,883	134.3%
Card	661	1,069	161.7%

본 연구 논문에서는 금융IT 업무 분류에 따른 역할 정의와 외주인력의 효율적 운영방안에 대해 고찰해 보고자 한다.

II. 관련연구 고찰

2.1 외주 도급계약의 정의 및 내용

인력 운용에 따른 계약의 형태는 근로자공급(직업안정법), 근로자파견(파견 근로자보호 등에 관한 법률), 도급(민법), 위임(민법)으로 구분된다.

우선, 근로자공급 계약은 공급사업주가 고용한 공급사업주가 고용한 근로자 또는 자신에 속해있는 있는 근로자를 근로자 공급 계약에 의하여 타인(사용사업주)에게 사용하게 하는 것이다. 단, 근로자 공급사업의 경우 노조법에 의한 일정 요건을 갖춘 노동조합만이 근로자 공급 사업이 가능하다.

근로자 파견 계약은 근로자 파견을 사업으로 하는

업체(파견업체)가 근로자를 고용한 후, 그 근로자를 다른 기업(사용업체)에 파견, 근로자는 사용업체의 지휘, 명령을 받아 업무를 수행한다. 적법 요건은 파견 대상 업무는 32개 업종이며 파견기간은 최대 2년(1년 + 당사자 간 합의 시 1년 연장), 파견허가는 파견사업주는 일정요건을 갖추고 고용노동부 허가를 요한다.

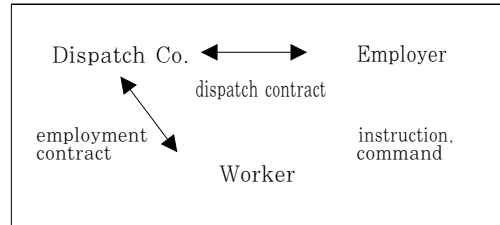


Fig. 1. Construction of dispatch of worker

도급계약은 민법 664조에 ‘당사자의 일방(수급인)이 어느 일을 완성할 것을 지정하고 상대방(도급인)이 그 일의 결과에 대한 보수지급을 약정하는 계약이다.’으로 명시되어 있다. 원사업자와 수급사업자의 근로자간에 지휘, 명령권을 행사할 수 없으며, 원사업자가 수급사업자의 근로자에 대하여 업무상의 지휘, 명령권을 행사한 다면 이는 그 계약의 명칭이 도급계약으로 되어 있다고 하더라도 사실상의 운영이 파견과 같은 것이 되어 파견 근로자보호 등에 관한 법률의 규율을 받게 된다.

도급계약은 원도급업체가 자기 사업장에서 이루어지는 업무의 일부를 하도급업체가 수행토록 하는 도급 유형으로 하도급 업체에서 원도급 업체의 생산시설을 이용하는 경우이며, 불법파견 또는 위장도급 시비가 가장 많은 형태이다.

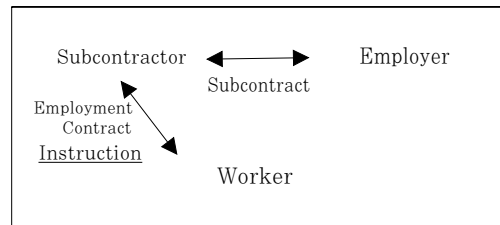


Fig. 2. Construction contract for any construction work

위임계약은 당사자 일방이 상대방에 대해 사무 처리를 위탁하고 상대방이 이를 승낙함으로써 성립하는 계약이다. 위임인과 수임인 근로자 간 지휘, 명령을 행사할 수 없다는 점에서 근로자 파견과 구별되고, 일

의 완성을 목적으로 하지 않고 위임 사무의 처리활동 그 자체를 목적으로 한다는 점에서 도급과 구별된다. 금융IT 외주 인력 계약은 주로 도급 계약을 채택하고 있다. 이는 외주 인력 고용 대상과 기간에 제한을 받지 않는다는 특성이 있다.

Table 2. Comparative table of subcontract and dispatch

Division	Subcontractors	Dispatch Co.
Object	no limit	Range set stated in Dispatch Law
Period	no limit	up to 2 years
Affiliation	Belongs to contractor company	Belongs to dispatch companies
Supervision	Independent performance	All authorities are assigned to dispatched company
Applicable Law	Civil law/Fair Trade	Law and act related to dispatched labor

이러한 외주 인력 운영 계약 형태에 따라 고용노동부는 사내하도급, 파견, 기간제 등 가이드라인을 제시하여 부당노동행위 위법을 적발하고 있다. 그러나 사내하도급은 개별, 기업 간의 민사상 계약 관계이므로 노동관계 법률로 규율하는 것에 대해 논란이 있고, 그간 일부 사내하도급이 불평파견에 해당되는지 여부가 주된 쟁점으로 부각되었다. 사내하도급을 둘러싼 논란을 해소하기 위해서는 도급, 파견 구별을 둘러싼 논란에서 벗어나 사내하도급 근로자의 근로조건이 실질적으로 개선될 수 있도록 하는 조치가 필요하다. Table 3.의 고용노동부의 사내하도급 가이드라인 체크리스트를 참조한다[9].

외주 인력 운영 도급계약 위반 시 처벌기준은 불법 파견이라고 고용노동부가 판단할 경우 사용사업주에게 즉시 직접 고용 명령을 시행할 수 있다. 만약 명령을 이행하지 않으면 외주인력 1명당 최대 3천만원의 과태료를 부과할 수 있다.

파견근로자 보호 등에 관한 법률 위반에 따른 형사처분은 동법(제5조, 제6조, 제7조 등)으로 파견사업주 및 사용사업주 공동 3년 이하 징역, 2천만 원 이하 벌금형이다.

민사책임으로 파견근로자 2년 이상 사용 시에는 사용사업주에게 고용의무를 부과한다. 파견근로자 보호

Table 3. Checklist in Ministry of Employment and Labor

Div.	Main Contents
Corrective measure for Subcontractor	
1	Guidelines for working condition protection : 5 items
2	Effort for better working conditions 1) Reasonable subcontract payment, fair wages : 3 items 2) Occupation ability development : 3 items 3) Difficulties treatment : 2 items
Corrective measure for Employer.	
1	Guidelines for working condition protection : 4 items
2	Effort for better working conditions 1) Ensuring fair wages : 4 items 2) Worker's welfare, Using recreational facilities : 2 items 3) Measures for health and safety : 2 items 4) Occupation ability development : 2 items 5) Difficulty treatments : 1 items
Corrective measure for both sides.	
1	1) Contractors operating : 3 items 2) Job security : 6 items 3) Improvement of working conditions : 2 items 4) Labor-management cooperation : 2 items

등에 관한 법률 제6조에는 파견 기간과 고용의무에 대한 사항을 명시하고 있다.

2.2 외주 인력 운영에 따른 이슈 및 판례

판례1. K타이어 사례

(대법원 2011.7.1 선고, 2011두6097 판결)

도급인(K타이어)이 근로자들에게 일상적인 작업 지시를 한 적이 없더라도, 이는 업무 지시를 할 권한이 없어서라기보다는 이 사건 포장 직위가 단순, 반복적인 업무여서 별도의 구체적인 업무 지시가 필요 없었기 때문인 것으로 보이는 반면, 수급인(T조합)은 근로자들의 작업 내용과 시간에 대하여 독자적인 영향력을 행사할 수 없었다고 보여 작업배치를 결정하거나 구체적인 업무를 지시한 주체는 근로자들을 고용한 수급인이 아니라 오히려 이 사건 도급계약에 따라 근로를 제공받은 도급인으로 판단할 수 있다.

또한, 근로자들의 출결, 휴무나 초과근무상황 등

근태관리 역시 오히려 도급인이 수급인보다 더욱 직접적으로 해온 것으로 보인다.

위와 같은 사정을 종합하면, 원고는 근로관계에 있어 근로자들에게 직접적인 지휘, 명령권을 행사하였고 봄이 상당하므로, 이 도급계약은 실질적으로 파견법상의 근로자파견계약이라 할 것이다[10].

판례2. H자동차 사내하청 불법파견 인정 판결 (대법원 2010.07.22. 선고, 2008두4367 판결)

H자동차 (“이하 “원청회사”)의 사내하도급 업체인 E기업(이하 “하청업체”)은 의장 공정을 맡아 업무를 수행하던 중, 노동조합 활동을 이유로 2005. 2. 2. 근로자 15명을 해고하였다. 이에 근로자들은 ‘부당해고 및 부당노동행위 구제신청’을 원청회사와 하청업체를 상대로 제기하자 하청업체는 곧 바로 폐업하였다. 이 사건은 하급심에서는 원청회사가 사용자가 아니고 실제 사용자인 하청업체는 폐업하였다는 이유로 모두 기각되었으나, 대법원은 원청회사와 하청업체와의 목시적 고용관계는 부정 하였으나, 원청회사와 하청 업체 간에 파견관계가 성립된다고 인정하였다. 개정전의 파견법에 따라 근로자의 근속년수가 2년을 넘는 경우 “고용의제” 조항에 따라 근로자가 사용사업주에 고용된 것으로 본다고 인정을 받았다. 즉 법원은 ‘근로자파견 법리’와 사실관계를 바탕으로 근로자가 하청업체에 고용된 후 원청회사에 파견되어 원청회사로부터 직접 노무지휘를 받는 근로관계 있다고 판단하였다 [10][16].

판례3. 하청계약에 따른 근무환경 범위판결 (광주지법 2013.9.26. 선고, 2012가합51068 판결)

2007년 3월과 2008년 3월 A소속 근로자들을 대상으로 직장 내 교육훈련을 실시한 점, 피고 소속 근로자와 A소속 근로자가 중앙제어실에서 함께 근무한 점 등에 비춰보면 피고가 원고들의 이 사건 도급계약에 따른 업무 수행에 있어 일정 부분 관여한 것으로 보인다. 그러나 한편 A는 피고와는 별도의 독립된 사업주체로서 독자적으로 원고들을 비롯한 소속 근로자들에 대한 작업 배치권 및 변경 권을 가지고 있었고, 채용, 징계 등에 관한 기본적 권한을 가지고 있었을 뿐만 아니라 A는 소속 근로자들의 조퇴, 휴가 등에 관한 근태관리를 독자적으로 했고, 직접 임금을 지급한 사실이 인정된다. 또 피고는 A의 현장책임자, 현장대

리인을 통해 원고들에게 작업에 관한 지시를 했지만 이는 도급 업무 범위를 특정해 도급 목적을 달성하기 위한 것으로 도급계약에 따른 당연한 내용으로 보이고, 피고 소속 근로자들을 안전 관리자 등으로 선임한 것은 관련 법령상 시설의 소유자인 피고에게 안전관리자 등의 선임의무가 부과되어 있기 때문으로 그 주된 목적이 원고들에 대한 지시, 감독을 하기 위한 것으로 보이지는 않는다. 추가로 피고의 근로자들과 원고들이 작업 과정에서 혼재되어 배치되지 않았고 피고의 근로자들에게 결원이 발생했다고 해서 원고들이 그에 대한 대체 업무를 수행하지도 않았으며, 원고들이 피고의 지시에 의해 도급계약 외의 추가적인 업무를 하지는 않았던 점 등을 종합한 후, 재판부는 원고들이 피고의 관여정도와 원고들이 제출한 증거들만으로는 원고들이 피고의 지휘, 명령을 받아 피고를 위한 근로에 종사해 온 것으로 보기 어렵다고 판단하였다.

결국, 도급계약의 당연한 내용으로서 도급 업무 범위를 특정해 도급 목적을 달성하기 위한 취지에서 현장책임자, 현장대리인 등이 작업지시를 할 수 있는 것이고, 이러한 지시가 있었다고 하여 파견근로성을 인정할 수 있는 것은 아니라고 판단하였다[10][17].

2.3 내, 외부 인력으로 인한 보안사고 현황

지난 3년간 금융업계는 해킹, 내부인력 및 외부인력으로 인한 보안사고가 연달아 터졌다. 2011년 4월 H캐피탈에서 외부 해킹으로 175만 건의 고객정보가 빠져나갔고, 9만7000건의 고객정보를 내부 직원이 빼내간 H카드사 개인정보 유출사건(2011년 7월), 47만 건의 정보가 새어나간 S카드사 사건(2011년 8월) 등 몇 만 건 단위의 고객정보가 유출된 사건이 반복되었다[11].

Table 4. 에서 내부직원과 해킹 및 외부직원의 유출의 양은 실로 현격한 차이를 보인다. 내부직원에게 해 소규모로 유출된 개인정보가 외부직원에게 의해서는 대규모로 변해가고 있다. 현대사회에서 금융정보를 요구하는 시장은 커지고 있다. 은행, 카드, 대출, 부동산, 통신, 교육, 유통, 영화, 도박, 마트, 텔레마케팅, 스미싱 등 거의 모든 기업과 업체들이 개인 신용정보를 원한다. 정보 거래 가격은 고객이름, 전화번호, 집주소와 같은 단순정보는 한 건당 50~300원 정보에 거래된다. 1억 건 이상의 개인정보 접근권을 가진 정보소유자는 유출 유혹에 넘어갈 수 있다. 더군다나 개인정보 중 주민등록번호, 신용등급, 대출이력 등 고급

Table 4. Critical accident of information leakage in financial

Occurrence time	Company	The number of information exposure	Staff who spilled
December 2013	K Card Co. L Card Co. N Card Co.	140 million	Outsourced staff
May 2013	M Insurance Co.	160,000	Internal staff
April 2013	S Bank	34,000	Internal staff
March 2013	I Capital	5,800	Internal staff
February 2012	C Bank	103,000	Outsourced staff
August 2011	S Card Co.	470,000	Internal staff
July 2011	H Card Co.	97,000	Internal staff
May 2011	H Damage insurance	150,000	Hacking
April 2011	H Capital	1,750,000	Hacking

정보 가격은 더 높게 형성되어 있기에 내부 정보접근권을 가진 자는 더욱이 관리가 필요하다[12].

이러한 정보유출의 사회적 비용은 단순히 거래된 금액뿐 아니라 Table 5. 와 같이 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 나눌 수 있다. 이 비용은 조직의 생존의 존망을 결정 할 수도 있는 큰 비용이다[18].

Table 5. Classification of the Privacy leakage costs

Indirect costs	Cost for System management and Replacement	Loss of corporate image
Direct costs	IR response cost. Labor cost for accident correspondence. Decrease in sales due to reduced customer.	Legal costs Fall in stock price
	Explicit costs	Potential costs

이러한 이유로 매년 보안사고가 터질 때마다 금융당국은 전자금융 감독규정을 개정하는 등 보안조치를 강화했다. H손해보험, H캐피탈 등 무려 4건의 대형 금융보안 사고가 터진 2011년 말에는 전체 직원의

5%를 IT인력으로 채용하고, IT인력의 5%는 보안인력으로, 또 IT예산의 7%를 정보보호 예산으로 편성하는 전자금융감독 규정이 개정 되었다[1][5][6]. 하지만 이러한 조치만으로는 외주 직원에 대한 보안교육, 권한설정, 인력관리, IT투자 등의 보안실효성은 검증하기 어렵다. 대부분의 공공기관, 금융사 및 일반 기업에서는 전문 외주직원을 두어 HW, SW, 및 기타 IT장비를 관리하는 것이 관례화 되어있다. 특히, 이들 외주 직원들 중에는 관련 경력이 풍부하여 내부 업무 및 관련 정보 등 기술이 전문화 된 직원이 많다. 따라서 이런 외부 직원은 내부 직원보다 강력한 보안정책을 적용해야만 한다. 대부분 조직들은 관리적, 물리적 및 기술적 보안을 대상으로 내부통제 조직을 운영하고 있으나 이러한 외부 직원의 모든 업무를 통제하기란 어려우며 인력, 예산 등의 제약이 따른다.

III. 도급관리 현황에 대한 분석

이번 카드사태 등 정보유출 사건을 보면 알 수 있듯이 보안의 최대 위험요소는 내, 외부 인적 자원 요소이다. 내부정보 유출의 관리 핵심은 결국 관리적, 물리적, 기술적 보안시스템 도입과 운영보다 더 취약한 인적 보안으로 말할 수 있다. 그러므로 외주 인력에 대한 명확한 사전 관리정책의 설정과 실질적인 통제가 중요하다. 좀 더 정확한 외주인력의 실태를 파악하기 위하여 IT 경력 10년 이상의 전문인 48명에게 IT 시스템 개발 도급계약의 대한 설문조사를 실시하였다 [15]. 이 중 43명(89%)에게 설문지 회수를 하였으며 43명 모두 IT도급 관련 업체와 계약하여 SM(도급인력)과 프로그램 개발 및 유지보수 업무를 진행한 경험이 있다고 대답하였다. 이 설문지에는 품질과 인력 관리 의 대한 설문내용으로 구성되어 있으며 관리적 요소, 기술적 요소에서 의미 있는 데이터가 산출되었다.

3.1 관리적 요소

효율적인 보안 관리를 위한 인력관리, 절차관리, 사고대책 및 보안정책 수립이 필요하다. 최근에는 기존 외부 침입 대응 중심에서 내, 외부 통합 전사적 보안 관리의 필요성이 증대 되고 있다. 또한 정보보호 관리 체계 인증과 보안교육에 대해서도 개선이 필요하다. 현재의 보안 인증은 기업의 보안 안정성을 100% 보장해주지 않는다. 보안교육도 형식적인 시간 배분으로 보안의식 수준 향상을 피하기는 어렵다. 이러한 측면

에서 조직은 실질적인 로그 데이터를 다양한 측면에서 분석하면서 정보보호 활동을 지속적으로 유지, 개선해야 한다.

일단 외주 인력과 관련하여 현 실태를 파악하기 위해 외부직원에 대한 근본적인 질문을 설문지에 포함하였다. 설문지에 '외주 인력에 대한 단점은 무엇이라 생각하십니까?' 라는 질문에 30% 이상이 인적보안에 대한 사항을 단점이라고 대답했다. Fig.3. 은 외주 인력에 대한 단점을 설문한 결과이다.

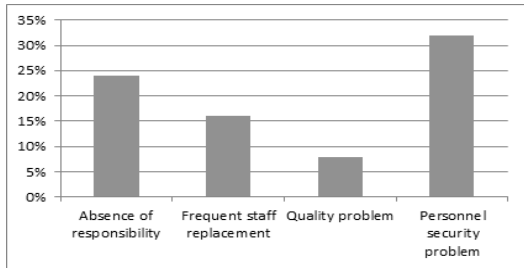


Fig. 3. Survey result of outsourcing weakness

사실 조직에서 효과적으로 인적 통제를 구현하는 것은 정보시스템을 통제하는 것보다 더 어렵다. 따라서 기업은 인적 보안에 대한 예방 활동을 어떻게 효과적으로 할 것인지 고민해야 한다. 결과적으로 관련 조직의 책임 및 리더십 그리고 지속적이고 체계적인 개인정보보호 수준 관리가 개인정보 유출을 비롯한 보안 사고를 예방하는 핵심 성공요소라고 할 수 있다. 다시 말해서 법규 요구사항 및 조직에 영향을 미칠 수 있는 여러 측면을 고려해 개인정보보호관리 활동을 실천하고, 효과적인 방법으로 이를 강화하는 것이 매우 중요하다고 할 수 있다[13][14].

3.2 기술적 요소

도급계약을 하는 이유는 여러 가지 이유가 있다. 설문지를 통하여 보면 가장 큰 이유는 비용절감(45%)에 있다. 이어서 업무 전문성(21%), 인력 탄력성(21%)가 뒤를 이어갔다. 즉 대부분의 도급계약은 내부인원으로도 충분히 시스템구축이 가능하나 시간, 비용 측면에서 좀 더 효율적인 도급계약을 이용하는 것이다

하지만 도급계약은 비용 및 시간을 절감하는 장점을 가진 대신 적정 품질 수준에 미치는 영향이 있다. 대부분의 설문자들은 '외주 인력이 도급업무에 대한 개발 프로그램 요구수준을 만족시켰습니까?' 라는 대

답에 대부분이 보통 이하를 대답하였다. 이유로는 프로그램 이해도 미비, 인력투입문제, 마감시한 문제, AS 미비 등 다양한 이유가 나왔다. 이처럼 도급계약은 비용과 시간을 절감 시켜줄 수 있지만 시스템 완성도에 대해서는 품질 수준이 떨어진다. 이러한 단점은 시스템 보안에 취약점으로 이어질 수 있다. 수준 미달의 시스템은 외부공격에 취약하며 재해 시 복구가 늦어질 수 있다. 따라서 외주 인적보안의 통제 및 모니터링을 통하여 외주 인력에 대한 위협에 대하여 위협 인자를 인식하고, 사고 예방 및 대응에 집중해야 한다.

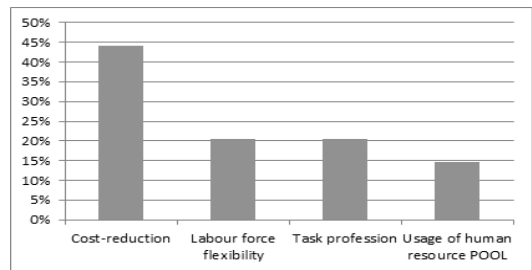


Fig. 4. Survey result of outsourcing reason

3.3 법률적 요소

금융권 정보보호 규제는 지속적 강화 또는 중복 되고 있다. ISO27001, 신용정보보호법, 개인정보보호법, 정보통신망법 및 금융전산 보안강화대책 등 내, 외부 인력에 대한 규정이 강화되고 있다. 금융감독원의 금융권 IT보안 실태 검사는 전자금융거래 안정성 확보, 전자금융거래 관련 내부통제, 이용자 PC 보안 대책 등 내부통제의 적정성과 전자금융 이용자 보호 관점에서 개인정보보호를 위한 필수불가결한 조치라 볼 수 있다. 앞으로 조직은 사후 방지 체계가 아닌 사전 방지를 위해 인력과 예산을 책정하고 개인정보보호 관리를 지속가능 핵심 사업전략으로 수립해야 한다.

IV. 도급관리의 리스크 관리를 위한 의사결정 모델

IT시스템의 원활하고 안정적인 운영 및 업무 개발에 필요한 인력을 확보하기 위해서는 첫째, IT도급에 관한 의사 정책 결정 절차가 필요하다. 이는 IT인력에 대한 기준 준수에 잘 나타나 있다. 둘째, IT내부인력과 외주 인력의 수행업무 조정이 필요하다. 특히, 금융기관의 영역을 계열사, 계정, 채널 및 서비스운영

등으로 구분하고 업체 간 경쟁체제를 조성하여 한다. 셋째, 효율적인 외주인력 운영 적용이다. 비용과 서비스 품질에 대한 실질적 운영 모델을 검증해야 한다.

4.1 IT도급에 관한 의사 정책 결정 Flow Task professionalism

IT도급 및 인력 재조정은 업무 전환 리스크를 최소화 하여야 한다. 이러한 금융보안 위협 리스크를 줄이고 정책을 수립하기 위해서는 IT도급 정책 결정 절차에 따라 진행해야 한다. 기존 수행업체 및 숙련된 인력을 포함하도록 유도하여 업무 연속성을 확보하며, 인계인수 및 장애대책 방안 수립하여 활용해야 한다. 또한 안정적인 운영과 경제적 효율성을 고려하여 계약기간을 장기화 할 필요가 있다. 보통 1년 주기이나 2년으로 계약기간을 연장하면 단기 계약으로 인한 잦은 외주인력 교체 및 인력수급 문제 해소를 할 수 있다. 장기계약은 안정적 계약기간 확보와 계획성 있는 인력 운영을 통한 비용 절감을 달성 할 수 있다. 최근 금융기관들은 품질을 높이기 위하여 서비스 수준협약 (SLA : Service Level Agreement) 체결을 통하여 품질을 보증하기도 한다.

4.2 IT내부인력과 외주 인력의 수행업무 조정

전자금융거래의 안정성 확보를 위한 '금융회사 정보 기술(IT)부문 보호업무 모범규준' 준수를 위하여 IT 내부인력, IT계열사 및 외주 인력의 수행업무 범위에 대한 재조정을 하였다.

금융기관의 인력운영은 원칙으로 금융위원회 IT모범 규준 준수를 위한 본질, 비본질 업무 분류 및 운영 기준을 준수한다. 업무 분류 원칙에 따라 IT업무를 구분하며, 업무별 수행 인력을 분석한다. IT모범 규준에 따라 본질적 업무는 금융기관 내부 IT인력 및 계열사 IT인력(분석, 설계 제외)만 수행 가능하며, 외주 인력은 비본질 업무(코딩관련 업무)를 수행함을 원칙으로 한다[6]. 업무 안정화를 위해 본질의

중요업무는 이동을 최소화 하고, 비본질의 일반 업무는 가급적 외주인력 위주로 운영한다. Table 7. 과 Table 8. 은 본질, 비본질 업무 분류를 보여 준다.

Table 6. The flow of a IT policy decision

Workflow	Business management	Details of Business affairs
Work classification and Workforce Planning	IT Staff management Legal Office Service Management Department	Business classification definitions Business classification Major/Trivial Classification IT Model Criteria reflection Subcontract and related law investigation
Performing Plan Establishment	IT Staff management	IT tasks for internal and outsourced classification budget and personnel adjustment Separation development process
Management's Decisions	Payment management Department Audit department	Compliance with regulation Audit Review
Vendor Selection	Selection departments	Personnel Computation Evaluating qualifications of contractor
Partner Agreement	Contract Department	Make IT contract Make SLA contract agreement
Operating	IT Staff management	Consultation of representative and IT personnel

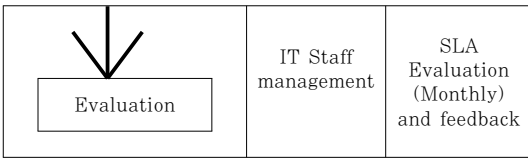


Table 7. Major, Trivial task classification (A company)

Division	Major	Trivial		Total
	Core	Important	Normal	
Tasks	127	150	76	353

Table 8. Define of IT performing business

Section	Contents
Major Tasks and Components (Business of internal personnel)	
1. According to IT Model Criteria : Business for internal personnel	1) Tasks including fundamental components of financial business with approval 2) Business that financial institutions are obligated to perform due to laws and regulations. 3) Significantly concerned business that occur from outsourcing which greatly reduces the reliability and integrity of the financial companies or occurrence of damage due to disorderly financial order in financial or user.
	4) Business that has critical social impact that directly deals with Financial Companies important information which has high risk on accidents caused by leakage of information. 5) Business in connection with the fund transfers such as stock trading and funding which can induce major monetary accidents that are directly caused by the information technology sector. 6) Business that has to be performed on administrator(root) authority in information processing system.
2. Finance Committee, Financial Company IT System Business	1) Tasks, including fundamental components such as deposit, loan, exchange transaction, etc., that prohibits commissioning in the Financial Holding Companies Act on IT systems 2) Among finance company's support service, business that deals with decision-making on important matters and back-office support. 3) IT strategies, Financial Management regulations 4) IT budgets, resource planning and management 5) IT resources and purchasing

	management 6) IT construction supervision resources and purchasing management 7) IT construction supervision Planning and implementation 8) Control of personnel according to outsourcing contract - Management and access control policies on computing center - Financial management on control procedures and applying outsourced personnel with separation duties to prevent leakage or falsification of information. 9) Establish internal information protection policy. The revision of the guidelines and information protection related regulations. 10) Development and implementation of information protection on electronic financial 11) IT internal control in order to protect the information (System restrictions, Account Management, etc.) 12) Development and implementation plan and enforcement on vulnerability analysis and evaluation.
Trivial Tasks (Business of IT Subsidiary & Resident Outsourcing Personnel)	
3. Finance Committee, Financial Company IT System Business	(Can be performed by IT Subsidiary Financial Group) 1) IT systems development and operation of task can be consigned among deposit, loan, exchange transaction, etc. (Payment through ATM, money transfer and balance inquiry, etc.) 2) Development and management of groupware, e-mail, personnel system, such as the accounting system to be used by the co-operation between subsidiaries 3) Development of the business program, which is an essential element (except for the analysis and design) 4) Operation and management of disaster recovery center 5) Other business can be performed by resident outsourcing personnel. (Can be performed by resident outsourcing personnel) 6) IT systems development and operation of task can be consigned among the fundamental components of financial business (except for the analysis and design)

	<ul style="list-style-type: none"> 7) IT systems development and operation of tasks, which are Non-fundamental financial business components. (groupware, e-mail, personnel system, accounting system, etc.) 8) Operation and management of system's hardware and software (Systems of mainframe and server, middle-ware, storages, etc.) 9) Operation and management of network's hardware and software 10) Operation and management on disaster recovery center (except for business program) 11) Construction and Operation of the attempts on control infringement 12) Human resources for a simple business of IT system 13) Managing personnel infrastructure such as Generators, UPS, constant temperature humidity chamber, fire equipment and etc. 14) Installation of security system to prevent electronic information infringement .(hacking, cracking) 15) Emergency maintenance for security system (Patch, update) for prevention.
	<p>Trivial Tasks (Can be performed by outsourcing)</p>
4. According to FSS : Can be Outsourced	<p>Agency for trading, utility billing, receiving and payment</p> <p>Management for supplies, tax, budget, accounts, performance, personnel, inspection, IFRS, end-terminal and automation device.</p> <p>Analysis report for individual & company customer</p> <p>Anti-money laundering</p>
5. Others internal classification IT business	<ul style="list-style-type: none"> 1) Stand-alone system (domain+task+independence) 2) Intensification of IT organization and technical capability 3) Tasks which has to be performed by internal personnel (trivial tasks but involving high risk) 4) Business that operated mainly by outsourcing personnel <p>※1), 4) can be outsourced 2), 3) cannot be.</p>

금융기관들은 Table 7. 과 Table 8. 의 외부주문 등 금지업무의 업무 위탁 운영기준을 반영하고 관련 외주주문 등 금지업무의 내부인력 수행방안과 외주인력 운용방안을 수립해야 한다. 이와같은 IT 내부인력과 외주 인력의 수행업무 조정은 본질 업무에 대한 내부인력의 운영 강화가 주목적이다. 한편으로 외주 인력의 수행업무 취약점을 개선할 방법은 개발 공정분리를 이용한다. 요구사항 정의, 분석, 설계, 구현, 테스트, 사용자 교육 및 이행 등 전산 개발단계에 있어서 IT개발 조직의 역할을 사전 협의 및 요청 접수(AM), 요구사항 정의 및 분석설계(BA), 구현, 테스트 및 이행(개발자) 등 개발 공정 단위로 분리함으로써 전문화된 IT 서비스를 제공하고 IT 인력의 운영 효율화를 도모하기 위한 IT 개발관리 방법론의 체계를 정비하는 것이다.

AM (Account Management)은 IT 부서의 전산개발 창구로 개발 사전협의 및 요청 접수를 담당하고, BA (Business Analyst)는 요구사항 정의 및 분석 설계 전문가이다.

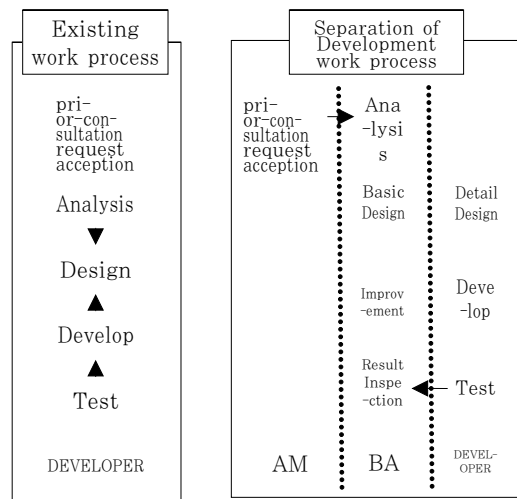


Fig. 5. Diagram of separation process

공정분리는 기존 1인 중심 전체 개발공정 전담체제를 기능중심 개발조직 체제(공정별 담당자 분리 체제)로 전환하는 것이다. 즉, BA 중심의 업무 수행으로 업무에 대한 가이드 제시 및 개발 결과에 대한 점검이 가능하다. BA는 업무 경험 및 개발 내용에 대한 이해를 바탕으로 개발 내용 개선 및 업무 개선까지 수행한다.

개발 공정분리는 전산개발 및 운영에 관한 중 주요 정책 결정사항이다. 금융상품의 복잡성과 정보보호의

중요성이 대두된 현 상황에서 BA 인력 분리에 따른 영향과 개발자 1인 전담 업무 방식을 공정분리 방식으로 전환 할 때 조직은 업무 영향을 고려 할 수 밖에 없으며 공정분리 관련 예상 리스크와 그에 대한 대응방안을 종합적으로 다음과 같다.

첫째, 업무연속성이다. BA 분리에 따른 업무 담당자 변경 및 순수 개발자 감소로 운영리스크가 증가 될 가능성이 있다. 이러한 리스크의 대응방안으로 안정화 시점까지 BA, 개발자간 탄력적 상호지원 운영이 필요하고 공정분리 적용 초기에 업무 연속성 유지를 위한 업무별 비상 대응 체제를 운영하여 문제 발생 시 조기 대응해야 한다.

둘째, 업무 적시성이다. 공정분리 조직 내에 내재화 되는 과정에서 업무수행 방식이 변경됨에 따라 업무 적시성이 저하될 가능성이 있다. 이러한 리스크의 대응방안은 복수 업무 연관 의뢰 건에 대한 신속한 R&R 조정하고 의뢰건별 대고객 서비스 영향 Time-to-Market의 중요도를 감안하여 차등적인 개발 계획을 수립(AM) 한다.

셋째, IT서비스 품질이다. BA와 개발자가 업무 전문 역량을 단기간 내에 확보하기 어려우며, 전문성 미 확보 상태에서 IT서비스 품질이 저하될 가능성이 있다. 이러한 리스크의 대응방안은 업무별 특성과 BA, 개발자 배치 인력의 업무 역량을 고려한 업무 도메인을 그룹별 공정분리 운영모델(세부역할, 작업 수준 등)로 최적화 설계 한다.

한편으로 현재 공정분리를 실시하고 있는 A사 적용 사례를 살펴보면, 공정분리 효율성은 5가지로 나타나고 있다.

첫째, 가용성 측면이다. 세분화된 직무 부여와 업무 할당으로 직급, 연공 구분 없이 개발인력 전체의 가용성 확대가 되며, 점진적으로 1인 담당 업무 커버리지가 증가 된다. 이는 개발자 인력 Pool제 운영에 보다 효율적이다.

둘째, 전문화이다. 담당업무 및 직무에 대한 전문성과 역량에 맞게 업무배치가 가능하다.

셋째, 업무부하 분산이다. 1인 중심 업무 방식과 비교하여 업무 부하와 특정한 의존도가 분산되고 있다.

넷째, 프로세스 개선이다. 복수 개발의뢰에 대해서 AM, BA, 개발자별 업무처리를 병렬처리 할 수 있다. 또한, 커뮤니케이션 활성화와 인수인계 활동이 가능하게 되었다.

다섯째, 문서화이다. 문서화를 통한 업무 자료의 최

신화를 유지함으로써 신규업무 및 유지보수가 용이해졌다. 그 만큼 분석력의 기술력이 축적되고 있다.

IT개발에 프로그램 품질이 가장 중요한 요소인 만큼 개발부서는 분석설계팀을 조직하여 IT업무 분류에 따른 본질업무와 비본질업무의 효율성을 높이는 활동을 하여야 한다.

4.3 효율적인 외주인력 운영 적용사례

금융보안사고의 재발을 막기 위해서 금융회사 차원에서는 내부직원 양성을 하고 외주 인력을 관리하는데 대한 투자를 확대해야 한다. 정부 차원에서 보안 전문 인력을 양성하기 위해서 사이버인력 양성, 장학금 등 투자를 늘리는 적극적인 지원이 필요하다.

4.3.1 비용측면

앞에서 IT시스템의 원활하고 안정적인 운영 및 업무 개발에 필요한 인력을 확보하기 위해서 도급 업체 확대를 통한 서비스 품질 향상 및 비용절감이 필요하다고 설명했다.

IT모범 규준에 따라 본질적 업무는 금융기관 내부 IT인력 및 계열사 IT인력만 수행 가능하며, 외주 인력은 비본질 업무를 수행함을 원칙으로 하고 금융지주 회사의 전산자회사 재하청 인력은 정보기술부문 IT인력으로 인정 불가능하다. 외주 인력은 도급계약을 통한 인력만이 금융회사 내부 IT인력 범위 내에서 정보 기술부문 IT인력으로 인정된다. 따라서 그동안의 IT

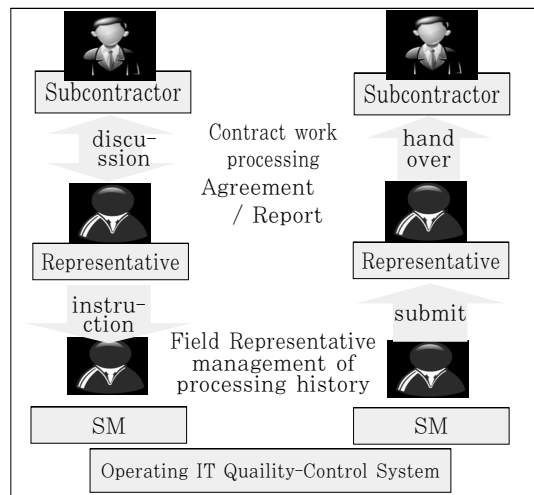


Fig. 6. Business process of IT outsourcing

계열사의 하청 등을 통하여 외주인력 공급방식이 외주 전문 업체와의 도급 직계약으로 변경되어 비용 절감이 발생했다. Table 9.에서 보여주듯이 2013년 도급 외주 인력의 도입으로 비용 절감이 발생한 사실을 확인할 수 있다. 외주인력 도급업체는 직계약에 따른 현장 대리인을 상주시켜 경영 및 노무 상의 독립성을 유지하고 도급 업무에 대한 전문성을 가지게 되었다.

Table 9. Monthly mean unit price of IT outsourcing(A company)

(Amount Units : One Thousand won)

2011y	2012y	2013y	remarks
8,032	8,032	7,522	

4.3.2 품질측면

Fig.6.은 IT전문가들이 외주 인력이 도급 업무에 대한 개발 프로그램 만족도를 나타낸 그래프다. 앞에서 언급했듯이 전체 설문자에 50% 이상이 보통 이하의 평가를 내리고 있다.

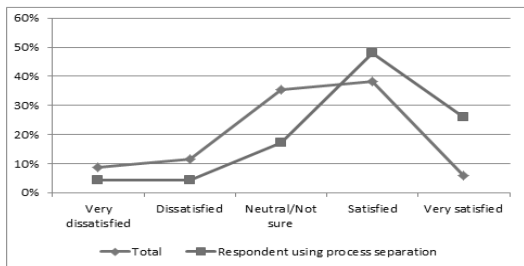


Fig. 7. Satisfaction Survey of IT outsourcing

따라서 도급계약에 따른 품질 관리 기준 마련이 꼭 필요하다. A사 경우 IT도급 업무인 경우 반드시 도급 업체의 현장대리인을 통하여 업무가 진행된다. 도급 계약 업체의 현장대리인은 인력의 신규, 교체, 퇴사, 본사 복귀 등의 사유 발생을 관리하고, 외주 인력에 대한 인원수 관리, 인원현황 및 근무상황 등을 수시로 파악하여 외주 인력의 효율적 운영을 기한다. 주요 변동사항에 대해서는 사용사업주의 IT인력관리 담당자에게 통보하고, 외주 인력에 대한 채용, 해고, 징계 등 인사결정권을 수행한다. 또한 외주 인력에 대한 작업 배치, 변경결정권 및 외주 인력의 업무지시감독권을 수행한다. 위와 같이 현장대리인을 갖추고 공정분리를 실시한 경우 도급 업무 성과물의 만족도가 만족이상이 80%가 넘음을 알 수 있다.

따라서 금융기관 등 회사 내의 외주 인력관리 업무 매뉴얼에 도급 업무를 통제하고 관리할 수 있는 규정 및 관리기준을 보완해야 한다. 외주활용 업무관리, 서비스수준 협약 등으로 관리범위를 명확하게 할 필요가 있다.

외주활용 업무관리는 IT외주인력 수급계획을 수립하며 외주활용 업무 정의를 통해 업무의 지속성과 안정성을 확보하며 업무표준화를 한다. 금융기관은 이를 통해 외주업무 운영, 중요도, 외주활용 및 접근통제 관리를 하며 외주활용 기준을 통해 기술자 등급을 관리하고 주기적 점검을 통해 효율적 외주활용 업무관리가 되도록 해야 한다.

서비스 수준협약(SLA : Service Level Agreement)의 목표 수준을 명시하여 투입인력, 업무량, 범위 등을 산정하고 합리적인 용역대가를 지불할 수 있어야 한다. 따라서 서비스 수준협약 체결을 통하여 업무운영, 서비스범위, 결과측정 및 점검을 하여야 한다. 또한 관리지표 기준을 명시하여 측정 항목을 관리하며, 대가 산정을 통하여 적적하고 합리적인 업무량, 서비스 기능, 서비스 기술 수준을 마련해야 한다.

Table 10. Organization principle of SLA

Section	Contents
1. Setting Clear Business Objectives	To set clear business objectives through consultation and review on business operations between the subcontractor.
2. The Definition of the scope and purpose of the service.	Define the desired product output performance and the range of IT services. For each item in the terms of the SLA, set the needs and documentations of them.
3. Consideration Service Measurement items.	Available SLA services should be composed of item with measurable result. The compensation system and corresponding penalties to each situation should be reflected. (regarding companies specific characteristics, it is often compromised as penalty)
4. Periodic inspection	It should be defined to allow documentation of actual performances and allow adjustment on the level of service objectives according to the changes in the environment.

Table 10.은 SLA 구성 원칙의 예이다. 이를 참조하여 IT도급 서비스 수준 합의서를 작성한다. 합의서 체결목적, 용어정리, 책임과 의무, 합의서의 운영관리, 합의서의 적용대상기간, 서비스 수준보고, 서비스 수준 측정, 서비스 수준 평가, 서비스 수준 목표 (MSL, ESL), 정산, SLA 개정 및 해석 및 분쟁의 해결 등을 명확히 정리 한다.

월 도급 비용 정산 시 서비스 수준 성과 측정 정의서 지표에 따라 서비스 수준 성과 보고서를 작성하여 서비스목표 수준(MSL, ESL) 준수 여부를 확인한다. 준수 확인여부 후 서비스수준 평가 보상기준에 대한 SLA 평가표와 종합등급 산정하여 제출한다.

Table 11. Define the SLA's aim level

Division		Achievement Rate.	Section Cost	Grade	Goal
Objective	Base-lines	Above 95%		A	Exceeded
ESL	85%	Above 85%		B	Attained
-	-	Above 75%		C	
MSL	75%	65%~75%	Penalty	D	Short
-	-	Below 65%	Section	E	-fall

서비스 목표 수준을 기본 Table 11. 처럼 정의하고 지표영역에 가중치를 두어 실제 현장 적용 평가 산정표를 작성했다.

Table 12. SLA application (A company)

Service level measurement item		Weighting	MSL	ESL
Satisfaction	Work satisfaction	25%	75	85
Productivity	Performance rate	25%	90	98
Quality	Problems	25%	100	100
Security	Observance	15%	75	100
Personnel	Rate of Change	10%	75	100
Total		100%		

관련 계산 수식은 만족도는 ((설문항목별 평가점수 합계) × 4) × 가중치, 생산성은 (((실적 - MSL) / MSL) + 1) × 100) × 가중치, 품질은 장애 등급별 점수 차감(100- 차감점수), 보안은 (100 - (적발건수 × 3)), 인력은 변동인원 표에 따른 점수로 각 서비스

수준 항목별 점수를 산출을 한다. 아래 Table 13.은 3개월간, A사 도급 현장의 11개 도급업체에 대하여 SLA 시범 적용 3개월간 적용한 결과 값이다. 데이터를 분석하여 보면 평균 97점 이상으로 관련 지표를 충분히 이해하고 도급업체 현장대리인의 독립적인 지시와 감독으로 안정적인 운영이 되고 있음을 볼 수 있으며 본 논문에서 제안하는 정책결정 과정 및 외주 인력 운영 정책이 효과가 있음을 보여주고 있다.

Table 13. Present state of application of SLA for 3 months (A company)

Service level measurement item		M1	M2	M3	Avg.
Satisfaction	Work satisfaction	22.90	22.36	22.57	22.61
Productivity	Performance rate	25.00	24.94	25.00	24.98
Quality	Problems	25.00	25.00	25.00	25.00
Security	observance	15.00	14.92	15.00	14.97
Personnel	Rate of change	9.83	10.00	10.00	9.94
Total		97.73	97.22	97.57	97.50

V. 결론

5.1 요약

현 카드 사태 등 금융 현황을 보았을 때 전자금융감독 규정 준수는 내부인력 증원에 따른 금융보안 리스크를 감소시키는 중요 요소가 되었다. 다만, 외주 인력에 대한 사전 및 보안에는 어느 정도 한계가 있다. 본 논문에서는 IT도급 정책 결정 절차에 따른 분석, 설계 등의 본질 기술 업무를 IT내부 직원이 수행하고 검증된 개발 설계서 요구를 이해하여 외주직원이 코딩함을 제안함으로써 비용, 품질 그리고 리스크에 대한 만족도를 높일 수 있으며 외주 인력의 내부시스템 접근을 제한함으로써 외주 인력 보안리스크를 줄일 수 있음을 확인하였다.

5.2 발전방향

본 논문은 은행 업무에 한정하여 외주 인력 운영리스크를 줄이는 방향으로 작성되었다. 앞으로의 연구는

증권사, 보험사 내부 데이터 및 업종의 특성을 반영하여 금융권 전체의 가이드라인이 될 수 있는 외주 인력의 운용방안 연구가 진행되어야 할 것이다. 또한 도급 계약약을 통한 자회사 영향도 또한 고려되어 정책을 수립 할 수 있도록 관련연구가 진행되어야 할 것이다.

References

- [1] Financial Services Commission, "Electronic financial supervision regulations general revision," Oct. 2011.
- [2] Financial Services Commission, "Electronic financial supervision regulations part revision," Oct. 2012.
- [3] Financial Services Commission, "Electronic financial supervision regulations part revision," Det. 2013.
- [4] Financial Services Commission, "Electronic financial supervision regulations part revision," Mar. 2014.
- [5] Financial Services Commission, "Best practice standards for the protection of IT in financial industrial," Oct. 2011.
- [6] Financial Services Commission, "Best practice standards for the protection of IT in financial industrial revision version," Nov. 2012.
- [7] The Bank Of Korea, "http://www.bok.or.kr/contents/total/ko/boardView.action?menuNaviId=559&boardBean.brdid=104055&boardBean.menuId=559," Feb. 2014.
- [8] spnam, "news.einfomax.co.kr/news/articleView.html?idxno=94088," Jan. 2014.
- [9] Employment and Labor Policy Report, "http://www.moel.go.kr/view.jsp?cate=2&sec=1&mode=view&bbs_cd=005&state=A&seq=1311642969853," Nov. 2011.
- [10] Eun Jung Park, "Distinction of worker dispatch contract and Subcontractor contract : 07.01.2011 Supreme Court sentenced, 2011 du 6097 rulings," Korea Labor Law, no. 40, pp. 316-320, Dec. 2011.
- [11] Bo Young Kim, "www.hankyung.com/news/app/newsview.php?aid=2014011343101," Jan. 2014.
- [12] Ki Wan Ko, "www.hankyung.com/news/app/newsview.php?aid=2014012750251," Feb. 2014.
- [13] Boannews, "www.boannews.com/media/view.asp?idx=39827," Feb. 2014
- [14] hkshin, "http://www.etnews.com/201401170509," Feb. 2014.
- [15] Myung-Sub Sim "An Empirical Study on the Improvement of Security Levels in IT Outsourcing Services," pp. 21-22, 2013.
- [16] General Legal Information, "http://glaw.scourt.go.kr/wsjo/intesrch/sjo030.do?q=%20%EC%84%A0%EA%B3%A0%202008%EB%91%904367&tabGbnCd=#//," Oct. 2010.
- [17] Gwangju District Court, "http://gwangju.scourt.go.kr/dcboard/new/DcNewsViewAction.work?seqnum=11777&gubun=44&score_kname=%BF%EC%B8%AE%B9%FD%BF%F8%20%C1%D6%BF%E4%C6%C7%B0%E1¤tPage=4&searchWord=&cbub_code=000510," Sep. 2013.
- [18] Seung Wan Chai, SIS 2006-KISA symposium, "Internet infringement accident damage costs calculated model," Jun. 2006.

〈저자소개〉



최 창 래 (Chang Lai Choi) 정회원
 1995년 2월: 광운대학교 전자통신공학과 졸업
 2013년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
 <관심분야> IT교육/인력관리, IT기획/구매/계약, 정보보호, 통신공학



윤 장 호 (Jang Ho Yun) 정회원
 2012년 8월: 고려대학교 정보수학과 졸업
 2014년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
 <관심분야> 금융보안, 위험관리, 정보보호컨설팅



이 경 호 (Kyung Ho Lee) 종신회원
 1989년 8월: 서강대학교 수학과 학사
 1997년 8월: 서강대학교 정보통신대학원 석사
 2009년 8월: 고려대학교 정보보호대학원 박사
 1994년 2월 ~ 현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
 2011년 9월 ~ 현재: 고려대학교 정보보호대학원 조교수
 <관심분야> 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책